journals.unizik.edu.ng/jcpl/index ISSN: 2736-0342
NNAMDI AZIKIWE UNIVERSITY, AWKA
JOURNAL OF COMMERCIAL AND PROPERTY LAW

Gaps and Bridges between Data Protection and Competition Law in Nigeria

Ikechukwu Chime*
Chidiebere Okoroafo**

Abstract
Digitization has improved data collection and processing, making data an invaluable commodity. This development has granted significant market power to companies with substantial personal data and raised concerns about the concentration of market power in digital markets, as dominant data power outmuscles competitors. Concurrently, these companies depend on robust data protection frameworks to make the necessary investments for economic growth. At the same time, the security of personal data is protected under various data protection laws and frameworks. This paper explores the link between policy challenges related to data protection and competition law under Nigerian legislation. It posits that when the material scope of these legal frameworks overlaps, competition law can integrate data protection law as a normative tool when evaluating non-price competition. Data protection can, therefore, serve as an internal constraint on competition law. Furthermore, it suggests that following recent legal and institutional developments, data protection and other fundamental rights also impose an external constraint on competition law and, in certain situations, can influence or dictate its application. As national and supranational regulators confront the challenge of fostering a dynamic information economy that upholds fundamental rights, acknowledging these constraints would facilitate a more coherent approach to Nigerian law concerning the digital economy society.
Keywords*:* data, data protection, competition, NDPR, FCCPC

1. Introduction
In today's socio-economic landscape, data is paramount and referred to as 'the new oil.'[1] Data can be defined as "characters, symbols, and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals and stored in any format or any device".[2] As this data may be personal to identify or identifiable natural persons, it is essential to determine how the data is used and how it can be shared with third parties. Accordingly, data privacy, a facet of the right to privacy, entails the right of individuals to regulate how their personal information is accessed, used, and shared. It also encompasses the protection of this information from unauthorized third parties. This recognition of the fundamental right to privacy necessitates a corresponding need for data to be protected.

Data protection encompasses processes and strategies used to secure data availability, privacy, and probity. It involves safeguarding important information from corrupt practices, loss, or compromise.[3] The strategies include laws designed to protect personal data from exploitation and abuse. Data protection laws restrain and shape the activities of parties with the most access to personal data, including companies and governmental bodies.[4] Today, nearly every action taken by individuals involves the generation and sharing of some personal data, which could be captured, stored, and even sold by companies without their knowledge. This underscores the importance of adopting robust data protection practices and legislation to mitigate potential data risks of exploitation of such personal data.

***Ikechukwu Chime,** PhD, Faculty of Law, University of Nigeria, Enugu Campus, Email: ike.chime@unn.edu.ng, https://orcid.org/0009-1818-0410
****Chidiebere Okoroafo,** LLB, BL, Senior Associate, Lex Telios LLP, Email: chidiebere.okoroafo@yahoo.com
[1] The Economist, 'The World's Most Valuable Resource is not Oil but Data' (The Economist, 6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 24 December 2024.
[2]NITDA, Nigeria Data Protection Regulation 2019' <https://nitda.gov.ng/wp-content/uploads/2020/> accessed 13 October 2023, s 1.3(iv).
[3]OBLP, 'Data Protection and Privacy Challenges in Nigeria (Legal Issues)' (6 September 2023) <https://olumidebabalolalp .com/privacy-challenges-nigeria/> accessed 12 October 2024.
[4]Privacy International, 'A Guide for Policy Engagement on Data Protection' (Privacy International, 2018) <https://privacyinternational.org/report/2255/data-protection-guide> accessed 24 October 2024.

In addition, while the need to protect personal information exists, companies that process and utilize data also require legal protection to realize the value of their investments. These companies depend on adequate data protection frameworks to make the necessary investments in economic growth. At the same time, providing these companies with unbridled protection presents a challenge to fostering competitive economic markets.

Today's dynamic digital age presents regulators with a significant challenge in balancing data privacy and competition frameworks. How does Nigerian law balance the need for data protection and protecting data owners while ensuring competition? This paper examines the connection between data protection and competition law in Nigeria. It explores the national frameworks for data protection and outlines areas of intersection and differences with competition laws.

2. The Nigerian Data Protection Regime

Data protection and privacy regulations have gained support globally in the struggle to create prominent frameworks for supervising digital ecosystems.[5] Various jurisdictions have enacted necessary legal frameworks, regulations, and guidelines. Until recently, Nigeria had no dedicated and comprehensive legislation on data privacy and protection besides the Constitution of the Federal Republic of Nigeria, 1999 (as amended). However, the 1999 Constitution, the Nigeria Data Protection Regulation (NDPR) 2019,[6] and the recently enacted Nigeria Data Protection Act (NDPA) 2023 have provided more explicit frameworks for governing and strengthening data privacy and protection in Nigeria.

