Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

Nigeria: Law & Practice

Ijeoma Uju, Oghomwen Akpaibor, Tomisin Olanrewaju and Victoria Oloni
Templars

practiceguides.chambers.com

NIGERIA

Law and Practice

Contributed by:
Ijeoma Uju, Oghomwen Akpaibor, Tomisin Olanrewaju and Victoria Oloni
Templars see p.22

Contents

1. Metaverse

1.1 Laws and Regulations

Regulating the Metaverse

Nigeria currently does not have any specific laws or regulations on the metaverse. However, as technology advances and the practical uses of the metaverse expand, it is highly probable that new legal and regulatory issues will arise and trigger some legislative response to address those nuanced features of the metaverse. Businesses will need to navigate questions around jurisdiction and conflicts of law, which as of today are yet to be satisfactorily resolved even for the current internet.

Over the past 30 years, nations with significant internet usage (including Nigeria) have developed or are in the process of developing new regulations in emerging sectors such as e-commerce, technologically based crimes, consumer rights for digital content, and the liability framework for internet service providers, among others. Despite this, Nigeria is yet to develop a specialised set of rules or guiding principles for the metaverse. Certain provisions under extant legislation, however, could be interpreted to extend their application to the metaverse.

Key Legal Considerations

Intellectual property

The metaverse creates new opportunities for intellectual property (IP) rights holders to exploit and monetise their works. While the legal jurisprudence around IP of the metaverse is still at a nascent stage, the current legal framework for intellectual property protection could be expanded to cover certain components of the metaverse.

Under the Nigerian Copyright Act, computer programs are protected as literary works, and this may be broadly construed to accommodate copyright protection in the metaverse. Separately, Nigeria is a signatory to various international treaties on IP and to the WIPO Copyright Treaty, which updates the Berne Convention for the digital age and makes clear that the storage or reproduction of a protected work in digital form on an electronic medium (such as an NFT or a file whose content is visible in the metaverse) constitutes a reproduction that requires the prior consent of the owner of the protected work. It should be noted that although Nigeria is a signatory to and has ratified a number of IP conventions/treaties, most of these are yet to be domesticated into laws in line with the Nigerian Constitution.

Trade mark protection is tied to registration under Nigerian law. Nigeria currently uses the ninth edition of the NICE Classification for its trade mark registrations. Although the NICE Classification does not expressly recognise trade mark protection in the metaverse, such protection may be classified under Class 9 specifically as "recorded and downloadable material". This is attributable to the 3D component of the metaverse, which may be used to create renderings in the metaverse. Trade marks in the metaverse can also be protected under the following classes:

- Class 35 – provision of advertising services via the internet;
- Class 36 – provision of financial services via the internet;
- Class 38 – telecommunications services, chat room services, portal services, email services, providing user access to the internet, radio and television broadcasting; and
- Class 42 – protection for marks involving scientific and technological services and the creation, maintenance and hosting of websites.

Another important aspect of IP protection in the metaverse is patents. To the extent that the component features of the metaverse meet the eligibility requirements under the Patents and Designs Act, they should be eligible for patent protection. To be eligible for patent protection under the Patents and Designs Act, the invention for which an application is filed must be new, result from inventive activity and be capable of industrial application.

Data protection and cybersecurity

Along with its tremendous growth potential, the metaverse raises serious privacy and data protection concerns, particularly regarding jurisdiction, consent, sensitive personal data, etc.

The Nigerian Data Protection Regulation (NDPR) is the primary law regulating data protection in Nigeria. The NDPR provides strict guidelines that regulate the use, processing and transfer of personal data of persons resident in Nigeria and Nigerian citizens resident abroad.

The NDPR could arguably apply to the metaverse, as could the Draft Data Protection Bill 2022. However, given the novel nature of the metaverse, to ensure that users' rights are protected, the provisions of these laws may need to be revisited. In the interim, companies that operate metaverse platforms and other parties must adhere to various standards before handling personal data belonging to users. These standards include identifying and documenting the lawful basis for processing data (in the case of sensitive data, explicit consent), disclosing the reason for data collection, the type of data collected and the intended use of the data. These companies are also required to report data breaches and file audit reports where applicable.

