Scientific Research Publishing

Beijing Law Review, 2025, 16(1), 1-28
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Unresolved Tensions in the Intersections of Corporate Insolvency, Data Protection and Conflict of Laws Under the Nigerian Legal Framework

Joseph Agburuwhuo Nwobike

Commercial Law Division at Osborne Law Practice, Lagos, Abuja & Port Harcourt, Nigeria
Email: joseph.nwobike@osbornelawpractice.com

How to cite this paper: Nwobike, J. A. (2025). Unresolved Tensions in the Intersections of Corporate Insolvency, Data Protection and Conflict of Laws Under the Nigerian Legal Framework. *Beijing Law Review, 16,* 1-28.
https://doi.org/10.4236/blr.2025.161001

Received: December 9, 2024
Accepted: January 12, 2025
Published: January 15, 2025

Abstract

Insolvent corporate debtors often possess a considerable amount of personal data, such as customer lists and user data. The insolvency and liquidation of biobanks and private hospitals even pose greater challenges in relation to the sensitive personal data in their holding. In liquidation, should the sensitive personal data in their holding be sold alongside other assets to satisfy the corporate debtor's debts? This question (or its kind) is yet to receive any judicial interpretation in Nigeria. Similarly, insolvency practitioners (e.g. administrators and liquidators) are typically appointed to manage and distribute an insolvent corporate debtor's assets to its stakeholders. An administrator's use of personal data to trade may qualify him as a data controller under the Nigerian Data Protection Act 2023 (NDPA). Likewise, where personal data are necessary for trading under administration, the cost of processing information requests from data subjects may impede the success of the administration. Although NDPA indicates that a data subject will bear the cost of processing if the underlying cost is "unreasonable", neither case law nor subsidiary legislations have clarified the quantum of cost as well as the circumstances that could meet the "unreasonable" threshold. The article finds that NDPA intersects with other business laws in Nigeria, and their intersections breed a considerable amount of uncertainty that is likely to impede commerce: the article proposes urgent reforms on these pertinent issues.

Keywords

NDPA, Data Protection, Corporate Insolvency, Personal Data, Conflict of Laws, Data Controllers, Southern Pacific, Liquidation

1. Introduction

The ubiquity of the Internet has necessitated the ease of human connectivity in the 21st century (Goldsmith & Wu, 2006). This inevitably entails the sharing and distribution of personal data in high volumes, thereby increasing the chances of personal data breaches (Clarke et al., 2001; Choi et al., 2018; Reidenberg, 2001). Recognizing this challenge, many legal systems have recently revamped their data protection regimes by enacting laws that are responsive to the heightened degree of threats (Colonna, 2022). For example, the European Union's GDPR—General Data Protection Regulation, among other rights for data subjects, provides for the right of erasure under its article 17: this is also known as the *right to be forgotten* (Carnegy-Arbuthnott, 2023). Since the last two decades, Nigeria has made considerable efforts to respond to the Internet cum personal data problem, by enacting legislations that aim to tackle the challenge (Omotubora & Basu, 2020; Abdulrauf & Fombad, 2016; Iwobi, 2017; Orji, 2017). Specifically, on personal data protection, the initial legislative response was via a regulation—Nigerian Data Protection Regulation (NDPR).[1]

Unlike in the EU, a "regulation" in Nigeria is a secondary legislation, and is of course subservient to primary laws, such as statutes or decisions of superior courts of record. Thus, during the regime of the NDPR, its binding force sat uneasily on the *ultra vires* doctrine, and could not have been able to successfully thwart settled rights or practices on personal data, which derived from an operative statute or case law. In June 2023, however, the Nigerian Data Protection Act (NDPA) was enacted as a comprehensive statute that applies across all sectors in Nigeria.[2] In large part, the NDPA resembles the European GDPR, satisfying most of the contemporary notions of data protection and privacy rights.[3]

Arguably, however, NDPA has some major defects which would likely threaten its effectiveness in both the short and long runs. The defects stem from NDPA's lack of harmonization with other relevant statutes that govern business transactions in Nigeria. In lieu of effective harmonization, NDPA resorts to a *non obstante* solution, stating that "where the provisions of any other law or enactment, in so far as they provide or relate directly or indirectly to the processing of personal data, are inconsistent with any of the provisions of this Act, the provisions of this Act shall prevail."[4] Arguably, this approach does not automatically cure or reconcile the following four inconsistencies (or defects) that exist in the intersections between NDPA and other areas of law, such as corporate insolvency, secured transactions and conflict of laws.

In relation to the defects, firstly, the Nigerian Secured Transactions in Movable Assets Act 2017 (STMA) recognizes both tangible and intangible assets as capable

[1]NDPR was a subsidiary legislation based on National Information Technology Development Agency (NITDA) Act 2007.
[2]Section 63 NDPA.
[3]See Part VI NDPA, entitled "Rights of a Data Subject".
[4]Section 63 NDPA.

of being used as collateral to secure debt transactions.[5] Personal data is an intangible asset—an example of which is a voluntarily obtained "list of customers". This type of asset, when systematically organized, is able to aid business activities for the main purpose of increasing productivity and profit margins. Both case law and entrenched business practices show that "list of customers" can be an integral part of a business's asset worth.[6] Secondly, the Nigerian Companies and Allied Matters Act 2020 (CAMA) recognizes the use of "floating charge" as a security device.[7] This device could be used to encumber the present and future assets of a corporate debtor until its crystallization, which converts it to a fixed charge.[8] Thus, if a floating charge encumbers all of a debtor's assets, including its "list of customers", the charge holder, may, towards satisfying his debts, dispose the personal data according to his rights under CAMA, which might infringe on protected rights under NDPA.

Thirdly, as was also advanced by Bruynseels and Hoven (2015), another CAMA-related challenge presents in the context of administration or liquidation of a corporate debtor, especially if the corporate debtors are private biobanks or hospitals that hold a considerable amount of (sensitive) personal data. Based on section 452 CAMA 2020, if an administrator is appointed to takeover a corporate debtor, he is statutorily empowered to oust the latter's directors from management (Payne, 2018). Subject to how Nigerian courts will interpret this issue in the near future, it is possible, indeed likely that a duly appointed administrator will be regarded as a data controller,[9] and thus, may become personally liable if his activities infringe on the rights of the corporate debtor's data subjects. Apart from the case law guide by the UK and US courts (discussed here), there is no statutory or judicial guide in Nigeria for the unavoidable relationship between insolvency practitioners (e.g. administrators and liquidators) dealing with personal data in an insolvency procedure and data subjects whose rights to request data information involve costs that may deeply erode their corporate debtor's assets and threaten the success of its administration procedure.[10]

Fourthly, the Nigerian conflict of laws regime favors freedom of contract and

[5]Section 63 STMA (see the definition of "collateral").

[6]See the cases discussed in parts 2 and 3 below.

[7]Sections 203 of the Nigerian Companies and Allied Matters Act 2020 ("CAMA 2020"); *Agnew v. Commissioner of Inland Revenue* [2001] 2 AC 710; *Re Spectrum Plus Ltd* [2005] UKHL 41.

[8]Section 203(1)(a) CAMA 2020 defines "floating charge" to "[m]ean an equitable charge over the whole or a specified part of the company's undertakings and assets, including cash and uncalled capital of the company both present and future, but so that the charge shall not preclude the company from dealing with such assets until—(a) the security becomes enforceable and the holder thereof, pursuant to a power in that behalf in the debenture or the deed securing the same, appoints a receiver or manager or enters into possession of such assets". As was also stated in *Buchler v Talbot* [2004] 2 AC 298, 309 (when "a floating charge crystallizes it becomes a fixed charge attaching to the assets of the company which fall within its terms.").

[9]This is based on the Information Commissioner's argument in the *Southern Pacific* case, discussed in detail in part 3 below.

[10]See section 34(d) NDPA. NDPA's meaning of "unreasonable cost" has not yet been judicially or administratively provided in Nigeria. Moreover, its meaning may depend on the circumstances of each case.

party autonomy—contractual parties are free to choose the law that governs their contractual transactions and dispute resolution. Both case law and statutes seem to favor this approach.[11] Thus, Nigeria's conflict of laws approach seems to be inconsistent with the objectives of NPDA.[12] For example, NDPA does not compel data controllers to always host the personal data of Nigerian data subjects in Nigeria.[13] In other words, the stronger contracting party in Nigeria may completely bypass the Nigerian courts and the Data Protection Commission through an exclusive foreign jurisdiction clause that appoints a foreign court and forum to resolve any contractual disputes wherein data breaches might be implicated. In that case, if Nigerian courts, in deference to freedom of contract and exclusive foreign jurisdiction clauses, grant stays of proceedings, impecunious contracting parties in Nigeria may be indirectly denied justice and the protections of NDPA due to the high costs of accessing the foreign forums nominated in their contracts. This article's central question is therefore this: in what ways does NDPA conflict with other business laws in Nigeria, and are these conflicts inimical to economic development? In answering this primary question, the article employs the doctrinal method, critiquing and analyzing relevant statutes and case law that shed light on the thematic elements of the discourse.