2.1 The Constitution of the Federal Republic of Nigeria, 1999 (as amended)

Section 37 of the Constitution of the Federal Republic of Nigeria provides that the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is guaranteed and protected. While the provision makes no specific mention of "data," it forms the bedrock of protection of data rights since information on homes, correspondences, and telephone conversations since the definition of data under the NDPR' includes characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device.[7] The Court of Appeal in *Nwali v Ebonyi State Independent Electoral Commission (EBSIEC)*[8] expansively interpreted the provision of section 37 to include all aspects of human life. The court held that the privacy of citizens is extensive as it extends to "his body, his life, his person, thought, conscience, belief, decisions (including his plans and choices), desires, health, his relationships, character, possessions, and family." It concluded that the provision protects the individual from coercive and unjustified intrusion. In this context, the court advocates a non-restrictive approach to the privacy rights the Constitution offers. Since data protection stems from information privacy, section 37 of the Constitution can rightly be seen as a source of data protection Nigeria.[9]

Subsequently, the Court of Appeal in *Emerging Market Telecommunication Services v Barr Godfrey Nya Eneye*[10] further held that the unsolicited messages received by the respondent as a result of access to his personal phone number, which was granted to unknown persons and companies by the appellant constituted a violation of the respondent's right to privacy guaranteed by section 37 of the Constitution, which includes the right to the privacy of a personal telephone line.

2.2 The Nigeria Data Protection Regulation 2019

The Nigeria Data Protection Regulation (NDPR/the Regulation) seeks to safeguard the rights of natural persons to data privacy, foster safe conduct for the exchange of personal data, prevent personal data manipulation, and ensure that Nigerian businesses remain competitive in international trade and align

[5] B Kira, V Sinha, and S Srinivasan, 'Regulating Digital Ecosystems: Bridging the Gap between Competition Policy and Data Protection' [2021] 30 *Industrial and Corporate Change,*1338.
[6] Para 1.3 (iv), NDPR
[7] OBLP (n 4).
[8] [2014] LPELR - 23682 (CA).
[9] O Babalola, 'Nigeria's Data Protection Legal and Institutional Model: An Overview' [2022] 12 (1) *International Data Privacy Law 44-52.*
[10] [2018] LPELR-46193.

with best practices.[11] The Regulation provides that anyone who is entrusted with or possesses the personal data of a data subject owes a duty of care to that data subject and is accountable for their acts and omissions regarding data processing in accordance with the governing principles.[12] In this context, the NDPR defines personal data as "any information relating to an identified or identifiable natural person such as a name, an identification number, location data, an online identifier, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person."[13] Thus, the specific purpose of the collection is made known to the data subject[14], who shall consent to the procurement without fraud, coercion, or undue influence.[15]

The NDPR further recognizes the privacy right of data subjects which is to be interpreted to advance and not to restrict their entitled safeguards under any data protection instrument enacted in furtherance of fundamental rights and Nigerian laws.[16] Sequel to this, individuals shall have, among other rights, the right to obtain and reuse their data for their purposes across different services (right to data portability).[17] The right to data portability allows data subjects, where technically feasible, to copy, move, or transfer their data from one controller to another safely and securely, without compromise to usability, and in conformity with constitutionally guaranteed principles of law for the general protection and enforcement of fundamental rights.[18]

Additionally, the Regulation stipulated that any medium through which personal data is being collected or processed shall display a simple, comprehensible, and conspicuous privacy policy that reflects what constitutes consent, a description of collectable personal data, the technical methods for collecting and storing the information, access (if any) of third parties to the data and purpose of access, remedies in the event of a violation of the privacy policy, and any limitation clause.[19] Equally, the data subjects are entitled to freely object to the processing of their data for marketing through the offered mechanism for objection[20] and may also request the deletion of their data.[21] While this encapsulates the right to be forgotten, a critical issue to consider in implementing the right to be forgotten is the cross-border nature of the internet. In the foreign case of *Google v CNIL*,[22] the Court of Justice of the European Union (CJEU) held that there was no obligation under the European Union (EU) law for Google to apply the European right to be forgotten globally. Thus, while EU residents have a right to be forgotten flowing from the General Data Protection Regulation (GDPR), its territorial limitation only applies to the EU states. The CJEU further held that the right to personal data protection is not absolute but must be considered in relation to societal function and be balanced against other fundamental rights. It is anticipated that the Nigerian Courts may lean towards the territorial limitation of this right on the basis of sovereignty.

2.3 The Nigeria Data Protection Act (NDPA) 2023

The Nigeria Data Protection Act (NDPA) was enacted in 2023 to protect the rights of data subjects and provide means of recourse and remedies in the event of the breach of the data subjects' rights, regulating the processing of personal data, safeguarding the fundamental rights, freedoms, and interests of data subjects, ensuring that data controllers fulfil their obligations to data subjects, strengthening the legal

[11]NDPR (n 2), section 1.1.
[12] s 1.3(xix).
[13]Ibid.
[14] The Regulation defines a "data subject" as any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
[15]Ibid, s 2.3.
[16]Ibid, s 2.9.
[17]Ibid, ss 3.1(14) & (15).
[18]Ibid s 3.1(16).
[19]Ibid s 2.5.
[20]Ibid s 2.8.
[21]Ibid s 3.1(9).
[22]curia.europa.eu <http://curia.europa.eu/juris/> accessed 13 October 2024.

foundations of the national digital economy, and guaranteeing Nigeria's participation in regional and global economies through beneficial and trusted use of personal data.[23]