The metaverse also raises cybersecurity concerns, including in regard to financial fraud, identity theft, security breaches, virtual/augmented/mixed/extended reality threats, and social engineering. In this respect, metaverse platforms will be required to comply with the Cybercrimes (Prohibition and Prevention) Act (CPPA) 2015. Under the CPPA, metaverse platforms are required to keep all traffic data and subscriber information as may be prescribed by the relevant authority for a period of two years. In addition, any person or institution who operates a computer system or a network, whether public or private, must immediately inform the National Computer Emergency Response Team (CERT) Co-ordination Centre of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that the National CERT may take the necessary measures to tackle such issues.

2. Digital Economy

2.1 Key Challenges

The Nigerian Communications Act 2003

The Nigerian Communications Act 2003 (NCA) is the principal law for the regulation of telecommunications services in Nigeria. The Act establishes the Nigerian Communications Commission (NCC) which is the primary telecommunications regulator in Nigeria. Under the Act, the NCC has the authority to make subsidiary legislation by way of regulations, guidelines, etc, to regulate the provision of communications services (including communication of things) in Nigeria.

The NCA provides that anyone who intends to operate a communications system or facility or to provide a communications service must have been authorised and licensed by the NCC or have been exempted from such requirements.

A separate licence is usually required for each type of telecommunications activity, although it is also possible for several activities to be undertaken under a single licence.

The NCC provides two general categories of licence – individual licences and class licences. Individual licences are typically bespoke licences where the terms and conditions upon which the licence is granted are specific to the activity undertaken by the licence holder; whereas for class licences, the terms and conditions upon which the licence is granted are common across all licensees.

The Nigerian Data Protection Regulation 2019

The Nigerian Data Protection Regulation 2019 (NDPR) is the principal data privacy law in Nigeria, with the core objective of safeguarding the privacy rights of natural persons residing in Nigeria or citizens of Nigeria residing outside the country in tune with international best practices.

As an improvement to the provisions of the NDPR, the Data Protection Bill 2022 (DPB) is being considered by the national legislature. The DPB designates the data freedom and data rights of data subjects as fundamental human rights, and seeks to protect these rights through technological and organisational measures.

The National Digital Economy Policy and Strategy

The National Digital Economy Policy and Strategy (NDEPS) is a national strategy plan developed by the Federal Ministry of Communications and Digital Economy. The policy document sets out a ten-year plan within which digital technologies would be adopted for the stimulation of growth in all sectors of the economy. A core objective of the NDEPS is that Nigeria achieve 95% digital literacy within the next ten years.

The Advertising Regulatory Council of Nigeria Act 2022

The Advertising Regulatory Council of Nigeria (ARCON) Act 2022 establishes a regulatory framework for the Nigerian advertising and marketing communications industry for the purpose of ensuring that Nigerians are only exposed to pre-approved content. The ARCON Act establishes the Advertising Regulatory Council of Nigeria (ARCON), which is empowered to formulate policies on all activities relating to advertising, advertisements and marketing communications in Nigeria. From this, the ARCON has set out the following policies:

- from December 2022, brand owners, digital agencies, secondary digital media space owners (such as bloggers and influencers) and other advertising stakeholders in the digital and online media space in Nigeria are required to obtain pre-exposure approval from the ARCON in respect of all advertisements, advertising and marketing communications; and
- from January 2023, all advertising, advertisement and marketing communications materials directed at the Nigerian market are required to achieve a minimum of 75% cumulative local content.

The National Information Technology Development Agency Act 2007

The National Information Technology Development Agency Act 2007 establishes the National Information Technology Development Agency (NITDA), an agency which operates under the supervision of the Federal Ministry of Communications and Digital Economy. The NITDA is at the forefront of efforts for the promotion and facilitation of the digital economy in Nigeria, as it has demonstrated through the proposal of guide-

lines, frameworks and regulations to enhance this economy.

