EXCESSIVE DATA COLLECTION PRACTICES OF WHATSAPP (RE)SCRUTINISED UNDER THE NDPR: A REVIEW OF FCCPC V. META

Excessive Data Collection Practices of WhatsApp (re)Scrutinised under the NDPR: A Review of FCCPC V. Meta

Chukwuyere Ebere Izuogu

Image credit: https://fccpc.gov.ng/

Introduction

On 19 July 2024, the Federal Competition and Consumer Protection Commission (FCCPC or Commission) in Nigeria imposed a fine of $220 million on Meta Platforms Inc (Meta), the parent company of WhatsApp LLC (WhatsApp), for violations of both the Federal Competition and Consumer Protection Act 2018 (FCCPA) and the Nigeria Data Protection Regulation 2019 (NDPR). In the investigation report that served as the basis for this penalty, the FCCPC formulated three main issues for determination. One of these issues was whether WhatsApp's 'business practices with respect to its data collection and management processes are excessive, unscrupulous, obnoxious and a deliberate tactic to exploit Nigerian consumers, contrary to the FCCPA and NDPR'. The FCCPC ruled in the affirmative on this issue.

In this article, I examine this particular aspect of the FCCPC's determination in relation to the provisions of the NDPR. Readers should note that in this review, I will endeavour to provide an objective and impartial analysis of this determination. My aim is to offer insights into the underlying analysis that informed the FCCPC's determination on this issue and to assess whether this analysis is consistent with the proper interpretation of the NDPR in the light of evolving data processing operations.

The legal basis for FCCPC's determination

The FCCPC in reaching this particular determination exercised among others, its section 17 (a) power under the FCCPA. This provision charges the FCCPC with the responsibility of enforcing any other enactment related to competition and consumer protection in Nigeria. In exercising this authority, the FCCPC interpreted the NDPR as a consumer protection law. Although this interpretation of the FCCPC's statutory function is novel in Nigeria and may be subject to scrutiny in appellate courts, there are persuasive case laws from the United States (U.S) where courts have recognised the Federal Trade Commission (FTC), the lead consumer protection agency in the U.S., as having broad data protection enforcement authority in instances where consumers are exploited. This authority is derived from section 5 of the FTC Act, which prohibits 'unfair or deceptive acts or practices'—a phrase that closely parallels the term 'obnoxious practices or the unscrupulous exploitation of consumers' found in section 17(s) of the FCCPA.

While the scope of the FCCPC's power to enforce the NDPR and address data privacy infringements as a form of consumer harm remains uncertain in Nigeria, the following U.S. cases may offer some guidance: *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014); *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 609 (D.N.J. 2014); and

FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 247–48 (3d Cir. 2015). These cases originated from a single matter in which Wyndham Worldwide Corp., a hotel chain, contested FTC's authority to enforce data security practices following a series of data breaches suffered by the hotel. Upon appeal to the U.S. Court of Appeals for the Third Circuit, the court upheld the FTC's authority, holding that lax cybersecurity practices leading to a data breach fall within the 'unfairness' prong of the FTC Act. This decision affirmed the FTC's jurisdiction to address and enforce violations related to data privacy.

It is crucial to emphasise that when the FCCPC chooses to exercise its consumer protection authority to enforce the NDPR, any subsequent determinations or outcomes resulting from such enforcement actions must be in strict adherence to both the spirit and letter of the NDPR.

Excessive data collection under the NDPR

Under the NDPR, one of the governing principles of data processing provided for in article 2.1 (1) b) is that personal data (processed) shall be 'adequate, accurate and without prejudice to the dignity of human person'. The reference to the word 'adequate' means that personal data collected must be limited to the minimum necessary to achieve the intended processing purpose, ensuring that the data collected is proportionate to the purpose pursued by the processing operation.

This principle is otherwise referred to as data minimisation under the General Data Processing Regulation (GDPR) and in most jurisdictions with a data protection framework. This principle (and others provided for in the NDPR and in the Nigeria Data Protection Act 2023) must be complied with whenever personal data is processed irrespective of the lawful base. In essence, data minimisation requires that data controllers and processors collect and process only the personal data that is directly relevant and essential to accomplishing the specific purpose of the processing operation. Consequently, data controllers and processors must exercise diligence to refrain from collecting excessive personal data from data subjects (in this case WhatsApp users in Nigeria) beyond what is necessary to achieve the intended purpose of the data processing operation

(Re)scrutinising the analysis of the FCCPC

As previously noted, one of the issues formulated by the FCCPC in determining that Meta violated the NDPR, and by extension the FCCPA, is:

> Whether WhatsApp's 2021 Updated Privacy Policy (Policy) and business practices with respect to its data collection and management processes are excessive, unscrupulous, obnoxious, or exploitative contrary to the FCCPA, including the mandate under [s]ection 17(a) regarding enforcing other enactments on competition and consumer protection.[1]

[1] FCCPC and NDPC, 'In the Matter of Investigation into Possible Violations of The Rights of Nigerian Consumers In The Provision Of Contact-Based Instant Messaging Service In Nigeria And Enquiries Into Obnoxious, Exploitative, and Unscrupulous Business Practices by WhatsApp LLC And Meta Platforms, Inc. Under The Federal Competition and Consumer Protection Act, 2018 Investigative Report of the Federal Competition and Consumer Protection Commission and the Nigerian Data Protection Commission' (13 November 2023) <https://fccpc.gov.ng/wp-content/uploads/2024/07/Excutive_Summary-_WhatsApp_Investigation-13.11.23.pdf> accessed 28 August 2024, p. 13.