The scope of application of the Act extends to the processing of personal data, whether by automated means or otherwise, by a data controller or data processor who is either domiciled in, resident in, or operates in Nigeria and processes personal data within Nigeria, or is not domiciled in, resident in, or operates in Nigeria but is processing the personal data of data subjects within Nigeria.[24] In essence, companies or entities incorporated and established under Nigerian law to carry on business in Nigeria, and those which, though not incorporated under Nigerian law or established in Nigeria, engaged in operations that involve the extensive utilization of personal data of Nigerian citizens and residents in their daily business, are all subject to the provisions of the NDPA.[25]

Furthermore, the Act established the Nigeria Data Protection Commission (NDPC) to regulate the deployment of technological and organizational measures for advancing personal data protection, fostering the development of standard personal data protection technologies, registering data controllers or processors of significant importance, receiving complaints relating to violations of the Act or subsidiary legislation made pursuant to the Act, etc.[26] As such, data subjects who are aggrieved by the action, omission, or decision of a data controller or data processor in violation of the Act or any subsidiary legislation made under the Act, may lodge a complaint with the NDPC who may investigate such non-frivolous complaint.[27] The NDPC may also, on its own accord, cause an investigation where it has reasons to believe that a data controller or data processor has violated or is likely to violate the provisions of the Act or any subsidiary legislation made pursuant to it[28] and if after the investigation is completed, the Commission is satisfied that there has been a violation, it may make any appropriate enforcement order or impose sanctions on the data controller or data processor.[29]

Worthy of note is the fact that the Act consolidates on the provisions of the NDPR with regard to the rights of data subjects, including the right to withdraw consent, the right to object to the processing of personal data, the right to not be subjected to a decision based solely on automated processing of personal data (including profiling) which produces legal or similar significant effects concerning the data subjects.[30] Equally, it recognized the right to data portability, which allows a data subject to receive, without undue delay from a data controller, personal data concerning the data subject, transmit the obtained personal data to another data controller without any hindrance, and have the personal data transmitted directly from one data controller to another, where technically feasible.[31]

While processing personal data, a data controller is mandated to adhere to the stipulated principles of ensuring that the data is processed in a fair, lawful, and transparent manner, collected for specified, explicit, and legitimate purposes, retained for no longer than is necessary to achieve lawful bases for its collection and further processing, accurate, up-to-date, and not misleading, and processed in a manner that ensures its appropriate security, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of a data breach.[32] A data controller is also required to implement appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of personal data in its possession or under its control, including protection against accidental or unlawful destruction, loss, misuse, alteration, unauthorised disclosure, or access.[33]

[23] NDPA, 2023, s 1.
[24] Ibid s 2.
[25] O Osundolire, T Bashir, and T Okorie, 'Nigeria Data Protection Act: What Individuals, Businesses and Organizations Should Know' (Banwo & Ighodalo, 22 June 2023) <https://www.banwo-ighodalo.com/grey-matter/nigeria-data-protection-act-what-individuals-businesses-and-organizations-should-know> accessed 13 October 2024.
[26] NDPA (n 23), ss 4 & 5.
[27] Ibid s 46.
[28] Ibid s 46(3).
[29] Ibid s 48(1)(a).
[30] Ibid ss 34 – 37.
[31] Ibid s 38(1 & 2).
[32] Ibid s 24.
[33] Ibid s 39.

Importantly, where a personal data breach occurs while such data is being stored or processed by a data processor, and such breach is likely to result in a high risk to the rights and freedoms of a data subject, the data controller shall, upon being notified of the breach by the data processor, immediately communicate the personal data breach to the data subject either privately or publicly (depending on which option is feasible) and provide advice on measures that could be taken to mitigate the potential adverse effects of the data breach effectively.[34]

Again, the Act in Section 41(1), prohibits the transfer of personal data from Nigeria to another country by a data controller or data processor unless the recipient of the personal data is subject to a law, binding corporate rules, code of conduct, contractual clauses, or certification mechanism that guarantees an adequate level of protection over the personal data, or the transfer is in line with the acceptable basis for processing of data under the Act. Sensitive personal data are also prohibited from being processed or permitted to be processed by a data controller or processor without the unwithdrawn consent of the data subject for the specific purpose(s) of the processing or where the processing is carried out in the course the controller's legitimate activities with appropriate safeguards; or is necessary to protect the vital interest of the data subjects or another person; or is necessary for performing the obligations of the data controller or exercising the rights of the data subject underemployment or social security laws or other similar laws, etc.[35]

As an improvement to the provisions of the NDPR, the Act equally made provisions for civil remedies by allowing a data subject who suffers injury, loss, or harm as a result of a data controller or processor's violation of the NDPA to recover damages from such data controller or data processor.[36] More so, the Court may, pursuant to Section 52 of the Act, make an order of forfeiture against a convicted individual, data controller, or data processor in accordance with the Proceeds of Crime (Recovery and Management) Act.