In its remainder, this article proceeds as follows. Part 2 maps the connections between secured transactions, corporate insolvency and data protection. Part 3 provides an overview of NDPA as well as a detailed discourse on its intersections and conflicts with other relevant business laws in Nigeria. Part 4 discusses the Nigerian approach to conflict of laws and how the dominant perspective, which is rooted in freedom of contract and party autonomy may create an unintended bypass of Nigerian courts. Ultimately, this will deny justice to impecunious Nigerian data subjects who are unable to afford the high costs of accessing foreign forums for dispute resolutions based on personal data breaches. It argues for a Nigerian mandatory rule (as obtainable in admiralty contracts) for all commercial contracts whose performance is in Nigeria. Part 5 is the conclusion.

2. Mapping the Linkages between Secured Transactions, Corporate Insolvency and Personal Data Protection

Modern legal systems personify corporations as human beings, enabling them to sue and be sued (Pollman, 2021). In that analogical sense, a corporate life could be ended voluntarily by its shareholders (Ripken, 2019); involuntarily by its creditors for failure to repay due debts;[14] or by an overpowering event, such as a financial crisis (Financial Crisis Inquiry Commission, 2011). The Great Recession of 2008-2009, for example, caused the insolvency and liquidation of many corporations (Skeel, 2021). The ubiquity of corporate liquidations in the aftermath of the

[11]For example, see section 52 STMA and the Nigerian Supreme Court decision in *Nika Fishing Company Ltd v Lavina Corporation* (2008) 16 NWLR 509.

[12]See section 1 NDPA.

[13]See section 43 NDPA.

[14]Sections 572-573 CAMA 2020.

crisis, inflicted ineffable hardships on corporate stakeholders.[15] More recently, the COVID-19 pandemic, which initially seemed like a health crisis, eventually morphed into an economic crisis (International Monetary Fund, 2020). Although lockdowns helped to contain the spread of the disease, it restricted the movement of people and goods (Onyeaka et al., 2021). Nigerian companies whose financial wellbeing depended on people's free movement, lost significant revenues that ultimately caused insolvency and liquidation.

Although the pandemic has been declared over by the World Health Organization, (United Nations, 2023) the negative effects on businesses continue to reverberate in the Nigerian business sector, and many corporate businesses are still under the imminent risk of insolvency and liquidation. Corporate liquidation primarily entails the selling of a corporate debtor's assets to satisfy the debts of its creditors and other stakeholders (Ben-Ishai & Lubben, 2012). These assets may include all kinds, including intangible assets such as personal data (Schwartz, 2004). And disposal of personal data implicates data protection law as was exemplified by the consumer protection concerns in the *Toysmart* case.[16]

Irrespective of the pandemic-triggered economic crisis, the 2020 amendment of the CAMA 1990 surprisingly overlooked the critical issues that deserved urgent reforms (Iheme & Mba, 2021). Although CAMA 2020 claims to be based on the philosophy of debtor-friendliness, some of its provisions still reflect its enduring kinship with creditor-friendliness (Ibid, 318). An example is its retention of floating charge in spite of its problematic history that culminated into corporate abuses. Before CAMA 1990 reform, floating charge holders usually appointed receiver-managers to takeover businesses and manage them in ways that did not benefit all of the corporate debtor's stakeholders (Ibid, 316).

Apart from CAMA 2020, there are other Nigerian legislations that unintendedly pose material risks for small businesses. An example is the STMA—Secured Transactions in Movable Assets Act 2017 (Nwobike, 2023). Although STMA was enacted to provide an increased access to credit for individuals and small businesses, some of its provisions arguably defeat this ultimate purpose.[17] Both legislations (CAMA 2020 and STMA) seem to also possess philosophical conflicts that could diminish the success of corporate businesses in Nigeria. Drawing insights from Ngo (2002), one of such conflicts relates to the existence of the CAMA-floating charge[18] and the STMA-floating lien.[19] The effect of the former's postponement of attachment until crystallization, and the latter's nature of being a combination of fixed and floating charges ought to be a subject-matter of interest to Nigerian law reformers (Esangbedo, 2020). Indeed, the internal conflicts within

[15]Business bankruptcy filings went from 28,322 in 2007 to 60,837 in 2009. The statistics can be accessed at Annual Business and Non-Business Filings by Year, 1980-2020, American Bankruptcy Institute (2020): https://abi-org.s3.amazonaws.com/Newsroom/Bankruptcy_Statistics/Total-Business-Consumer1980-Present.pdf, accessed 20 July 2024.

[16]*In re Toysmart.com Inc. LLC*, No. 00-13995 (Bankr. D. Mass., August 2000).

[17]E.g., sections 2(3) and section 52 STMA.

[18]Sections 207(4) and 577 CAMA 2020.

[19]Section 6(1)(b) STMA.

CAMA 2020 on the one hand, and the conflicts between CAMA 2020 and STMA on the other hand, are some of the statutory conflicts that deserve reconciliation.[20]

As earlier stated, corporate liquidation relates to how an insolvent corporate debtor's assets are distributed among its stakeholders based on their statutory hierarchies.[21] The assets for distribution would typically cut across the various types of assets.[22] Corporate assets are broadly categorized as "tangible" and "intangible" assets. The STMA recognizes both types of assets as acceptable collateral for securing debts.[23] Incontrovertibly, *personal data,*[24] as defined by the Nigerian Data Protection Act 2023 (NDPA) can form part of the corporate assets being used as collateral to secure debt obligations. The *Toysmart* case also shows that in modern business practices, personal data can be sold to third parties for profit. In *Toysmart,* the corporate debtor violated section 5 of the US Federal Trade Commission Act "by misrepresenting to consumers that personal information would *never* be shared with third parties and then disclosing, selling, or offering that information for sale in violation of the company's own privacy statement" (Federal Trade Commission, 2000).

A further example of how corporate activities infringe on personal data relates to social media corporations such as Facebook, Google, LinkedIn, etc. In 2019, *Green v SCL Group Ltd and others,*[25] involved a litigation surrounding the 2018 Facebook-Cambridge Analytica (UK) scandal. Thus, based on the business models of social media corporations as well as the relevant case law, it can be concluded that personal data are valuable assets and increasingly being purchased from multiple vendors for processing and eventual use for "[t]argeted advertising and messaging for clients".[26] Similarly, as illustrated by *Douez v Facebook*,[27] Facebook's overreaches on personal data occurred through "Sponsored Stories",[28] "[w]hich used the name and picture of Facebook members to advertise companies and products to other members for the purpose of targeted advertising".[29]

Under the Nigerian legal framework, there are arguably unsettled perspectives about personal data and the possibility of its use as business collateral. Similarly, its interface with corporate insolvency has not been clearly charted based on the following observations. Firstly, the (im)possibility that personal data is an asset that can be collateralized may still require specific textual evidence in the STMA,

[20]Ibid.

[21]Section 657 CAMA 2020.

[22]These include both movable and immovable assets. In relation to use of assets to secure debts, while the latter (immovable assets) are governed by the federal Conveyancing Act 1881 and other state legislations, the former (movable assets) are governed by the federal STMA.

[23]Section 63 STMA—"collateral means movable property, whether tangible or intangible that is subject of a security interest."

[24]Section 65 NDPA.

[25]*[2019] EWHC 954 (Ch).* Available at <https://www.judiciary.uk/wp-content/uploads/2019/04/17.04.19-cambridge-judgment.pdf>

[26]Ibid, para 1.

[27]*Douez v Facebook* [2017] SCC 33. Available at <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/16700/index.do>

[28]Ibid, para 6.

[29]Ibid, para 7.

NDPA, as well as the Constitution. So far, this is unclear. Secondly, NDPA requires that irrespective of a data subject's consent to process their personal data, processing such data must not violate their data privacy as guaranteed by the Nigerian Constitution. Section 37 of the Nigerian Constitution only provides that "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected".[30]

Inspired by Bygrave (2014a, 2014b), the textual value of section 37 has aged considerably in the era of Internet and Social Media. A literal statutory interpretation does not allow for any expansion of statutory texts in order to infuse purpose. Based on a literal interpretation, which the Nigerian Supreme Court tends to use for constitutional interpretation,[31] section 37 of the Nigerian Constitution does not sufficiently cover the contemporary means by which data privacy can be breached. Similarly, there is little or no apex case law around section 37 in the last six decades as to provide a comprehensive guide on data privacy and breaches. This lacuna is understandable considering that after Nigeria's independence in 1960, the country was under military dictatorships for a cumulative period of 29 years (Kennedy, 2004). As can be seen in the cases decided during the military rule era, individual privacy, rule of law and military dictatorial rule are self-evidently oxymoron.[32] Additionally, due to judicial slowness in Nigeria, it takes an average case a period of fifteen years or more to move from the court of first instance to the Nigerian Court of Appeals or Supreme Court.[33] Based on procedural rules of court, the Nigerian Supreme Court (unlike its US counterpart that is selective of the cases it takes on appeal) entertains (almost) every appeal including on legal issues that have been previously settled by it (Essen, 2000).

Thus, even though it is nearly three decades since Nigeria embraced democracy and adopted the 1999 Constitution, the case law on data privacy has not sufficiently developed to provide a comprehensive guide on the use of personal data in modern business practices. For example, the extent to which NDPA's provisions affect collateralized personal data as well as creditors' rights in insolvency is still unclear, especially in the insolvency of private hospitals and biobanks that hold large amounts of sensitive data. In other words, in view of sections 586 - 588 (liquidators) and section 504 - 505 (administrators) of CAMA 2020, which

[30]Section 37, CFRN 1999 (as amended).