As an initial matter, the reference to 'other enactments on … consumer protection' in this context should be understood as specifically referring to the NDPR.[2] Consequently, the analytical framework that should be applied will be solely based on those established under the NDPR.

In its analysis, the FCCPC asserted that WhatsApp collects 44 metadata points, in contrast to Signal and Telegram, which collect only 4 metadata points each.[3] Based on this comparison, the FCCPC questioned the necessity of such extensive data collection for providing WhatsApp-related services to users in Nigeria.[4] While the FCCPC's assertion regarding WhatsApp's (meta)data collection practices may be accurate, it is essential to first establish that each of these metadata points constitutes personal data to trigger the application of the NDPR. For ease of reference, article 1.3 xix of the NDPR defines personal data as follows:

> 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, Personal Identifiable Information (PII) and others.

Although these metadata points were listed in Annexure 1 of the investigation report, it is improbable that all of them would be capable of identifying a natural person, either directly or indirectly, and thereby come within the meaning of personal data in the NDPR. An individual is identified when he is capable of being 'distinguished' or 'singled out' from among a group of persons, and identifiable when, 'although the person has not been identified yet, it is possible to do' so.[5] From my perspective, it remains unclear to what extent the FCCPC has determined that each of the metadata points collected by Meta constitutes personal data capable of identifying an individual. If it can indeed be demonstrated that these metadata points qualify as personal data, then the FCCPC's claim regarding the collection of such data, especially in comparison to platforms like Telegram and Signal, may be legitimate.

Another key consideration in assessing the FCCPC's determination on this issue is the question of how 'excessive' WhatsApp's data collection practices are,

[2] See also ibid., p. 60; FCCPC and NDPC, 'In the Matter of Investigation into Possible Violations of The Rights of Nigerian Consumers In The Provision Of Contact-Based Instant Messaging Service In Nigeria And Enquiries Into Obnoxious, Exploitative, and Unscrupulous Business Practices by WhatsApp LLC And Meta Platforms, Inc. Under The Federal Competition and Consumer Protection Act, 2018 Investigative Report of the Federal Competition and Consumer Protection Commission and the Nigerian Data Protection Commission Executive Summary' (13 November 2023) <https://fccpc.gov.ng/wp-content/uploads/2024/07/Excutive_Summary-_WhatsApp_Investigation-13.11.23.pdf> accessed 29 August 2024, p. 7.

[3] FCCPC and NDPC (n 1) 14 – 15.

[4] FCCPC and NDPC (n 1) p. 15.

[5] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' (20 June 2007) <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf> accessed 23 April 2021, pp. 12 - 13.

considering the specific factual scenario surrounding its data processing operations. This determination is not an abstract concept and should not rely merely on the recitation of provisions from the NDPR or general data protection principles. Instead, the FCCPC must present clear and objective evidence to substantiate its claims. The crux of the matter is not solely the volume of personal data collected; rather, it concerns whether any of these metadata points are not directly relevant and necessary for achieving the specific purpose of the processing operation conducted by WhatsApp.

In other words, WhatsApp's data collection practices would be deemed excessive—and thus unnecessary in relation to the processing purpose—if it can be shown that the purpose could be accomplished without including certain metadata points (assuming they constitute personal data) in the collection or processing. Therefore, WhatsApp's data collection practices would violate the data processing principle of being adequate as provided in article 2.1(1) b) of the NDPR if there is clear and convincing evidence demonstrating that the metadata points collected are not relevant to the provision of WhatsApp services to users in Nigeria.

In this context, it is noteworthy that the FCCPC did not provide a detailed analysis demonstrating how any of these metadata points are irrelevant to the services provided by WhatsApp in Nigeria. Instead, the FCCPC requested Meta to provide a log of all data points collected, along with an explanation of the necessity or otherwise of such data.[6] This approach appears to fall short of the well-established evidentiary standard that 'he who asserts must [convincingly] prove'[7] required to substantiate the claims of excessive data collection.