Given the requirement to give away data for almost all human operations, data-driven companies increasingly occupy an important role in the modern economy. As such data are collected from consumers to optimise business operations and make decisions from accurately predicted analysis, the application and use of consumers' data have become a source of concern.[37] The need to regulate situations where the market dominance of an undertaking is significantly based on personal data processing in the digital economy, has thus, necessitated privacy and data protection, as well as competition and consumer protection laws and policies which are increasingly overlapping on consumer data issues.[38]

3. Competition Law in Nigeria

The competition law in Nigeria is still at its early stage but it is gradually improving with the introduction of new guidelines and frameworks. The principal legislation that protects the rights of consumers and governs competition is the Federal Competition and Consumer Protection Act (FCCPA) of 2018.[39] It should be noted that the Nigerian competition law is modelled after South Africa's competition law, given its consideration as a model of competition law implementation in developing countries.[40] The Act serves as the unifying Statute for Nigeria's competition and consumer protection regulation, and prior to its enactment, the laws regulating competition and consumer protection were separate, fragmented, and industry-specific.[41] It seeks to promote and maintain competitive markets in the

[34]Ibid s 40(1 & 3).
[35]Ibid s 30(1).
[36]Ibid s 51.
[37] M Wasastjerna, 'The Facebook Case and Beyond: The Crossroads of Personal Data Protection and Competition Law' (2020) <https://www.youtube.com/watch?v=zOWigMVBWtg> accessed 26 September 2023.
[38] Directorate for Financial and Enterprise Affairs Competition Committee, Summary of Discussion of the Roundtable on Consumer Data Rights and Competition (DAF/COMP/M, 2021) 6.
[39]FCCPA 2018.
[40] E Uwadi, 'Challenges to the Implementation of Competition Law in Nigeria: Lessons from South Africa' (Antitrust Writing Awards, 2020) <https://awards.concurrences.com/en/>accessed 28 September 2023.
[41]A Idigbe, 'Overview of the Development of Competition Law in Nigeria' (Afronomics Law, 23 September 2019) <https://www.afronomicslaw.org/2019/09/23/overview>accessed 28 September 2024.

Nigerian economy, promote economic efficiency to contribute to the suitable development of the Nigerian economy, protect and promote the interests and welfare of consumers by providing them with a wide variety of quality products at competitive prices, and prohibit and restrict unfair business practices that prevent, restrict, or distort competition or constitute an abuse of a dominant position of market power in Nigeria.[42]

The FCCPA applies to all commercial activities within or having effect in Nigeria.[43] It also applies to all government departments, state-owned corporations, and all commercial activities aimed at making a profit.[44] The Act applies extraterritorially to any prohibited conduct by a Nigerian citizen or a person ordinarily resident in Nigeria, a corporate body registered in Nigeria or carrying out business within Nigeria, any person supplying or acquiring goods or services into or within Nigeria, and any person having shares or assets outside Nigeria which results in the change of control of the business, part of the business, or any asset of the business in Nigeria.[45]
Section 3 of the Act established the Federal Competition and Consumer Protection Commission (FCCPC), which shall carry out its functions and responsibilities in accordance with the powers vested upon it by the Act and declares the FCCPC supreme over other regulators in matters relating to competition regulation and consumer protection.[46]

Market Dominance and Competition in the Digital Age
Since the advent of the internet and the rapid technological improvement in all sectors, there has been an increasing fear of the concentration of the market on a few dominant firms. These firms have seen an increase in market power and capitalization, creating concern for the state of competition in the economy. For instance, Google exists as the most used search engine globally, and when you input a question into the search engine, it drives web traffic to the most popular websites. This web traffic allows those firms to benefit further from economies of scale and gives them access to consumer data, which is an emerging source of market power.[47]

Competition in the digital age remarkably differs from what was obtainable in the 'traditional market.'[48] Companies selling digital products and services generally have high fixed costs and low variable costs and also exhibit network effects. A product having network effects means that its value increases as more users join the network. The stronger the network effects in a market, the greater the degree of market concentration and power. As a result, digital markets can be highly concentrated, especially due to network effects, scale economies, and the need for large amounts of data to make them work. A large, installed base of users can also act as an entry barrier for prospective new entrants, even if a new entrant offers a better product.[49]

Determining whether a business has a dominant market position is different from determining if it is abusing that power or position. Significantly, holding a dominant market position or power is not contrary to anti-trust law as it forms a make-up of the free-market system where competition is guaranteed.[50] The abuse of the power is contrary anti-trust laws and prohibited. However, before determining if there's abuse, it is important to determine first if a dominant position exists, which the most challenging task between the two is.[51] Factors to consider in determining a dominant market

[42] FCCPA (n 58), s 1(a-e).
[43] Ibid s 2.
[44] Ibid.
[45] Ibid s 3.
[46]Ibid s 104

[48] In the traditional market, competition involved the presence of a large number of firms producing the same goods and competing against themselves for consumers but this practice is not the case in the digital economy.
[49]V Jain, 'Competition and Antitrust in The Digital Age' (Forbes, 5 October 2023) <https://www.forbes.com/sites/forbesbusinesscouncil/> accessed 28 September 2024.
[50]J Bestmann, 'Review of the Abuse of Dominance Regulations' (Mondaq, 8 March 2024) <https://www.mondaq.com/nigeria/antitrust-eu-competition/> accessed 25 August 2024.
[51] *Ibid.*

position include relevant market, market share and barriers to entry.[52] These are some of the major factors; some other factors are exit from a market, the financial strength of a company, and the number of competitors.