[31]*Ifezue v. Mbadugha* [1984] 1 SCNLR 427, *Chief Obafemi Awolowo v. AlhajiShehu Shagari Ors.* (1979 6-9 S.C. 51, *Global Excellence Comm. Ltd v Duke* [2007] 16 NWLR (pt. 1059) 43-44, *Amaechi v INEC* (2008) 5 NWLR (Pt. 1080) 227, *Okumagba v. Egbe* [1965] 1 All NLR 62, *A.G. of Ondo State v. A.G. of the Federation* [1983] 2 SCNLR 269, etc.

[32]See *Ojokwu v Military Governor of Lagos State* (1986) All NLR 233; *Awojugbagbe Light Industries v Chinukwe* (1995) 4 NWLR (pt. 390) 379 (where the appointed receiver used security dogs to takeover possession of the debtor's premises).

[33]A few case law examples are: *Union Bank Nigeria Plc v Ayodara Sons (Nig) limited* (2007) 13 NWLR (pt 1052) 567, instituted in 1989 at court of first instance, but was decided by Supreme Court in 2007 (18 years); *Adisa v Oyinwola* (2000) 10 NWLR (pt 674) 116 was worse because the case's journey between the Court of Appeal and Supreme Court took a period of 15 years; *Bank of the North v* Muri [1998] 2 NWLR (pt 536) 153 (10 years from High Court to the Court of Appeals); Ojikutu *v Agbonmagbe Bank Ltd* (now known as Wema Bank Plc) [1996] 2 Afr LR (comm) 433 (11 years).

respectively vest the assets of a corporate debtor on its appointed liquidators/administrators, will the latter be responsible for personal data breaches prior to (and during) their appointment? Although these questions have received sufficient answers in the UK based on the decision in *Southern Pacific,*[34] they are yet to obtain any judicial response in Nigeria, understandably due to the nascence of NDPA.

Thirdly, the Nigerian CAMA-floating charge is capable of being used as security against all of a corporate debtor's assets including its intangible rights in personal data. A specific guide is thus necessary on how to liquidate collateralized personal data without breaching the privacy rights of the data subjects. As the facts of *Southern Pacific* show, the disposal of personal data in the context of liquidation may be practically exigent in order to prevent a significant erosion of the corporate assets earmarked for distribution to stakeholders.[35] In crafting a Nigerian idiosyncratic approach towards personal data and its treatment in insolvency, Nigerian lawmakers may study the experiences of the US and European Union where court cases on data protections are considerably sufficient to provide guidance. The US and the EU also seem to have differing perspectives on how personal data should be managed (Charlesworth, 2000; Schwartz, 2013). Commenting on the differing philosophical perceptions about personal data, Whitman (2004) argued that while the US "[a]nxieties and ideals focus principally on the police and other officials, and around the ambition 'to secure the blessings of liberty,' ... in the European Union, they focus on the ambition to guarantee everyone's position in society, to guarantee everyone's 'honor'" (ibid, pp. 1152-1221). As would be seen in the next part, NDPA intersects with other business laws in Nigeria and the intersections breed legal tensions that are yet to be resolved.

3. Nigerian Data Protection Legal Framework and Its Intersections with Other Nigerian Business Laws

3.1. Terminological Differences: EU, US and Nigeria in Perspective

In June 2023, the Nigerian Data Protection Act (NDPA) was enacted. The term "data protection" follows the European terminology under the GDPR, where it was mentioned 144 times.[36] As Bygrave (2014a) stated, in the US however, "data privacy" is the functional equivalent of the GDPR's data protection terminology (Ibid, 1). NDPA uses both terminologies, with "data privacy" referring specifically to the fundamental right of privacy as stipulated by section 37 of Constitution of Federal Republic of Nigeria (CFRN), as well as article 12 of Universal Declaration of Human Rights.[37] Before the enactment of NDPA, Nigeria only had a patchwork

[34] *Re Southern Pacific Personal Loans Ltd* [2013] EWHC 2485 (Ch). See part 3.7 below for the facts and analysis.

[35] Ibid, para 41.

[36] GDPR is freely downloadable at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

[37] Article 12 UDHR states that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence .... Everyone has the right to the protection of the law against such interference or attacks."

of data privacy laws, ranging from section 37 CFRN, relevant treaties, to legislations such as the Cybercrimes (Prohibition, Prevention, etc.) Act 2015,[38] Nigerian Data Protection Regulation (NDPR), etc. Unlike in the European Union where the term "regulation" is used to describe a primary legislation that has a binding force across the member states of EU, such as the GDPR (Craig & Burca, 2011); in Nigeria, a "regulation" (the equivalent of EU's directive) is a secondary legislation that is subservient to a statute. Thus, the main limitation of the NDPR was its subservient status in relation to any Nigerian statute (including statutes of general application applicable in England on or before 1st January 1900) in the event of any conflict on matters of data protection. Based on such low ranking of NDPR, the need for its replacement with a more authoritative legal framework became urgent and necessary.

In the European Union, the GDPR constitutes a comprehensive European data protection law. This is similar to the extant Nigerian regime which has consolidated data protection law in the NDPA.[39] By comparison, however, the US data privacy regime is fragmented across the various industry sectors, and constitutes mainly constitutional doctrines, sector-specific legislations such as the Privacy Act 1974 (which introduced the Code of Fair Information Practices for federal agencies), Children's Online Private Protection Act of 1998, Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act, etc. (Solove & Schwartz, 2018; Bennett, 1992). In the US, data privacy is usually confronted with the more venerable right of freedom of expression under the First Amendment of the US Constitution as well as the underlying principle of "reasonable expectation" of privacy which limits an individual's rights over their data recorded from public spaces (Bennett, 2008).[40] This is unlike the EU where "the right to be forgotten" is recognized by article 17 of the GDPR (Ambrose & Ausloos, 2013),[41] and judicially endorsed in the *Google Spain SL* case.[42] Like the US, the constitutional superiority of the First Amendment and civil liberties over individual privacy (Dutton & Meadow, 1987; Westin, 1970), is similarly found in the Nigerian regime whereby the NDPA stipulates that in relation to personal or household purposes, a given consent to process personal data shall not in any circumstance "[v]iolate the fundamental right to privacy of a data subject".[43]

The GDPR has inarguably inspired a global trend that favors enactment of data protection statutes that are comprehensive and generally apply across all sectors in society (Schwartz, 2019). However, as earlier stated, this trend differs from the US experience with its US sector-specific approach (Schwartz & Peifer, 2017). In the case of Nigeria, given the newness of NDPA, it is difficult to conclude with

[38]See section 3 of the Cybercrimes Act 2015 (Nigeria). This Act was amended in 2024.
[39]Section 2 NDPA.
[40]See *Katz v United States* (1967) 389 US 347, 361.
[41]Also see articles 65, 66 and 156 GDPR.
[42]*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos [es], Mario Costeja González* (C 131/12) ECLI:EU:C:2014:317. See paras 89-91. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>
[43]Section 3(1) NDPA.

finality whether its comprehensiveness[44] will result to effectiveness given that some of its provisions already seem irresponsive to the realities in some sectors, such as corporate insolvency and debt reorganization.[45]

3.2. What Is Personal Data?

According to NDPA, personal data means any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual.[46] Personal data or sensitive personal data that can lead to an identification of an individual include but not limited to:

- Full name of a person;
- National Identification Number and Bank Verification Number;
- Passport number and mobile telephone number;
- Facial image (e.g. in a photograph or video recording);
- Voice recording;
- Biometrics;
- DNA information held by biobanks and hospitals, etc.

NPDA's definitions of "personal" and "sensitive" data are consistent with those of other countries that have enacted a similar statute.[47] Interestingly, NDPA accommodates the various technological advancements that have been ongoing since the last century. Inspired by Collins (2010), it is argued that NDPA's definition of "sensitive data" is sufficiently wide to accommodate individuals' biometrics, iris imagery and DNA profiling. Increasingly, as provided for in section 3(2)(a) NDPA, these types of data are being regularly used in the resolution of crimes, biological parenthood, as well as civil disputes (Liu, 2011).

An Italian case—*Shardna*—demonstrates the judiciary's delicate approach to sensitive personal data because the primary attribute of personal data is its perpetual ability to specifically attach to an individual (Piciocchi et al., 2018). In *Shardna,* the Italian bankruptcy court believed that genetic data are incapable of being de-anonymized (ibid, p. 183). *Shardna* was an insolvent company that was subject of a purchase by Tiziana Life Sciences—a biotechnology company. The buyer's aim was to exploit "[t]he right to use the biological samples, the declaration of consent by participants, the equipment and the content of the biobank as well as the database comprising the medical histories of the donors. This aim was however defeated on the basis that biological samples are ultimately able to reveal information which refers to an identified or identifiable person, and are thus

[44]Section 63 NDPA provides that "where the provisions of any other law or enactment, in so far as they provide or relate directly or indirectly to the processing of personal data, are inconsistent with any of the provisions of this Act, the provisions of this Act shall prevail."

[45]See part 3.7 below for a detailed discussion.

[46]See section 65, NDPA.

[47]For example, see section 2 of Singapore's Personal Data Protection Act 2012.

protected as sensitive personal data" (ibid).