The Cybercrimes (Prohibition and Prevention) Act 2015

The Cybercrimes (Prohibition and Prevention) Act 2015 (CPPA) creates an effective and comprehensive regulatory framework in Nigeria for the promotion of cybersecurity and the protection of Nigerians in the cyberspace. In line with global best practices, the CPPA criminalises a plethora of activities such as identity theft, hacking, cyberstalking, bullying and pornography, among others, being acts which are peculiar to the cyberspace and which have the capacity to fetter the thriving digital economy in Nigeria.

Importantly, the Act declares the offences it creates as extraditable. In view of the borderless nature of cybercrimes, the CPPA sets up a regulatory regime within which the Attorney General of the Federation may request or receive assistance from any agency or authority of a foreign state in the investigation or prosecution of offences created under the Act. Alternatively, the Attorney General of the Federation may authorise or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding to or prosecuting any offence created by the Act.

The Nigerian Copyright Act

The digital economy has introduced unprecedented ease in the creation and publication of digital and creative works. This continuous digitalisation of the Nigerian economy has brought to fore the inadequacy of the Nigerian Copyright Act, which does not anticipate most of the recent technological innovations.

In view of this, a Copyright Bill with more expansive provisions was proposed in 2021, and is expected to cater more appropriately to the demands of the digital economy. Among other provisions, the Bill provides that the owner of copyright in online content may issue a notice of infringement to the relevant service provider with a request that the service provider take down or disable access to any infringing content hosted on its system. In this regard, the service provider has an obligation to take down or disable access to the infringing content where the alleged infringer or subscriber fails to provide any justification for the continued hosting of the content complained of.

The Securities and Exchange Commission's Rules on Issuance, Offering Platforms and Custody of Digital Assets

Digital and/or virtual assets, which include cryptocurrencies such as Bitcoin, form an intrinsic part of the digital economy.

While there is still uncertainty as to the manner in which virtual assets should be regulated, many advanced countries have adopted a progressive and liberal approach while the specifics of the relevant laws are thought through and firmed up. The Nigerian Securities and Exchange Commission (SEC) has adopted a similar approach by assuming regulatory authority over virtual assets which it classifies as securities. In the same vein, the SEC has rolled out a body of rules on the issuance, offering and custody of digital assets in Nigeria (the "Rules").

The Rules contain more specific rules on:

- the issuance of digital assets as securities, targeted at all issuers of digital assets seeking to raise capital through digital assets offerings;

- the registration requirements and procedures for digital assets offering platforms and digital assets custodians; and
- specific rules targeted at virtual assets service providers.

Guidelines for Nigerian Content Development in Information and Communication Technology

Local content development guidelines were issued by the NITDA for the purpose of boosting local participation in the information and communication technology (ICT) industry in Nigeria and, consequently, gearing up the ICT industry to compete globally. In view of its core objectives, the guidelines contain provisions which support the transfer of technology into Nigeria in efforts to build local capacity within the industry.

Companies Income Tax (Significant Economic Presence) Order 2020

The digital economy is here to stay, and companies rendering digital services have established their presence in Nigeria now more than ever. Accordingly, the Finance Act 2019 and subsequently the Finance Act 2021 provide for the taxation of companies rendering digital services in Nigeria where they are established as having significant economic presence in Nigeria. In determining taxable businesses in Nigeria, the Companies Income Tax (Significant Economic Presence) Order 2020 focuses on economic substance as opposed to traditional establishment.

A foreign company is said to have significant economic presence in Nigeria in any accounting year where it earns any income or receives any payment from a person resident in Nigeria or a fixed base or agent of a company, other than a Nigerian company, in Nigeria, and such foreign company is taxable in the case of the following.

- It derives NGN25 million (annual gross turnover or its equivalent in other currencies from any of, or a combination of, the following:
  (a) streaming or downloading services of digital content, including but not limited to movies, videos, music, applications, games and e-books to any person in Nigeria;
  (b) transmission of data collected about Nigerian users which has been generated from such users' activities on a digital interface including websites or mobile applications;
  (c) provision of goods or services directly or indirectly through a digital platform to Nigeria – in this regard, the activities carried out by connected persons in the relevant accounting year shall be aggregated; or
  (d) the provision of intermediation services through a digital platform, website or other online application that links suppliers and customers in Nigeria.
- It uses a Nigerian domain name (ie, ".ng") or registers a website address in Nigeria.
- It has a purposeful and sustained interaction with persons in Nigeria by customising its digital page or platform to target persons in Nigeria, including reflecting the prices of its products or services in Nigerian currency or providing options for billing or payment in Nigerian currency.

The Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries

The Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries (the "Code") sets out best practices and expectations required of certain digital platforms to combat online harm such as disinformation/misinformation and to make the digital ecosystem safer for Nigerians. Platforms are classified

as either interactive computer service platforms (ICSPs) or internet intermediaries (IIs) (collectively referred to as "Platform Providers") both of which are subject to the same compliance obligations. The Code defines ICSPs as electronic mediums or sites where services are provided by means of a computer resource for remuneration and on demand, and where users create, upload, share, disseminate, modify or access information, including websites that provide reviews and gaming platforms. The definition of IIs includes social media operators, websites, blogs, media sharing websites, online discussion forums, streaming platforms, and other similarly oriented intermediaries where services are provided, transactions are conducted and where users can create, read, engage, upload, share, disseminate, modify or access information.

The Code further prescribes obligatory provisions that Platform Providers are required to comply with, including:

- takedown requirements (within 48 hours) for unlawful content even without a court order (upon receiving substantiated notice from an authorised government agency);
- takedown requirements (as soon as is reasonably practicable) for unlawful content (upon receiving substantiated notice from a user to remove, disable or block access to non-consensual content that exposes a person's private information);
- disclosing the identity of individuals that are the source of certain unlawful or harmful content further to a court order; and
- filing annual compliance reports with the NITDA.

The NITDA Bill

As previously mentioned, the NITDA is at the forefront of efforts for the promotion and facilitation of the digital economy in Nigeria. To improve the efficiency of the NITDA in the regulation of the digital economy, a bill has been introduced to "repeal the National Information Technology Development Agency Act No 28, 2007 and enact the NITDA Act to provide for the administration, implementation and regulation of information technology systems and practices, as well as digital economy, in Nigeria and for related matters (2022)". This legislative process is an attempt to keep the NITDA Act up-to-date with the current realities in the Nigerian digital economy space.

Key Legal Challenges in Nigeria in Relation to the Digital Economy

Although the digital economy in Nigeria has experienced significant growth in the last few years, it is still beleaguered by certain challenges, such as the following.

Archaic laws and systems

Despite the efforts of the NITDA in facilitating and improving the digital economy in Nigeria, subsistent laws are still catching up and are unable to adequately cater to the unique legal problems that characterise the digital economy.

The digital economy relies very heavily on IP protection. However, Nigerian IP laws are not comprehensive enough and do not provide adequate protection that reflects current global realities. In addition, the systems and mechanisms for the registration and enforcement of IP in Nigeria are not progressive. Filings for IP registrations are mostly manual and protracted. The process for the enforcement of infringed IP rights is also challenging due to the slow pace of the judicial process in Nigeria.

Lack of regulatory co-ordination
The approach of the SEC to the regulation of digital assets is progressive and liberal. As previously discussed, the SEC has set out a regulatory regime for the regulation of digital assets and the registration of all digital asset exchanges, offering platforms and custodians. The Central Bank of Nigeria (CBN) has, however, taken a stricter approach by restricting the access of digital assets exchanges to the Nigerian banking system, an effect which renders SEC rules impracticable.

Digital skills knowledge gap
In Nigeria, the skills and capabilities required to explore various digital products and innovations are significantly limited and only concentrated in a small segment of the populace. This, among other factors, is a result of lack of good-quality education and of inadequate digital skills training programmes, which are essential for building such skills and capabilities.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Regulatory Landscape for Cloud and Edge Computing

Governmental and regulatory bodies in Nigeria have increased their attention on the TMT industry over the past few years in the hope of creating legal precedents that might aid in the development of a strong regulatory framework for governance. In furtherance of this objective, the Nigeria Cloud Computing Policy (the "Cloud Policy") was issued. The goal of the Cloud Policy is to ensure a 30% increase in adoption of cloud computing by 2024 among FPIs and SMEs that provide cloud services to the government. The Cloud Policy also targets a 35% growth in cloud computing investments by 2024, and recognises three basic kinds of cloud computing service offerings or cloud-based service models:

- Software as a Service (SaaS);
- Platform as a Service (PaaS); and
- Infrastructure as a Service (IaaS).