A key consideration in determining dominance even before the market share is establishing the specific market in which a business operates. In order to be able to analyze the relevant market, the following elements should be taken into account:

1. The product market: the set of goods and services that consumers generally consider to be interchangeable, the characteristics of these, and the prices and benefits that can be obtained from them.
2. The geographical market is the area in which the demand and supply of goods and services are distributed, with homogeneous conditions of competition, so that it can be separated from other areas where conditions are heterogeneous.

While determining market dominance is the most difficult task in determining abuse of dominant position, determining abuse is not without its difficulties. Abuse is grouped into two main groups in accordance with their economic effects, which are exploitative and exclusionary agreements.[53] Exploitative agreements has negative effects on consumers. Most of the abuses that take place are exclusionary abuses. Exploitative agreements aim to attack the interests of consumers, customers or suppliers. They are carried out by taking advantage of the company's superiority.[54] Examples of behaviour that could be included are excessive pricing, discrimination between customers without objective justification, and paying unreasonably low prices for supplies.

Additionally, the digital world moves at a rapid pace with new technologies churned out every day, reemphasizing the need for regulations on competition to be at par with these changes but the regulations guiding competition in the traditional market will not suffice. As posited by the EU Commission, recent competition and data policy-related reports indicate that monopolistic behaviour occurs majorly in very large online platforms that have become online market gatekeepers.[55]Accordingly, the three key characteristics of the digital economy are:

a. **Extreme Returns to Scale:** This entails that the cost of production is much less than proportional to the number of customers served, a phenomenon that is greatly advanced in the digital world. With increasing returns to scale, competition between two firms producing the same product will not allow them to cover their costs and consequently, no firm, unless equipped with much cheaper and superior technology, would consider penetrating a market dominated by an incumbent, notwithstanding the large amount of profits being made by such incumbent.[56]
b. **Network Externalities:** The increase in the number of users of a technology or service results in the increased usefulness of such technology or service. For instance, using social media platforms becomes more important when there are other users to communicate with; Airbnb (a unique network externality known as two-sidedness) connects owners of properties with renters and eBay buyers with sellers. Beyond connecting two different and well-identified groups of users, the benefit that one side derives from these two-sided platforms is dependent on the opposite participants: their number, but also on their identity.[57]
c. **Role of Data:** Technological evolution has enabled companies to collect, store, and use large amounts of data. This has and will continue to enable considerable changes to the way markets function. Furthermore, because data is sometimes accumulated as a by-product of the normal

[52]EligGürkayna, 'Definition of Dominant Position and the Board's Approach' (Mondaq, 13 May 2019) <https://www.mondaq.com/advicecentre/content/1666> accessed 25 August 2024.
[53]EmmiKuivalainen and H Mostyn and Patrick Bock, 'abuse of dominance in European Union' (Lexology, 21 March 2023) <https://www.lexology.com/library/detail.aspx?g=bf4763de-36a3-452d-b12c-ce86cab94de1> accessed 25 August 2024.
[54] Ibid.
[55] B Martens, 'An Economic Perspective on Data and Platform Market Power' (2020) JRC Digital Economy Working Paper 09/2020 <https://joint-research-centre.ec.europa.eu/system/files/2021-02/jrc122896.pdf> accessed 28 September 2023.
[56] Ibid, 20.
[57] Ibid, 21.

functioning of a platform, incumbents are better placed to have access to more recent data than other firms, availing them with a competitive advantage over others.

Clearly, the incidents of digital dominance can impede competition in favour of dominant firms. There is, therefore, an overwhelming need to check the potential abuse of market dominance in order to prioritize consumers' welfare, ensure the availability of good quality products and service options, promote technological innovation and market efficiency, ensure the absence of market power abuse, and guarantee market price competition for economic development.

Combating Abuse of Dominance in the Digital Age

A dominant position allows an undertaking to wield so much economic strength, enabling it to prevent effective competition and act independently of other factors in the relevant market.[58] This anti-competitive practice raises concern especially regarding the use of big data in this digital era, necessitating the need for a regulatory scope. Correspondingly, the FCCPA in regulating business conducts with an impact in Nigeria (including conduct by foreign entities), prohibits abuse of dominant position by one or more undertakings wielding such strength in the market.[59] It further empowered the Federal Competition and Consumer Protection Commission (FCCPC) to eliminate anti-competitive agreements, misleading, unfair, deceptive, or unconscionable marketing, trading, and business practices,[60] as well as agreements that restrain or are likely to restrain competition in any market.[61]

Again, the Act provides for imprisonment for a term not exceeding 3 years or a payment of a fine not exceeding N10, 000,000 or to both against a natural person, and a fine not exceeding 10% of the turnover in the preceding business year against a body corporate that conspires, combines, agrees, or arranges with another undertaking to unduly restrain or injure competition.[62] Accordingly, it subjects to a review, any proposed merger between one or more undertakings in order to determine whether the merger is likely to substantially prevent or lessen competition.[63] More so, where it appears that there are grounds for believing that a monopolistic situation may exist in any sector or across various sectors of the economy, the FCCPC is empowered to cause an investigation to be held into such sector(s) or into a particular type of agreement across various sectors in order to determine the extent of the situation in relation to the market.[64]