However, there is an inevitable challenge. The level of technology and data harmonization needed to prevent leakage of sensitive data in Nigeria is arguably lacking. This stems from the fact that currently, there is no comprehensive/unitary database at the federal or state level for the storage of dematerialized sensitive data. Sensitive health records are usually in paper form and exist independently in the various health facilities. Thus, moving paper data from one point to another increases the risk of interception and unauthorized leaks to criminals. As would be seen below, this is not the only challenge regarding personal data processing in Nigeria.

3.3. Data Controllers and Processors

Section 65 NDPA defines a "data controller" to be "an individual, private entity, public Commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data". A data controller is different from a data processor (Blume, 2013). The latter, according to NDPA, is "an individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of a data controller or another data processor".[48] The main difference between the two is that while a data processor can determine jointly or alone the purposes and means of processing personal data; a data processor can only undertake a similar task *on behalf of or at the direction of a data controller or another data processor.*[49]

Like the European Union GDPR,[50] NPDA provides that "data protection officers" must be appointed by all *data controllers of major importance*, and the latter shall "designate a Data Protection Officer with expert knowledge of data protection law and practices, and the ability to carry out the tasks prescribed under this Act and subsidiary legislation made under it".[51] By providing for the compulsory appoint of DPOs by data processors of major importance the Nigerian legal framework demonstrates, prima facie, a strong commitment to protect personal data. However, as would be shown below, gaps exist which could threaten the realization of this purpose.

3.4. The Role of Consent: NDPA and CAMA in Perspective

NDPA stipulates that a data controller shall bear the burden of proof for establishing a data subject's consent. In determining whether consent was freely and intentionally given, account shall be taken of whether, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[52] Arguably, NDPA's purpose for consent can easily be bypassed through

[48]Section 65 NDPA.
[49]Emphasis by author.
[50]See article 37 GDPR.
[51]section 32(1) NDPA.
[52]Section 26 NDPA.

entrenched corporate practices whereby the contracts between individuals and (big) corporations are drafted exclusively by the latter (Ayres & Schwartz, 2014). In response to this social trend, for centuries, the common law contract has been wary of unconscionable and unfair contract terms which occur as a result of unfair bargains whereby the economically stronger party abuses its dominance (ibid, p. 589).

As a remedy, the doctrine of *contra proferentem* as argued by McCunn (2019), as well as statutory remedies (e.g., the English Unfair Contract Terms Act 1977) have been devised to ascertain and "punish" an abusive stronger party in contracts. However, there have been kickbacks against this equitable remedy. For example, one of the tools of contractual interpretation is textualism (Nelson, 2005). Textualism, unlike contextualism that emphasizes "purpose" (Collins, 2003: p. 196) is anchored on the parol evidence rule (Posner, 1998). Altogether, both concepts operate to the effect that when interpreting contracts, a judge ought to prioritize the plain and ordinary meaning of the contractual document rather than its purposive meaning.[53] Stronger party abuses in contract formation such as unfairness and factual inequality are usually exposed in the contextualist approach to interpretation whereby the background facts, the pre and post contractual documents leading to the contract are admitted into evidence to determine the intention of the parties.[54]

However, the Nigerian Supreme Court has held *ad nauseam* that literal/textual rule should be the preferred method of interpretation.[55] Thus, while section 26 NDPA emphasizes purpose, the Nigerian regime of statutory interpretation seems to favor the textual rule, and its application in the circumstance will likely yield an outcome that differs from the purposive approach to consent. Similarly, commercial contracts typically contain a "Solicitor Clause" which stipulates that in relation to the contractual provisions, each party has consulted with their legal adviser to understand the contract terms before execution. Indeed, if the weaker contractual party is orally pressured to depose to a verifying affidavit in support of the Solicitor Clause, it will be difficult for them to later wriggle away through section 26 NDPA without personally being guilty of perjury, which carries a 14-year imprisonment in Nigeria.[56] Reluctance to admit to perjury may functionally deter the weaker party (the data subject) from alleging oppression, unfairness or breach.

Both statistical and anecdotal evidence support the view that contractual relations between individuals and corporations are generally unequal (Davis & Pargendler, 2022). This view is true irrespective of any statutory provisions of NDPA that purport to give an impression of habitual equality and fairness between contracting parties. Inarguably, equality vanishes on the face of unevenly matched economic powers: the party with more economic power is prima facie more likely to control the formation and performance of the contract. Since

[53]See the cases in footnote 35 above.

[54]See *Investors Compensation Scheme Ltd. v West Bromwich Building Society* (1998) 1 WLR 896.

[55]See the cases in footnote 35 above.

[56]Section 118, Criminal Code Act (Nigeria).

economic power is usually what bequeaths control, an economically powerful individual could also control a corporation, if the latter is financially weaker. In deference to Moore (2016), an equivalent of this situation in company law and CAMA, is the existence of "shadow directors".[57] In relation to NDPA, while the concern about abuse of consent under section 26 is presumably on corporations against individuals; in other instances, a high net worth (human) secured lender or supplier of goods "[w]ho wields real influence"[58] (i.e. shadow director) may also manipulate and acquire corporate consent or cause the company to perform acts that may be inimical to its data subjects.

An example of the forgoing is the potentiality of abuse that lurks beneath section 480 CAMA which provides that "[w]here a company is in administration, no step shall be taken to—(a) enforce security over the company's property except with (i) the consent of the administrator, or (ii) the permission of the Court; or (b) repossess goods in the company's possession under a hire purchase agreement except with the (i) consent of the administrator, or (ii) permission of the Court." As a precondition for lending or supplying of goods, a lender or supplier may obtain a section 480-CAMA consent in advance of any debt restructuring by requiring an undated but executed contract that contains carefully worded provisions that give consent. Upon being dated, the holder may tender it and enjoy the exemption of section 480 towards their security realization. However, subject to whether Nigerian courts will follow the holding in *Southern Pacific* for similar issues, Nigerian administrators and liquidators may be unable to completely avoid liability if their actions during data processing infringe on the fundamental right of privacy as stipulated under section 37 of the Nigerian Constitution.[59]

3.5. Personal Data and Asset Collateralization

Movable (or personal) property is divided into two major categories, namely; tangible and intangible assets.[60] Tangible assets are concrete and can be felt. However, intangible assets cannot be felt by touch and are regarded as *choses in action* (Sobel-Read et al., 2022). In other words, intangible rights can only be enforced through court actions. Section 63 of STMA recognizes intangible assets as capable of being used as collateral to secure debts. An example of an intangible asset is personal data of customers being held by a corporation in the course of business (Litman, 2000). Section 65 NDPA, defines personal data as "any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual".

Based on the *Toysmart* case, an example of personal data that is considered an

[57]See section 270 CAMA 2020.

[58]*Secretary of State for Trade and Industry v Deverell* [2001] Ch. 340 per Morritt LJ, para 33.

[59]See sections 1 and 3 NDPA.

[60]Section 63 STMA.

asset is "list of customers" (Pissott, 1992: p. 1031). A list of customers (in an organized form) comprises of consumers' personal information such as names, date of birth, home addresses, phone numbers, email addresses, etc. (ibid). These personal data may be gathered over a period of time in the ordinary course of business. Indeed, they have commercial value that could add to the estimated worth of a business (ibid). For example, if a business is being evaluated for a liquidation sale, its trade secrets, goodwill, and list of customers are equally evaluated as assets of the business owing to their commercial value. Thus, there is no justifiable (legal) reason why an interpretation of section 63 STMA should not include 'list customers' as an asset that could be used as collateral to secure debts. The cases discussed here show that personal data are regarded as corporate assets that could be sold in the context of liquidation to satisfy stakeholders' debts.[61]

3.6. Personal Data and Insolvency Practitioners

Based on CAMA 2020, a company can be wound up on the basis of inability to repay due debts.[62] The process commences by a creditor making a demand for repayment of debt N200,000 or above.[63] If the corporate debtor fails to repay the debt after lapse of the statutory grace period of three weeks, then the creditor could commence process to wind it up.[64] Similarly, a creditor with a crystallized CAMA-floating charge can choose to either appoint a receiver-manager or an administrator:[65] the former operates under the more entrenched receivership regime which was also practiced under the CAMA 1990.[66] In deference to Milman (1981), receivers act mainly as agents (and for the interests of their appointors) by taking over corporate management. CAMA 2020 however provides an alternative: holder of a crystallized floating charge can also choose to appoint an administrator who is statutorily mandated to act for all the corporate debtor's stakeholders.[67] An administrator can manage the corporate assets or sell them if he believes that sale rather than management will be more beneficial to the corporate debtor's stakeholders.[68] Whether a receiver, an administrator or liquidator is chosen in the context of corporate insolvency/liquidation, the questions of how personal data as defined under the NDPA are processed as well as the possible liability of the insolvency practitioner are yet to be answered in the Nigerian context.

Thus, it is important to determine whether insolvency practitioners as established under the CAMA 2020 (i.e., lawyers, accountants, etc.), accredited to carry

[61]The concern that data can be "sold, distributed, or otherwise shared through bankruptcy proceedings without adequate protections for Illinois citizens" formed the major issue for determination in the US case *Heard v. Becton* 440 F.Supp. 3d 960 (2020).

[62]Section 571 (d) CAMA 2020.

[63]Section 572 (a) CAMA 2020.

[64]Ibid.