The Cloud Policy is applicable to all public institutions, at the federal, state and local government levels. It also applies to all corporations fully or partially owned by the federal government in Nigeria, as data generated by these institutions is regarded as "government data". By extension, the Cloud Policy also encourages the adoption of cloud services by SMEs to ensure they are able to provide quality, reliable and secure services to the public sector.

The Cloud Policy was developed by the NITDA, to promote a "Cloud First Policy" to federal public institutions (FPIs) and SMEs as an efficient way of acquiring and deploying computing resources for better and improved quality of digital services. The Cloud First Policy refers to the Nigerian government's strong commitment and support for cloud computing service adoption, especially from local cloud service providers, as a first-choice consideration while deploying and accessing computing resources in the public sector and by the SMEs that provide computing services to the public sector.

Developments in the Regulated Sector – Financial Services

The CBN regulates the banking sector and has explored the impact and power of cloud computing on the financial services sector. In 2010, the IT Standards Council of the Central Bank of Nigeria developed the Nigerian Financial Services Industry IT Standards Blueprint (the "Blueprint") to provide a framework and point of

reference for the utilisation of information technology in the Nigerian financial services sector. The Blueprint was issued in 2014 and revised in 2019. It recognises cloud computing as one of the emerging trends in digital technology, highlights the positive implications and the risks of adopting cloud computing, and provides for minimum standards for deploying cloud computing in the financial services sector.

Data Protection and Cloud Computing

One of the key issues of cloud computing is data protection and privacy. Cloud computing poses risks to personal data in a number of ways, including through unauthorised disclosure or access, malicious activities targeting the cloud service provider (eg, hacking or viruses) and poor security practices.

A key data protection concern in cloud computing is the territorial nature of data protection laws vis-à-vis the global nature of cloud services. Data protection laws are typically applied based on the physical location of personal data – ie, where personal data is collected, processed, stored, used, etc. In a distributed system, this can be difficult to determine and control. To cure this mischief, the Cloud Policy provides that although cloud information may be processed or stored in jurisdictions with privacy and information protection laws different from those in Nigeria, government agencies must do so in line with requirements of the NDPR and any other content regulation. Under the Cloud Policy, routine government business data (data of moderate sensitivity) and secret, sensitive government and citizen data are required to reside primarily in a cloud framework within the Nigerian territorial boundary, while classified or national security information must reside only on the premises of public institutions or collocated in a cloud within the Nigerian territorial boundary.

However, as highlighted above, the Cloud Policy has a limited scope of application and does not bind all persons. The NDPR, on the other hand, has general application and can be broadly interpreted and applied. Under the NDPR, the user of cloud services will most likely be classified as a data controller if they determine the purposes for which, and the manner in which, the personal data is being processed. The cloud service provider will be classified as the data processor. Therefore, persons who store or process personal data in the cloud and cloud service providers are required to comply with the NDPR.

To the extent that data controllers choose to store personal data with cloud services located outside Nigeria, they will be required to comply with the transfer of personal data provisions of the NDPR, among other numerous compliance obligations. Under the NDPR, transfer of personal data to a foreign country can only take place:

- after a decision by the NITDA or Attorney General as to the adequacy of safeguards in the foreign country;
- where as regards the transfer of data within a group of companies or an affiliate company, standard contractual clauses (SCCs) or binding corporate rules (BCRs) adopted by the NITDA or the specific industry are in place; or
- where there is verifiable documentation of one of the exceptions under the NDPR.