Although from the highlighted provisions, the FCCPA explicitly prohibits undertakings from leveraging their dominant positions to prevent effective market competition, its consideration or market definition are mainly in relation to the traditional market that focuses on the production or distribution of goods and services or any description, or the export of goods or services of any description from Nigeria. However, competition in the traditional market differs from the data-driven market competition in the digital economy. Nevertheless, big technology companies are enjoined to play fair and build consumer trust in the market by avoiding anti-competitive practices.

4. Competition Law AND Data Access

Digital transformation is changing our economies and societies as different technologies are increasingly becoming a part and parcel of daily living. This has been powered largely by the collection and use of increasing quantities of data. According to the European Commission, the volume of data generated globally is expected to grow from 33 zettabytes in 2018 to 175 zettabytes in 2025, reflecting the prevalent nature of data in the world.[65] Presently, a range of businesses rely on consumers' data collected

[58] FCCPA (n 58), s 70(1&2).
[59]Ibid, ss 71 – 73.
[60]Ibid, ss 2 & 17(g).
[61]Ibid, ss 59 – 63.
[62]Ibid, s 108(1)(d).
[63]Ibid ,ss 92 – 102.
[64]Ibid, s 76.
[65]A Barker, 'Consumer Data and Competition: A New Balancing Act for Online Markets?' (Going Digital Toolkit, 18 December 2020) <https://www.oecd-ilibrary.org/> accessed 30 September 2023.

as they use the Internet, digital applications (apps), and connected devices.[66] Thus, personal data has become an item for trade in the digital economy, with companies fighting for the right to own and process these data. Digitalization makes data an important part of the economy which companies seek to process, trade, and own because of its numerous benefits.

Equally, data protection and privacy regulations have gained support in the struggle to create prominent frameworks for the supervision of digital ecosystems. Against this backdrop, there is a need to create a balance between facilitating a wide and competitive use of data for innovative purposes and ensuring that businesses and other actors do not use data, especially personal data, in a manner that will cause harm to the consumers.[67]

4.1. Data Access in the Digital Economy

Data is at the core of the transition from the brick-and-mortar economy to a digital economy. It has been widely noted that data have become an important input for the production, distribution, marketing, and innovation processes in almost all sectors of the economy.[68] It has also become a key element for companies to compete in different areas of the economy, given its use in optimising business operations, making data-driven decisions, improving technologies, and enhancing productivity throughout the value chain.[69]

As data collection has grown in leaps and bounds, it means that data is increasingly important to competition assessments. This can manifest in two key ways: privacy and data protection might be an aspect of quality on which businesses may compete; and the collection and ownership of consumer data and access to that data, might impact competition.[70] In the digital economy, data is used to drive innovation and serves as a catalyst for growth in all sectors. Increasing the availability, use, and demand for data and data-enabled products can be achieved through the following means:

a. Government-to-business (G2B) data sharing: This entails opening up public sector information for business use supported by a regulatory framework.[71]
b. Business-to-Business (B2B) data sharing: To create an avenue for easy access to huge amounts of data as well as the necessary infrastructure for handling data.[72]
c. Business-to-Government (B2G) data sharing: To encourage voluntary data by establishing data access obligations to govern the public sector's re-use of privately-held data for public policy goals.[73]

In accessing data, there have been countless debates on the approach to be used by government organisations and businesses alike. These debates have divulged into two different frameworks that can be used to understand data access and competition in the digital economy. They are:

a. Private Control Framework: Where data remains under private control and access is granted on the basis of freely negotiated contracts.
b. Open Access Framework: Where data is regarded as a common good and access is guaranteed based on broad legal obligations.

This classification has raised concerns as to whether data should be regarded as a type of privately owned resource - this may result in the creation of a new type of intellectual property right in data, or whether it should be a new type of infrastructure in the evolving data economy.[74] Again, given the recognized

[66] Ibid, 5.
[67] Barker (n 89).
[68] Ibid.
[69] H Schweitzer and R Welker, 'A Legal Framework for Access to Data: A Competition Policy Perspective' in German Federal Ministry of Justice and Consumer Protection / Max Planck Institute for Innovation and Competition (eds), *Data Access, Consumer Interests and Public Welfare* (SSRN 2020) 103 – 153.
[70] Ibid.
[71] Ibid.
[72] Ibid.
[73] Ibid, 20.
[74] H Schweitzer and A Metzger, 'Data Access Under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?' [2023] 72 *GRUR International*, 337.

importance of data for economic growth, there have been concerns surrounding how the legal framework on data access can be adapted to these realities and ensure access to sufficient data by companies and organizations. Against this backdrop, there is a need to examine the relationship between competition law and laws protecting the access to and use of data in Nigeria.