[65]See sections 205 and 452 CAMA 2020.

[66]See Part XIV: sections 387- 400 CAMA 1990; *West African Breweries Ltd v Savannah Ventured Ltd* (2002) LPELR-3475 (SC).

[67]Section 452 CAMA 2020.

[68]Section 444(4) - (6) CAMA 2020.

out insolvency practice can be regarded as data controllers or processors in their capacity as insolvency practitioners who deal with all types of corporate assets including personal data? Answering this question necessitates a reproduction of section 25 NDPA in its entirety. Section 25 provides as follows:

"Without prejudice to the principles set out in this act, data processing shall be lawful, where—(a) the data subject has given and not withdrawn consent for the specific purpose or purposes for which personal data is to be processed ; or (b) the processing is necessary—(i) for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract, (ii) for compliance with a legal obligation to which the data controller or data processor is subject, (iii) to protect the vital interest of the data subject or another person, (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or data processor, or (v) for the purposes of the legitimate interests pursued by the data controller or data processor, or by a third party to whom the data is disclosed. (2) Interests in personal data processing shall not be legitimate for the purposes of subsection (1)(b)(v), where—(a) they override the fundamental rights, freedoms and the interests of the data subject; (b) they are incompatible with other lawful basis of processing under subsection (1)(b) (i)-(iv); or (c) the data subject would not have a *reasonable expectation* that the personal data would be processed in the manner envisaged."[69]

A careful reading of section 25 above, shows that processing of personal data for the purpose of realizing assets of a corporate debtor during an insolvency procedure, constitutes a "lawful basis".[70] This makes insolvency practitioners potentially data controllers/processors in the Nigerian context although the decision in *Southern Pacific* seems to indicate a contrary view.[71] Section 25(2) NDPA states that nothing in the act of processing personal data "[s]hall override the fundamental rights, freedoms and the interests of the data subject". As would be seen below from the facts of *Southern Pacific*, the processing of data subjects' requests in administration/liquidation may pose enormous costs that threaten a complete erosion of corporate assets that are held for distribution. The Nigerian business community may be legitimately curious to know how Nigerian courts will balance the reality of financial costs on businesses engendered by section 34(d) NDPA in relation to processing data subjects' requests in liquidation with their fundamental (constitutional) rights.[72]

Similarly, when administrators are appointed under the CAMA 2020 framework, they may oust the corporate debtor's management and assume overall

[69]Interestingly, NDPA uses the term "reasonable expectation" twice in the Act, namely in sections 25 and 30, but did not provide any definition for it even though the term has received interpretation in other countries since several decades ago. Italics by author.

[70]Also see section 34(2)(b) NDPA.

[71]See part 3.7 below for details.

[72]If eventually, section 34(d) NDPA's "unreasonable cost" is interpreted to be borne by data subjects, this will invariably discourage access. A debtor company may project a high cost of implementation to satisfy the "unreasonable" threshold, so as to require the data subject to bear the cost of access.

corporate leadership.[73] Although administrators may appoint DPOs or third parties to assist with personal data processing, the lesson from *Southern Pacific* indicates that such administrators/liquidators may not be generally liable for personal data breaches that occurred prior to their appointment. This is because administrators/liquidators are regarded as corporate agents, whose agency prevents from being vicariously liable for their principals' breaches prior to appointment. However, towards ensuring compliance with NDPA, insolvency practitioners in Nigeria (as a precondition for undertaking insolvency practice) need to be specifically trained on the various intersections between insolvency practice and data protection. In what follows, the article discusses the facts of *Southern Pacific*. The precedent is foreseen to provide guidance to Nigerian judges who may soon face issues of personal data processing in the context of corporate administration or liquidation.

3.7. In Re Southern Pacific Personal Loans Ltd: Any Lessons for Nigeria?

The provisions of NDPA are foreseen to challenge how businesses were organized and managed prior to its enactment. One such challenge relates to costs of implementation—who will bear the cost of implementing the rights of data subjects under the NDPA. Since the cost of implementation is usually satisfied from corporate assets, should there be a maximum limit in terms of cost?[74] In the case of an insolvent company under administration/liquidation, an unlimited right of data subjects to apply for access to information adds a considerable cost to the administration/liquidation, and could erode the assets available for distribution. Poor returns on creditors' investments due to eroded corporate assets may gradually demotivate corporate lenders from providing affordable credits for doing business. In *London Oil and Gas Ltd (In Administration),*[75] one of the issues the court had to resolve was the type of documents administrators should have access to, including the bearer of cost of search, as well as the practicable manner for processing data subjects' information.

The problem of cost regarding the processing of personal data was much more detailed in *In Re Southern Pacific Personal Loans Ltd.*[76] The case reveals that implementation of privacy rights as stipulated in the data protection law could be exorbitant, and in many cases, the cost bearer is unclearly delineated especially when the corporate debtor is no longer a *going concern*. Similarly, the case shows that corporate stakeholders such as creditors, employees, directors, and shareholders of a corporate debtor can be affected in an insolvency procedure, being that the assets available for distribution could be threatened by the sums deducted for the implementation of personal data rights, which rank above security interest

[73]Sections 496 - 501 CAMA 2020.

[74]See section 34(d) NDPA.

[75]*London Oil and Gas Ltd (In Administration)* [2019] EWHC 3675.

[76]*Re Southern Pacific Personal Loans Ltd* [2013] EWHC 2485 (Ch), (referred to as "*Southern Pacific*" throughout this paper). An electronic version of the case may be accessed from https://www.bailii.org/ew/cases/EWHC/Ch/2013/2485.html

rights, owing to the former's constitutional element.

In *Southern Pacific,* the personal loans provided by the corporate debtor to individuals in the UK were secured by way of second charge on their homes prior to its insolvency.[77] Although details of the loans were transferred to special purpose vehicles (SPVs),[78] the personal data of the individual debtors remained with the corporate debtor which later went into a voluntary liquidation.[79] However, irrespective of the company's liquidation status, its appointed joint liquidators continued to receive an overwhelming amount of applications (Data Subject Access Requests—DSARs) from data subjects regarding their personal data. Based on evidence, it cost GBP 455 exclusive of value added taxes to satisfy one DSAR.[80] This was in addition to the cost of storage and processing of personal data which a third party company (Acenden Limited) incurred by processing DSARs on behalf of *Southern Pacific*.[81] Based on the calculations of the joint liquidators, 88 DSARs were filed monthly, costing about GBP 40,000.[82] At this rate, it would cost about GBP 589,000 per year to process DSARs.[83] While GBP 3 million was available for distribution to creditors, the overall debt of the company was a little over GBP 10 million.[84] In that case, a yearly deduction of GPB 589,000 to process DSARs will significantly erode available assets and impede the liquidation process.

Based on a literal construction of the UK Data Protection Act 1998 (i.e. prior to the court's verdict), the joint liquidators qualified as data controllers or processors.[85] On this basis, they applied to the court for clarification on whether (in view of the unaffordable costs for processing DSARs) they could refuse to comply with DSARs, or alternatively dispose of the personal data that were costing the corporate debtor GBP 589,000 annually to keep and process.[86] The corporate debtor was already in liquidation and therefore no longer in need of the personal data for trading. Holding that the joint liquidators may dispose the personal data, the court relied on section 5 of UK's DPA, which states that "personal data shall not be kept for longer than is necessary for the purpose or purposes for which it was processed."[87]

Another clarity that was provided by the *Southern Pacific* case relates to the status of insolvency practitioners (administrators, liquidators, etc.) in the context

[77]Ibid, para 5.
[78]Ibid.
[79]Ibid, para 6.
[80]Ibid, para 10.
[81]Ibid.
[82]Ibid.
[83]Ibid.
[84]Ibid.
[85]Sections 1 and 4(4) UK DPA 1988.
[86]For example, section 7(8) UK DPA 1988, requires a data controller to comply with a request promptly and in any event within 40 days or such other period as may be prescribed after receipt of the request. See *Southern Pacific*, para 16. In Nigeria the cost of processing requests as typified by the *Southern Pacific* case may likely pass the unreasonable cost test and thus borne by the data subjects.
[87]*Southern Pacific*, para 39. The equivalent of this principle in NDPA is section 24(1)(d) that "a data controller or data processor shall ensure that personal data is retained for not longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed".

of corporate administration or liquidation. Before the case, the general impression regarding the status of insolvency practitioners was similar to what the Information Commissioner thought in the *Southern Pacific* case, which was that insolvency practitioners (liquidators and administrators) can also be regarded as data controllers/processors.[88] However, in *Southern Pacific,* the court held that liquidators and administrators are mere agents of an insolvent company and cannot be held liable for the personal data collected and processed before their appointment.[89] One of the relevancies of this precedent is that insolvency practitioners will not be liable for breach of personal data that occurred prior to their appointment by the debtor company. Accordingly, this meant that if they refused to respond to requests in respect of the data processed by the debtor company (DSARs), they will not be held liable for breach of rights of the data subjects.[90]

4. Conflict of Laws: Defense of Legal Claims Outside of Nigeria

According to NDPA, one of the grounds on which a data controller/processor shall transfer personal data from Nigeria to another country is "if the transfer is necessary for the establishment, exercise, or defense of legal claims".[91] Similarly, STMA contains its choice of law provision. It states that "the law applicable to the mutual rights and obligations of the grantor, the borrower and the secured party arising from their security agreement is the law chosen by the parties and, in the absence of any choice of law, the law governing the security agreement."[92] Based on the provisions of these legislations and relevant case law, it can be ascertained that in enforcement of contracts, the Nigerian legal framework defers to freedom of contract and its party autonomy principle.[93]