While it is pertinent to state that the National Information Technology Development Agency (NITDA) provided information which, according to the FCCPC indicated that:

> certain data collected by Meta Parties were indeed necessary for the efficient provision of the service for which "consent" may be dispensed with; however, some other data collected were not necessary for the provision of WhatsApp services, and as such is excessive, optional, and unnecessary with respect to the service WhatsApp provides.[8]

However, neither the FCCPC nor NITDA provided concrete details regarding the specific meta data points collected or how they were determined to be necessary or unnecessary for the provision of WhatsApp services. In my view, a thorough and detailed examination of these data points would have significantly strengthened the argument, demonstrating which metadata points are essential and which are not in the context of WhatsApp's data collection practices related to the services provided to users in Nigeria. Meeting this evidentiary standard would undoubtedly bolster the FCCPC's finding that WhatsApp engaged in excessive data collection practices,[9] a claim that is more likely to be upheld upon appellate review.

A further point to consider in the FCCPC's analysis of WhatsApp's data collection practices is their statement from the above quotation which reads

[6] FCCPC and NDPC (n 1) p. 15.
[7] See *Alade v. Alic (Nig) Ltd & Anor* (2010) 19 NWLR (Pt. 1226); *Intercontinental Bank Ltd. v. Brifina Ltd.* (2012) 13 NWLR (Pt. 1316); *Noibi v. R. J Fikolati* (1987) 1 NWLR (Pt. 52).
[8] FCCPC and NDPC (n 1) p. 15.
[9] FCCPC and NDPC (n 2) p. 8; See also FCCPC and NDPC (n 1) p. 38.

'certain data collected by Meta Parties were indeed necessary for the efficient provision of the service for which 'consent' may be dispensed with'. The ambiguity of this statement raises questions about whether the reference to 'necessary' pertains to any of the legal bases outlined in article 2 b), c), d), and e) of the NDPR, all of which incorporate the concept of necessity. Additionally, this statement seems to imply that consent as a legal basis could legitimise a data processing operation even if the data processed is not necessary for the purpose of the processing, thereby making it excessive. This approach is problematic, as consent is just one of several legal bases provided in the NDPR. The principle of data minimisation, which requires that data collected be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed, applies universally to all data processing operations, regardless of the legal basis.

Lastly, the FCCPC's assertion that 'Meta Parties went beyond what is necessary for service delivery, and such data including device fingerprinting may be shared with third parties and commercialised',[10] suggests that device fingerprinting is one of the unnecessary metadata points, and its collection by WhatsApp constitutes excessive data collection. This assertion is problematic for two key reasons. First, 'device fingerprinting' is not listed in Annexure 1 of the investigation report, which lists the metadata points collected by WhatsApp. Second, and more importantly, from a technical perspective, device fingerprinting is not a type of data or metadata point. Rather, it is a technological method used to gather certain information—such as screen resolution, browser settings, or operating system specifics—about a mobile device or terminal equipment used by an individual to access the internet.[11]

Conclusion

In conclusion, the FCCPC's determination that WhatsApp engaged in excessive data collection practices under the NDPR raises significant questions about the adequacy and relevance of the metadata points processed by WhatsApp in Nigeria. The Commission's analysis, while highlighting disparities in the volume of data collected by WhatsApp compared to other instant messaging service like Signal and Telegram, fails to adequately consider the unique characteristics of each service and the distinct technical infrastructures underlying their data processing operations. Additionally, it does not comprehensively address the critical issue of whether these metadata points constitute personal data within the meaning of the NDPR. Furthermore, the FCCPC's reference to the concept of necessity, particularly in the context of consent, appears somewhat ambiguous and potentially inconsistent with the principle of data minimisation that underpins the governing principle of personal data processing being adequate under the NDPR.

The FCCPC's approach to enforcing data privacy laws through the lens of consumer protection is novel in Nigeria and could set a significant precedent. However, the lack of concrete evidence and detailed analysis in the Commission's findings may present substantive challenges during an appellate review. As the case is currently under review at the Competition and Consumer Protection Tribunal the outcome will no doubt be pivotal in determining the scope of the FCCPC's authority to enforce data privacy laws as a

[10] FCCPC and NDPC (n 1) p. 15.

[11] Chukwuyere Ebere Izuogu, 'Conducting Data Protection Impact Assessment for Online Profiling under the NDPR 2019' in Muhammed Tawfiq Ladan, Osatohanmwen Eruaga and Nkiruka Maduekwe (eds), *Digital Economy Law and Policy* (Nigerian Institute of Advanced Legal Studies, November 2022), p. 340.

form of consumer protection. The ramifications of this case could significantly influence the future enforcement of data privacy laws in Nigeria, particularly regarding the interpretation of the NDPR in the context of a consumer harm.

As we await the Tribunal's decision, it will be interesting to see how the arguments presented by both parties will shape the evolving interconnectedness between data protection and consumer protection in Nigeria. The outcome of this case could either reinforce the FCCPC's role in safeguarding consumer privacy or necessitate a recalibration of how data privacy laws may be enforced as a consumer protection law in Nigeria.

Contact person for this article
Chukwuyere Izuogu, LL.M (Hannover), CIPP/E
Partner
chukwuyere@sskohn.com