4.2. Intersection between Competition Law and Data Access in Nigeria

While the importance of data is clear, adequate structure and guidelines on how it can be used, accessed, and protected are sacrosanct, raising the debatable subject of data protection and how it can regulate anti-competitive practices that harm privacy. While it is believed that the concept of "competition on privacy" can be used to point out anti-competitive behaviour since market power does not ensure adequate protection of the privacy of its consumers, some critics are not convinced that this concept can help identify anti-competitive behaviours if consumers do not mind giving away personal data for quality goods and services.[75] However, it has been noted and agreed that data protection can help provide competition law with the normative tools it lacks in this regard and can serve as a yardstick for accessing competition on data in all its ramifications i.e., quality and choice.

Particularly, the two ways in which data protection provides a normative yardstick for assessing exploitation in the context of personal data processing include:

i. The failure to honour rights granted by data protection law, or the infringement of dedicated data protection safeguards;[76]
ii. The issuance of an ultimatum to users which must be accepted in order to continue the usage of that online service. This may be considered exploitative in the same way that a sudden and unjustified increase in price has been considered abusive.[77]

As such, where data is processed in accordance with legal safeguards, they are more likely to improve competition in the market as opposed to deteriorating in the presence of market power.[78] On the other hand, a dominant business with access to a large amount of data can affect competition in the relevant market.[79] For instance, the *German Antitrust case*[80] was the first competition law decision that was reached by a competition authority in which the protection of privacy was explicitly taken into account. In this case, the German competition authorities opened an investigation into Facebook for a suspected infringement of data protection provisions as an abuse of dominant position. The investigation was based on the abuse of market power alleged against Facebook, whereby Facebook leveraged its terms of service to force users to give consent to the merging of personal data that it collects inside and outside of its social media platform.

These contractual terms and conditions were only accepted by its users as a result of its market power, notwithstanding that these terms violated data protection rules. In 2019, the ruling authority affirmed the position of the competition authorities and held that Facebook had abused its dominant position as a social network in Germany by imposing exploitative business terms on its users and was thus, prohibited from making the collection of user data and combining or giving away such data to third parties as a condition precedent to the use of its social network. The authority further imposed an obligation on Facebook as to the method of data collection it employs and required it to prevent the integration of user data from third-party applications into a Facebook account without explicit consent by the user.

Competition law and data protection law are two fields that seek to protect individuals and their choices, though the nature of harm they seek to address can be distinguished - competition law aims to avoid economic harm on the parameters of price, quality, choice, and innovation which affect efficiency or consumer welfare while data protection law seeks to avert harm to an individual's fundamental right to

[75] A Kuenzler, 'What Competition Can Do for Data Privacy (and Vice Versa)' [2022] 47 *Computer Law & Security Review.*
[76] Ibid, 9.
[77] Ibid.
[78] Ibid.
[79] Wasastjerna (n 37).
[80] [2019] B6-22/16 *Bundeskartellamt.*

privacy in addition to its strive to prevent economic harm.[81] Although data protection and competition law originate from different social concerns and specific legal tenets and methodologies, the emergence of digital markets and the role played by data in driving the business models of technology firms have closely brought these two fields together.[82] On the one hand, there are concerns that the growing market power of digital platforms that collect and process large amounts of data could impede individuals' fundamental right to privacy. Conversely, data is seen as an important source of market power and this has caused a change to traditional market competition and revenue models.

Furthermore, data protection law is a framework designed to identify and achieve an optimal level of personal data protection and provide guidance that competition law lacks in relation to non-price competitive parameters.[83] An instance of this can be when an infringement of competition laws occurs, indicating potential consumer exploitation or anti-competitive practices, the use of data protection law can provide the normative backdrop for competitive activity.[84] Thus, although data protection law safeguards the integrity of individual decision-making regarding personal data processing while competition law protects consumers against unlawful exercises of market power, nevertheless, both laws seek to advance the welfare of the individual at different ends of the same spectrum.[85]

Nevertheless, there is an overwhelming need for a regulatory instrument that provides clarity on how conducts within the digital markets will be assessed by competition regulators, and how entry barriers to access to data will be addressed. With this in mind, the FCCPC is currently developing guidelines for market definitions which will include a section on "Zero Price and Digital Platforms."[86] This will be instrumental in providing clarity on the roles of players in the digital market i.e. acknowledging that users are the producers in the digital platforms, the platforms play the role of distributors, and advertisers play the role of consumers.

Again, it will enhance consideration of digital platforms as multi-sided markets with network effects while facilitating a modified definition of digital markets either as a small but significant non-transitory change in quality (SSNIQ) or a small but significant non-transitory change in cost (SSNIC), although the cost in this sense is not mandatory.[87] The Nigerian Data Protection Regulation (NDPR)[88] is also charting the way towards entrenching the recognition of users as producers in the digital market by providing in its Section 3.1(14 & 15) that data users/subjects own their data and data sets gathered and utilized by big digital platforms can be made available to other platforms if the users choose to transmit them.

Clearly, access to data has the potential to level the digital market field in many ways. Hence, a competition law or regulation that thrives on the twin concepts of data portability and democratization will certainly aid in achieving open and accessible digital markets while advancing economic development.