However, the challenge is that NDPA did not expressly compel data controllers to always host the personal data of Nigerian data subjects in Nigeria.[94] Scholars such as (Kuner, 2013; Newman, 2008; Wagner, 2018) have discussed extensively on cross-border transfer of personal data and underlying issues. Thus, hypothetically, a foreign based company (e.g. an English company) may choose to operate in Nigeria through a subsidiary that may obtain the personal data of Nigerians and subsequently host them abroad or transfer them to its parent company in England. If a dispute arises over an English law-and-forum-governed secured debt

[88] *Southern Pacific*, para 29.
[89] Ibid, para 19.
[90] Ibid, paras 20 and 21.
[91] Section 43(1)(e) NDPA. Given that NDPA draws largely from GDPR, the "adequate protection" threshold under NDPA may be interpreted based on the lessons from GDPR. See Julian Wagner, "The Transfer of Personal Data to Third Countries Under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?" (2018) 8 *International Data Privacy Law* 318.
[92] Section 52, STMA.
[93] *Nika Fishing Company Ltd v Lavina Corporation* (2008) 16 NWLR 509, 535 (Mohammed JSC, as he then was, held that in determining whether or not to grant a stay of proceedings in deference to a forum selection agreement, Nigerian law "requires such discretion to be exercised by granting a stay unless strong cause for not doing so is shown. The burden of showing such strong cause for not granting the application lies on the doorsteps of the respondent as the plaintiff".)
[94] See section 43 NDPA.

contract between the subsidiary and Nigerian data subjects, the applicable law in the circumstance will be English law and forum, especially in reference to section 2(2) NDPA, which stipulates that NDPA does not apply to data processing outside of Nigeria. Similarly, if the subsidiary is undergoing an insolvency procedure, the applicable English law and forum in the circumstance implies a lack of access for Nigerian data subjects as well as the application of *Southern Pacific* which may absorb appointed liquidators of liability if they refuse to honor the requests of Nigerian data subjects applying from Nigeria.

Before the enactment of STMA and its section 52 which favors party autonomy in choice of law, the insolvency rule in *Gibbs*[95] had already been part of English law for over a century. The rule in *Gibbs* is a public law rule to the effect that a foreign insolvency proceeding cannot be used to restructure debts of an English governed contract unless the impacted creditor submits willingly to the jurisdiction of the foreign court.[96] While the *Gibbs* rule shows the overprotectiveness of the English legal system for its national interests over international comity, the Nigerian legal system bends towards freedom of contract and party autonomy, which enable contracting parties in Nigeria to utilize foreign laws and forums to bypass the statutory/consumer protections afforded to the Nigerian people.[97] Indeed, one of the section-1 objectives of NDPA is to "[p]rotect data subjects' rights, and provide means of recourse and remedies, in the event of the breach of the data subject's rights…and to also establish an impartial, independent, and effective regulatory Commission to superintend over data protection and privacy issues, and supervise data controllers and data processors".[98] However, these objectives can possibly be defeated with a contractual foreign jurisdiction clause under the principles of freedom of contract and party autonomy. The suggested solution, as argued below, resides in crafting mandatory rules on choice of law which must accommodate Nigerian economic interests.

4.1. Proposal for a Restrictive Mandatory Rule on Choice of Law vis-a-vis NDPA: Lessons from the Nigerian Admiralty Legal Framework

Inarguably, the Nigerian jurisprudence on foreign jurisdiction clauses (FJCs) evolved from, or is dominated by maritime or admiralty contracts. Although much of the FJC case law stems from admiralty claims, the principles enunciated in these cases should arguably apply to other types of commercial contracts other than those of admiralty. In that regard, the question is what the attitude of Nigerian courts is or ought to be where there is an exclusive FJC in a commercial (non-admiralty) contract in which one or both parties are Nigerians, and performance of contract is in Nigeria? The Nigerian judicial attitude in relation to FJC is a more challenging

[95] *Antony Gibbs Sons v. La Société Industrielle Et Commerciale Des Métaux* (1890) 25 QBD 399 (Court of Appeal).

[96] Ibid, p. 405, per Lord Esher.

[97] See *Nika Fishing Company Ltd v Lavina Corporation* (2008) 16 NWLR 509, 535.

[98] Section 1 (e) and (f) NPDA.

question to answer considering the seeming bifurcation of commercial contracts into admiralty and the non-admiralty types. By focusing on the admiralty type of contracts and its legal framework, the article shows that it will not be outrageous if Nigerian law extends similar mandatory rules in admiralty contracts to their non-admiralty counterparts.

4.1.1. The Admiralty Legal Framework in Nigeria

In respect of the admiralty legal framework, the starting point is section 251(1) (g) of the Constitution of Federal Republic of Nigeria (CFRN) 1999, which confers admiralty jurisdiction on the Nigerian Federal High Court (Nwobike, 2013). Similarly, section 20 of the Admiralty Jurisdiction Act (AJA) 1991 gives the Federal High Court the exclusive jurisdiction to entertain disputes concerning admiralty matters. Section 20 AJA 1991 prohibits any agreement which ousts the jurisdiction of Nigerian courts if the contract is to be performed in Nigeria.[99] In other words, the consequence of FJC in such contracts is nullity and voidance of such contracts. This directly means that inclusion of FJC in admiralty contacts will render the contract illegal by statute (i.e. section 20 AJA 1991), and thus invalid and unenforceable by courts.

Being that an admiralty contract which contains FJC becomes immediately invalid by operation of law, it is questionable whether a foreign court (such as the one nominated by contracting parties in their contract in breach of section 20) would be willing to enforce the contract knowing that its formation contravened a Nigerian statute *ab initio*. It is hardly the public policy ambition of any country to enforce contracts which they are aware (or ought to be aware) contravened with a legitimate law in force in another country.[100]

Will a party suing in breach of the stipulation of section 20 AJA 1991 in an English court, for instance, be excused on the basis of the fifth factor in the *Eleftheria* case?[101] Going against this basic principle of international comity (as also held by a Malawian court) will attract negative perceptions in the international commercial arena.[102] However, if the foreign (English) court enforces and gives judgment on the basis of such a contract in disregard to section 20 AJA 1991, an attempt to recognize and enforce it in a Nigerian court will likely fail because the courts will characterize the foreign judgment as invalid owing to its contravention with Nigerian public law and policy.[103] Thus, the question of the extent to which

[99]Section 20 AJA 1991 has eight paragraphs: a-h. For lack of space, only section 20(a) and (b) are reproduced: "Any agreement by any person or party to any cause, matter or action which seeks to oust the jurisdiction of the Court shall be null and void, if it relates to any admiralty matter falling under this Act and if (a) the place of performance, execution, delivery, act or default is or takes place in Nigeria; or (b) any of the parties resides or has resided in Nigeria."

[100]Although it is easy for a judge relying on the fifth (5e) factor in *The Eleftheria* to come to the decision to deny enforcement of FJC because he or she whimsically suspects that the plaintiff will not get a fair trial in the agreed forum owing to *political, racial, religious or other reasons. Emphasis by author.*

[101]Ibid.

[102]*Mzumacharo v. Osman's Garage* [1978–80] 9 MLR 68.

[103]In Suit No FHC/L//CP/469/2014: *Access Bank Plc v. Akingbola* (Unreported, delivered on 17 November 2014); *Jones v. Krok* 1996 (1) SA 504 (South Africa).

a foreign judgment in contract will be recognized and enforced in Nigeria depends on the type of commercial contract.[104] For admiralty contracts, the answer is fairly straightforward and settled: if an admiralty contract contains FJC in disregard of section 20 AJA 1991, then the adjudication of such contract in a foreign forum will ultimately produce an invalid and unenforceable judgment if the judgment holders seeks to recognize and enforce it in a Nigerian court.

4.1.2. Lessons from the Admiralty Legal Framework: NDPA in Perspective

For non-admiralty commercial contracts, such as those that may touch upon the STMA, CAMA and NDPA, it is not yet settled whether the Nigerian law will totally oppose the inclusion of FJCs or invalidate them, or whether validity has to be determined on a case by case basis. In fact, the Supreme Court's decision in *Nika Fishing Company Ltd,*[105] shows that freedom of contract and party autonomy will largely apply in non-admiralty contracts. It is argued that the Nigerian judicial attitude towards admiralty contracts on the basis of the meaning and effect of section 20 AJA 1991 be taken as Nigeria's "mandatory rule" for contracts implicating the NPDA, as well as all commercial contracts (whether or not they are admiralty contracts) in which an exclusive FJC was included to bypass the Nigerian courts. This will prevent instances in which the personal data of Nigerians are breached without any legal redress because the underlying contracts contain FJCs. In other words, while it is almost settled that a Nigerian court could refuse to stay proceeding in deference to section 20 AJA where an admiralty contract is involved, it is still debatable whether they can or should be able to refuse a stay of proceeding irrespective of a well worded exclusive FJC in non-admiralty contracts, and sought to be enforced on the basis of freedom of contract.