Another point of convergence between cloud computing and data protection is the requirement under both the Cloud Policy and the NDPR to ensure timely reporting of data breaches to the NITDA. The Cloud Policy mandates cloud service providers to report breaches immediately as they become aware of them. A similar requirement under the NDPR mandates con-

trollers and processors to report data breaches within 72 hours of knowledge of the breach.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Regulatory Landscape for Artificial Intelligence and Big Data

There is currently no legal/regulatory framework specifically dedicated to artificial intelligence (AI) in Nigeria. In 2022, the NITDA made a call for contributions to the National Artificial Intelligence Policy (NAIP). According to the call for applications, the policy is being developed to create a framework for the planning, research, development, standardisation, application, coordination, monitoring, evaluation and regulation of IT practices, activities and systems in Nigeria.

As part of its digital technology drive, the federal government developed the National Digital Economy Policy and Strategy (NDEPS) (2020–2030) to reposition the Nigerian economy to take advantage of the numerous opportunities that digital technologies provide. The NDEPS document in based on the Federal Ministry of Communications and Digital Economy (FMoCDE) eight pillars for the acceleration of the national digital economy for a digital Nigeria. The seventh pillar is digital society and technologies, which focuses on the introduction of an emerging technologies programme that will deal with AI and other emerging technologies.

Notwithstanding the absence of an AI strategy, Nigeria leads the African continent in the area of AI research and development, being the first country on the continent to establish a dedicated government institution to promote the research and development of AI systems in Nigeria. In November 2020, the Honourable Minister of the FMoCDE commissioned the National Centre for AI and Robotics (NCAIR), a state-of-the-art facility, along with its modern digital fabrication laboratory (FabLab). In accordance with the NDEPS, the NCAIR was established as a digital innovation and research facility that focuses on AI, robotics and drones, the internet of things, and other new technologies.

The building of a thriving ecosystem for innovation-driven entrepreneurship (IDE), job creation, and national development is another goal of the NCAIR. Since its establishment, the NCAIR has introduced various programmes including SB4Kids (a programme aimed at enabling young children to be conversant with emerging technologies like 3D design, coding, VR and digital communication around the world), NCAIR Project Drive and digital skills training.

Another AI initiative of the federal government was the partnership between the FMoCDE and IBM in January 2020 to provide Nigerians with over 280 hours of free learning and over 85 courses on key emerging technologies such as AI and Blockchain.

In the financial services sector, the Blueprint also recognises big data and AI as emerging trends in digital technology. The Blueprint also highlights the positive implications and the risks of adopting these emerging technologies, and provides for minimum standards for their deployment in the financial services sector.

Key Challenges

The absence of a formal legal or regulatory framework means that the creation and application of AI, machine learning and big data have mainly been left to industry practices.

Intellectual property

Nigerian IP laws do not consider instances in which an AI creation such as AI-generated computer codes would be protected, or in which AI could be granted any IP rights. The Copyright Act attaches the idea of authorship to individuals (natural persons), and eligibility for copyright protection to both individuals who are citizens of or are domiciled in Nigeria and to body corporates established by or under the laws of Nigeria. Under the Patents and Designs Act, the right to a patent in respect of an invention is vested in the statutory inventor, the person (individual or corporate body) who, whether or not they are the true inventor, is the first to file.

Data protection

In the area of data protection, machine learning (which is a subset of AI) involves the collection of increasing amounts of data and large-scale monitoring of human behaviour, which presents privacy and data protection challenges. Under the NDPR, data controllers and data administrators are required to conduct data protection impact assessments (DPIAs) where they intend to embark on a project that would involve the intense use of personal data. The Nigerian data protection regulator, the Nigerian Data Protection Bureau (NDPB), is empowered to request the submission of a DPIA where the processing activities are deemed to involve high impact on data subjects, including activities involving evaluation or scoring (profiling) and systematic monitoring, which are all important elements of AI.

Another important area of intersection between data protection and AI is automated decision-making. Under the NDPR, in addition to the requirement to conduct a DPIA, data controllers are also required to obtain the consent of data subjects prior to deploying automated decision-making algorithms of this nature. Data subjects also have a right to data portability (the right to receive and request the transfer of personal data concerning them from data controllers, to obtain their personal data from the data controller in a structured medium, and to have this data transmitted across data controllers and platforms).