5. Case Analysis: FCCPC v META

The FCCPC issued a press release on 19 July, 2024, announcing the findings of its investigation into Meta Platforms Inc and WhatsApp LLC for alleged violations of the FCCPA, the NDPR, and other applicable laws. Meta had modified its privacy policy in January 2021 allowing certain information (such as contact details and message content) to be shared with Facebook and potentially used for advertising purposes. Individuals who did not want to share this data were given the option of deleting

[81] F Costa-Cabral and O Lynskey, 'Family Ties: The Intersection between Data Protection and Competition in EU Law' [2017] 54 (1) *Common Market Law Review* 11 – 50.
[82] Ibid, 3.
[83] Ibid.
[84] Ibid.
[85] Ibid.
[86] FCCPC, 'Competition Law, Policy and Regulation in the Digital Era' (UNCTAD, 8 July 2021) 6 <https://unctad.org/system/files/non-official-document/ccpb_IGECOMP2021_Nigeria_Irukera_en.pdf>accessed 12 January 2025.
[87] Ibid.
[88]NDPR (n 2).

their accounts, however, individuals who gave their consent were not given the ability to later revoke their approval.[89]

Meta clarified that the data intended to be collected and shared was for interactions with business accounts, not private messages between friends and family. Despite this statement, privacy worries about Meta lingered. The FCCPC and the Nigerian Data Protection Commission ("NDPC") launched a joint investigation into potential violations of Nigeria's data privacy and competition laws as a result of the privacy policy amendment. On July 12, 2024, the FCCPC assessed a fine of US$220,000,000 (Two Hundred and Twenty Million United States Dollars) on Meta based on the joint report for allegedly breaking the Nigeria Data Protection Regulation, 2019 (the "NDPR").[90]

According to the joint report, Meta has repeatedly violated the FCCPA and the NDPR, including abusive and invasive practices against Nigerian data subjects, such as appropriating personal data without consent and discriminatory practices against Nigerian data. The investigation also found Meta in violation of the FCCPA for abusing its dominating market position.

The Commission found that Meta parties repeatedly violated the FCCPA and NDPR, including abusive and discriminatory practices and abuse of dominant market position against Nigerian data subjects and consumers by:

a. Denying Nigerian data subjects the right to self-determine;
b. Unauthorized transfer and sharing of Nigerian data-subjects personal data;
c. Discrimination and disparate treatment; and
d. Tying and bundling.

The Commission directed the Meta Parties to take steps and actions to comply with current law (the NDPA), to stop exploitation of Nigerian consumers, to stop market abuse, and to refrain from future and similar conducts or practices that do not meet nationally applicable standards and undermine consumer rights. Second, the final ruling assessed a monetary penalty of $220,000,000 (two hundred and twenty million dollars) in accordance with the Federal Competition and Consumer Protection (Administrative Penalties) Regulations 2020.

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 section 17(a) regarding enforcing other enactments on competition and consumer protection?

According to the FCCPC's investigation, WhatsApp gathers 44 metadata points, while Signal and Telegram collect only 4 each. Based on this comparison, the FCCPC questioned the need for such substantial data collecting when delivering WhatsApp-related services to Nigerian users. While the FCCPC's allegation about WhatsApp's (meta) data collection techniques may be correct, it is critical to first show that each of these metadata points represents personal data before applying the NDPR. Article 1.3.xix of the NDPR defines personal data as 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.

[89]TemitayoJaiyeola, 'Timeline of Nigeria's Meta $220 million case' (Business Day, 23 July 2024) <https://businessday.ng/technology/article/timeline-of-nigerias-meta-220-million-case/> accessed 22 January 2025.
[90] Ibid.

Although these metadata points were provided in Annexure 1 of the investigative report, it is unlikely that all of them could be used to directly or indirectly identify a natural person, and so fall under the definition of personal data in the NDPR. An individual is identified when he can be 'distinguished' or 'singled out' from among a group of people, and identifiable when, 'while the person has not been recognized yet, it is conceivable to do'. If the FCCPC can demonstrate that these metadata points qualify as personal data, then the FCCPC's argument about collecting such data, particularly in relation to services such as Telegram and Signal, may be valid.

6. Conclusion

Data plays an important role in business activities and ensures the existence of effective competition in relevant markets. Large multi-sided online platforms serve as gatekeepers to data and have been identified as having collected vast volumes of highly valuable consumer data, which makes it difficult for smaller companies and new market entrants to compete with them since they control the clouds of their respective ecosystems. Yet, ensuring that quality products and services are available to consumers still requires healthy competition and innovation. It is, therefore, optimal for competition authorities to take a holistic approach to regulating the digital market through the instrumentality of modified competition laws or regulations, as what may be beneficial for digital market controllers or operators may not always be in the overall interest of that market. Achieve a levelled playing field for all, running a seamless enforcement ecosystem for administrative sanctions and compensatory redress for victims, and creating a balance between data access, data protection, and market protection will, thus, involve the regulators' effective management of market conduct by the numerous sectors that converge in the digital market. Impressively, the FCCPC is already looking in that direction while the NDPR already lays the relevant foundation for this to become operationalized in Nigeria, given the potential benefits to both competition regulation and consumer protection in digital markets.