To summarize, the clarity of the applicable legal framework in respect of admiralty contracts is no longer in doubt because in their respects, section 251(1)(g) CFRN and section 20 AJA 1991 are applicable, and any type of FJC whether exclusive or otherwise which ousts the Federal High Court will automatically become null and void and thus unenforceable. Similarly, as already argued, such treatment should be extended to all commercial contracts (whether admiralty or non-admiralty) that are performed in Nigeria as demonstrated by the case of *Lignes Aeriennes Congolese vs. Air Atlantic Nigeria Ltd.*[106] In this case the parties chose Congolese law and forum to govern their aircraft lease agreement even though performance of the contract was in Nigeria. However, when a dispute arose regarding performance of the contract, the Nigerian party sued in the Federal High Court, Lagos. The defendant objected that the Nigerian court lacked jurisdiction owing to the forum selection agreement that conferred jurisdiction to a Congolese court. The Federal High Court held that the forum jurisdiction clause in the aircraft agreement had purported to oust its jurisdiction and by virtue of section 20 AJA 1991, it has the jurisdiction to entertain the matter. On appeal, the

[104] *Access Bank Plc v. Erastus Bankole Oladipo Akingbola* [2013] EWCA Civ 744.
[105] *Nika Fishing Company Ltd* (n 11) above.
[106] (2006) 2 NWLR (Pt.963) 49.

Court of Appeal also agreed with the Federal High Court.

5. Conclusion

In conclusion, the article reiterates that insolvent corporate debtors often possess a considerable amount of personal data, such as customer lists and user data. Similarly, the insolvency/liquidation of biobanks and private hospitals pose significant challenges vis-vis-vis the sensitive personal data in their holding. An example of what requires clarification under Nigerian law is whether such sensitive personal data can be liquidated to satisfy the corporate debtors' debts. Insolvency practitioners (e.g. administrators and liquidators) are typically appointed to manage and distribute corporate debtors' assets to their stakeholders, and these tasks may implicate data processing. By this very fact, they most likely fit into NDPA's definition of controllers/processors, and therefore, are subject to personal liabilities if their activities infringe on the fundamental privacy rights of data subjects. Likewise, where personal data are necessary for trading under administration, the cost of processing information requests from data subjects may impede the success of the administration. Although NDPA indicates that a data subject will bear the cost of processing if the underlying cost is "unreasonable", neither case law nor subsidiary legislations have clarified the quantum of cost as well as the circumstances that will meet the "unreasonable" exception.

Moreover, the conflict of laws in Nigeria defers to freedom of contract and party autonomy principles. Abusive contract parties intending to bypass the stringent measures of the NDPA as well as Nigerian courts may succeed through exclusive foreign jurisdiction clauses that prevent Nigerian courts from adjudicating on contracts that possibly infringe on the provisions of NDPA. The article therefore recommends that the NDPA be reformed based on the forgoing legal analysis.

Biographical Note

Dr. Joseph Nwobike is a highly sought-after lawyer that leads the *Osborne Law Practice* in Nigeria. He is a Senior Advocate of Nigeria (SAN), a Fellow of the Chartered Institute of Arbitrators (UK), and has over 30 years of litigation experience in commercial law and human rights. He has provided a countless number of national and foreign clients with authoritative legal advice in the areas of Corporate Law, Insolvency and Debt Restructuring, Data Protection, Mergers and Acquisitions, Foreign Investments, Contracts and Finance Transactions. He is a scholar-practitioner and enjoys academic legal research and writing.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Abdulrauf, L. A., & Fombad, C. M. (2016). Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms. *Liverpool Law Review, 38,*

105-134. https://doi.org/10.1007/s10991-016-9189-8

Ambrose, M. L., & Ausloos, J. (2013). The Right to Be Forgotten across the Pond. *Journal of Information Policy, 3,* 1-23. https://doi.org/10.5325/jinfopoli.3.2013.0001

American Bankruptcy Institute (2020). *Annual Business and Non-Business Filings by Year, 1980-2020*. https://abi-org.s3.amazonaws.com/Newsroom/Bankruptcy_Statistics/Total-Business-Consumer1980-Present.pdf

Ayres, I., & Schwartz, A. (2014). The No-Reading Problem in Consumer Contract Law. *Stanford Law Review, 66,* 545-609.

Ben-Ishai, S., & Lubben, S. (2012). Involuntary Creditors and Corporate Bankruptcy. *UBC Law Review, 45,* 253-282.

Bennett, C. J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell University Press. https://doi.org/10.7591/9781501722134

Bennett, C. J. (2008). *The Privacy Advocates: Resisting the Spread of Surveillance*. The MIT Press. https://doi.org/10.7551/mitpress/7855.001.0001

Blume, P. (2013). Controller and Processor: Is There a Risk of Confusion? *International Data Privacy Law, 3,* 140-145. https://doi.org/10.1093/idpl/ipt002

Bruynseels, K., & van den Hoven, J. (2015). How to Do Things with Personal Big Biodata. In B. Roessler, & D. Mokrosinska (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (pp. 122-140). Cambridge University Press. https://doi.org/10.1017/cbo9781107280557.008

Bygrave, L. A. (2014a). *Data Privacy Law*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199675555.001.0001

Bygrave, L. A. (2014b). Data Privacy Law and the Internet: Policy Challenges. In N. Witzleb, D. Lindsay, M. Paterson, & S. Rodrick (Eds.), *Emerging Challenges in Privacy Law: Comparative Perspectives* (pp. 259-289). Cambridge University Press.

Carnegy-Arbuthnott, H. (2023). Privacy, Publicity, and the Right to Be Forgotten. *Journal of Political Philosophy, 31,* 494-516. https://doi.org/10.1111/jopp.12308

Charlesworth, A. (2000). Clash of the Data Titans? US and EU Data Privacy Regulation. *European Public Law, 6,* 253-274. https://doi.org/10.54648/265901

Choi, H., Park, J., & Jung, Y. (2018). The Role of Privacy Fatigue in Online Privacy Behavior. *Computers in Human Behavior, 81,* 42-51. https://doi.org/10.1016/j.chb.2017.12.001

Clarke, I., Sandberg, O., Wiley, B., & Hong, T. W. (2001). Freenet: A Distributed Anonymous Information Storage and Retrieval System. In H. Federrath (Ed.), *Designing Privacy Enhancing Technologies* (pp. 46-66). Springer. https://doi.org/10.1007/3-540-44702-4_4

Collins, F. S. (2010). *The Language of Life: DNA and the Revolution in Personalized Medicine*. HarperCollins.

Collins, H. (2003). Objectivity and Committed Contextualism in Interpretation. In S. Worthington (Ed.), *Commercial Law and Commercial Practice* (pp. 189-209). Hart Publishing.

Colonna, L. (2022). Addressing the Responsibility Gap in Data Protection by Design: Towards a More Future-Oriented, Relational, and Distributed Approach. *Tilburg Law Review, 27,* 1-21. https://doi.org/10.5334/tilr.274

Craig, P., & Búrca, G. (2011). *EU Law* (5th ed.). Oxford University Press.

Davis, K. E., & Pargendler, M. (2022). Contract Law and Inequality. *Iowa Law Review, 107,* 1485-1541.

Dutton, W. H., & Meadow, R. G. (1987). A Tolerance for Surveillance: American Public

Opinion Concerning Privacy and Civil Liberties. In K. Levitan (Ed.) *Government Infostructures* (pp. 147-170). Greenwood Press.

Esangbedo, G. (2020). Secured Transactions in Moveable Assets Act, Company Charges and Funding Micro, Small and Medium Enterprises under Nigerian Law. *Journal of African Law, 64,* 81-105. https://doi.org/10.1017/s0021855319000354

Essen, E. (2000). Conflicting Rationes Decidendi: The Dilemma of the Lower Court in Nigeria. *African Journal of International and Comparative Law, 12,* 23-30.

Federal Trade Commission (2000, July 21). *FTC Announces Settlement with Bankrupt Website, toysmart.com, Regarding Alleged Privacy Policy Violations*. https://www.ftc.gov/news-events/news/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding-alleged-privacy-policy-violations

Financial Crisis Inquiry Commission (2011, February 25). *The Financial Crisis Inquiry Report*. https://www.govinfo.gov/content/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf

GDPR. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World* (p. 176). Oxford University Press.

Iheme, W. C., & Mba, S. U. (2021). A Doctrinal Assessment of the Insolvency Frameworks of African Countries in Coping with the Pandemic-Triggered Economic Crisis. *Stellenbosch Law Review, 2021,* 306-329. https://doi.org/10.47348/slr/2021/i2a7

International Monetary Fund (2020, April 14). *The Great Lockdown: Worst Economic Downturn since the Great Depression*. https://www.imf.org/en/Blogs/Articles/2020/04/14/blog-weo-the-great-lockdown-worst-economic-downturn-since-the-great-depression

Investors Compensation Scheme Ltd. v West Bromwich Building Society [1998] 1 WLR 896.

Iwobi, A. U. (2017). Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime. *Transnational Law and Contemporary Problems, 26,* 14-61.

Katz v United States (1967). *389 US 347*.

Kennedy, P. I. (2004). *Military Adventurism in Nigeria Politics*. Mentors Communications Limited.

Kuner, C. (2013). *Transborder Data Flow Regulation and Data Privacy Law*. Oxford University Press.

Litman, J. (2000). Information Privacy/Information Property. *Stanford Law Review, 52,* 1283-1313. https://doi.org/10.2307/1229515

Liu, N. Y. (2011). *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics*. Routledge.

McCunn, J. (2019). The Contra Proferentem Rule: Contract Law's Great Survivor. *Oxford Journal of Legal Studies, 39,* 483-506. https://doi.org/10.1093/ojls/gqz002

Moore, C. R. (2016). Obligations in the Shade: The Application of Fiduciary Directors' Duties to Shadow Directors. *Legal Studies, 36,* 326-353. https://doi.org/10.1111/lest.12110

Nelson, C. (2005). What Is Textualism? *Virginia Law Review, 91,* 347-418.

Newman, A. L. (2008). *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Cornell University Press. https://doi.org/10.7591/9781501729218

Ngo, M.V. (2002). Getting the Question Right on Floating Liens and Securitized Assets. *Yale Journal on Regulation, 19,* 85-169.

Nwobike, J. A. (2013). Jurisdiction and the Contractual Freedom of Parties—Do Expropriatory

Contracts Really Expropriate? In S. A. M. Ekwenze, I. Chibuzor, A. O. Okeke, & N. Okeke, (Eds.), *Demand for Justice: Essays in Honour of Hon* (pp. 33-52). Snap Press Ltd.

Nwobike, J. A. (2023). The Incompatibilities of the Secured Transactions Law Reform in Nigeria with Access to Credit: What Did the Lawmakers Get Wrong? *Beijing Law Review, 14,* 87-110. https://doi.org/10.4236/blr.2023.141005

Omotubora, A., & Basu, S. (2020). Next Generation Privacy. *Information & Communications Technology Law, 29,* 151-173. https://doi.org/10.1080/13600834.2020.1732055

Onyeaka, H., Anumudu, C. K., Al-Sharify, Z. T., Egele-Godswill, E., & Mbaegbu, P. (2021). COVID-19 Pandemic: A Review of the Global Lockdown and Its Far-Reaching Effects. *Science Progress, 104,* 1-18. https://doi.org/10.1177/00368504211019854

Orji, U. J. (2017). Regionalizing Data Protection Law: A Discourse on the Status and Implementation of the ECOWAS Data Protection Act. *International Data Privacy Law, 7,* 179-189. https://doi.org/10.1093/idpl/ipx013

Payne, J. (2018). The Role of the Court in Debt Restructuring. *The Cambridge Law Journal, 77,* 124-150. https://doi.org/10.1017/s0008197318000016

Piciocchi, C., Ducato, R., Martinelli, L., Perra, S., Tomasi, M., Zuddas, C. et al. (2018). Legal Issues in Governing Genetic Biobanks: The Italian Framework as a Case Study for the Implications for Citizen's Health through Public-Private Initiatives. *Journal of Community Genetics, 9,* 177-190. https://doi.org/10.1007/s12687-017-0328-2

Pissott, L. J. (1992). The Amortization of Customer-Based Intangibles: The "Separate & Distinct from Goodwill" Requirement and H.R. 3035's Proposal for Change. *The Tax Lawyer, 45,* 1031-1043.

Pollman, E. (2021). Corporate Personhood and Limited Sovereignty. *Vanderbilt Law Review, 75,* 1727-1753.

Posner, E. A. (1998). The Parol Evidence Rule, the Plain Meaning Rule, and the Principles of Contractual Interpretation. *University of Pennsylvania Law Review, 146,* 533-577. https://doi.org/10.2307/3312625

Reidenberg, J. R. (2001). E-Commerce and Transatlantic Privacy. *Houston Law Review, 38,* 717-749.

Ripken, S. K. (2019). *Corporate Personhood*. Cambridge University Press. https://doi.org/10.1017/9781108241366

Schwartz, P. M. (2004). Property, Privacy, and Personal Data. *Harvard Law Review, 117,* 2056-2128. https://doi.org/10.2307/4093335

Schwartz, P. M. (2013). The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. *Harvard Law Review, 126,* 1966-2009.

Schwartz, P. M. (2019). Global Data Privacy: The EU Way. *New York University Law Review, 94,* 771-818.

Schwartz, P. M., & Peifer, K.-N. (2017). Transatlantic Data Privacy Law. *Georgetown Law Journal, 106,* 115-179.

Skeel, D. (2021). Pandemic Hope for Chapter 11 Financing. *The Yale Law Journal Forum, No. 10,* 315-336. https://www.yalelawjournal.org/pdf/F7.SkeelFinalDraftWEB_3s3482o2.pdf

Sobel-Read, K., Anderson, G., & Salminen, J. (2022). The Critical Role of Choses in Action: A Call for Harmonization across Common Law Jurisdictions. *Fordham International Law Journal, 45,* 513-574.

Solove, D. J., & Schwartz, P. M. (2018). *Information Privacy Law* (6th ed.). Aspen Publishers.

United Nations (2023, May 5). *WHO Chief Declares end to Covid-19 as a Global Health Emergency*. https://news.un.org/en/story/2023/05/1136367.

Wagner, J. (2018). The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection? *International Data Privacy Law, 8*, 318-337. https://doi.org/10.1093/idpl/ipy008

Westin, A. F. (1970). *Privacy and Freedom*. Atheneum.

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal, 113,* 1151-1221. https://doi.org/10.2307/4135723

Legislation

1. Companies and Allied Matters Act 2020 (Nigeria)
2. Criminal Code Act (Nigeria)
3. Cybercrimes Act 2015 (Nigeria)
4. Data Protection Act 1988 (United Kingdom)
5. Nigerian Dara Protection Regulation
6. Nigerian Data Protection Act 2023
7. Personal Data Protection Act 2012 (Singapore)
8. Secured Transactions in Movable Assets Act 2017
9. General Data Protection Regulation (European Union)
10. Universal Declaration of Human Rights
11. Constitution of the Federal Republic of Nigeria 1999
12. Privacy Act 1974 (United States)
13. Children's Online Private Protection Act 1998 (U.S)
14. Health Insurance Portability and Accountability Act (U.S)
15. Gramm-Leach-Bliley Act (U.S)

Cases

1. *A.G. of Ondo State v. A.G. of the Federation* [1983] 2 SCNLR 269
2. *Access Bank Plc v. Erastus Bankole Oladipo Akingbola* [2013] EWCA Civ 744.
3. *Adisa v Oyinwola* (2000) 10 NWLR (Pt 674) 116
4. *Agnew v. Commissioner of Inland Revenue* [2001] 2 AC 710
5. *Amaechi v INEC* (2008) 5 NWLR (Pt. 1080) 227
6. *Antony Gibbs Sons v. La Société Industrielle Et Commerciale Des Métaux* (1890) 25 QBD 399 (Court of Appeal).
7. *Awojugbagbe Light Industries v Chinukwe* (1995) 4 NWLR (pt. 390) 379
8. *Bank of the North v* Muri [1998] 2 NWLR (pt 536) 153
9. *Buchler v Talbot* [2004] 2 AC 298
10. *Chief Obafemi Awolowo v. AlhajiShehu Shagari Ors.* (1979) 6-9 S.C. 51
11. *Douez v Facebook* [2017] SCC 33.
12. *Global Excellence Comm. Ltd v Duke* [2007] 16 NWLR (pt. 1059) 43
13. *Green v SCL Group Ltd and others* [2019] EWHC 954 (Ch).
14. *Heard v. Becton* 440 F.Supp. 3d 960 (2020).
15. *Ifezue v. Mbadugha* [1984] 1 SCNLR 427
16. *In re Toysmart.com Inc. LLC*, No. 00–13995 (Bankr. D. Mass., August 2000).
17. *Jones v. Krok* 1996 (1) SA 504 (South Africa).
18. *Lignes Aeriennes Congolese vs. Air Atlantic Nigeria Ltd* (2006) 2 NWLR (Pt.963) 49.
19. *London Oil and Gas Ltd (In Administration)* [2019] EWHC 3675.
20. Milman, D. (1981). Receivers as agents. *Modern Law Review, 44(6),* 658-671.
21. *Mzumacharo v. Osman's Garage* [1978–80] 9 MLR 68.
22. *Nika Fishing Company Ltd v Lavina Corporation* (2008) 16 NWLR 509.

23. *Nika Fishing Company Ltd v Lavina Corporation* (2008) 16 NWLR 509.
24. Ojikutu *v Agbonmagbe Bank Ltd* (now known as Wema Bank Plc) [1996] 2 Afr LR (comm) 433
25. *Ojokwu v Military Governor of Lagos State* (1986) All NLR 233
26. *Okumagba v. Egbe* [1965] 1 All NLR 62
27. *Re Southern Pacific Personal Loans Ltd* [2013] EWHC 2485 (Ch).
28. *Re Spectrum Plus Ltd* [2005] UKHL 41
29. *Secretary of State for Trade and Industry v Deverell* [2001] Ch. 340.
30. Suit No FHC/L//CP/469/2014: *Access Bank Plc v. Akingbola* (Unreported, delivered on 17 November 2014)
31. UK DPA 1988.
32. *Union Bank Nigeria Plc v Ayodara Sons (Nig) limited* (2007) 13 NWLR (pt.1052) 567
West African Breweries Ltd v Savannah Ventured Ltd (2002) LPELR-3475 (SC).