Human rights

In relation to human rights, AI has the potential to negatively affect a wide range of human rights, including the right to privacy (eg, large-scale monitoring of human behaviour) and the right to freedom of expression (eg, deployment of AI in content moderation). In the absence of AI-related strategies, regulations or case law, it is difficult to determine how AI-related human rights infringements will be determined in Nigeria.

Liability

The deployment of AI also raises questions around legal liability for AI computer systems. Nigerian law does not recognise AI as a legal person, which means that AI may not be held personally liable for damage it causes. The question of who is liable for the harm that results from the actions of AI logically emerges. It is safe to conclude that Nigerian liability laws will need to change to ensure that AI and big data are not utilised as a loophole by organisations to avoid liability. To mitigate this risk, parties to an AI service agreement must carefully consider how to allocate liability for the AI's functionality ahead of entering such agreement.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Regulatory Landscape for the Internet of Things (IoT)

Presently, there is no law in Nigeria that specifically relates to or regulates the IoT. However, there are laws and regulations that are broad enough to apply to IoT projects as well as sector-specific guidelines that govern the IoT. Examples of these laws, rules and regulations are listed below.

Telecommunications

Under the NCA, a "communication" is defined as any communication, whether between persons and persons, things and things, or persons and things, in the form of sound, data, text, visual images, signals or any other form or any combination of these forms. This brings IoT technology under the regulatory scope of the NCC. The NCA sets out a broad licensing and regulatory framework for telecommunications and, in the absence of explicitly stated exemptions, the jurisdiction of the NCC extends to the licensing of IoT projects. Therefore, as appropriate, such IoT projects must be carried out in compliance with the general requirements and any unique conditions of approval under their various NCC-issued licences.

In recent times, the NCC has taken interest in the IoT space. As part of its Strategic Vision Plan (SVP) 2021–2025, the NCC has organised an IoT code camp and hackathon, with a focus on two categories:

- development of IoT solutions for kidnapping and banditry in Nigeria; and
- assistive robotics solutions for effective e-waste management.

In 2022, the NCC also held a stakeholders' consultative forum on emerging technologies, with the theme "Regulatory Roadmap for the IoT Ecosystem in Nigeria". At the event, key officials of the NCC were in agreement that, considering all the challenges and issues surrounding the IoT ecosystem, the regulation of the sector was of essence.

Financial services

The Blueprint recognises the IoT as an emerging trend in digital technology. The Blueprint also highlights the positive implications and the risks of adopting the IoT, and provides for minimum standards for the deployment of the IoT in the financial services sector.

Cybersecurity and data protection

The deployment of an IoT system raises a major cybersecurity challenge, as IoT devices are prolific breeding grounds for cybersecurity attacks such as distributed denial of service (DDoS) attacks.

The primary cybersecurity legislation in Nigeria is the CPPA 2015, which sets out a framework for:

- the protection of critical information infrastructure;
- the promotion of cybersecurity; and
- the protection of computer systems and networks, electronic communications, data and computer programs, IP and privacy rights.

It is the responsibility of every service provider in Nigeria to comply with all the provisions of the CPPA, and failure to comply attracts various levels of sanctions including imprisonment. Although the CPPA does not expressly provide

for the IoT, with the increasing adoption of IoT solutions, service providers in the sector need to pay particular attention to the CPPA as it affects their projects.

With respect to data protection, to the extent that IoT projects involve the processing of personal data, data controllers and data processors must process personal data in compliance with the NDPR and other relevant data protection laws.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Regulatory Landscape for Audio-Visual Media Services

Generally, the provision of audio-visual services in or from Nigeria (eg, TV or radio) is regulated under the National Broadcasting Commission Act (NBCA). Under the NBCA, the National Broadcasting Commission (NBC) may grant licences:

- in the case of a radio station, for frequency modulation, medium wave and short wave;
- in the case of television, for very high frequency and ultra high frequency; and
- for such other broadcast frequencies as the commission may, from time to time, determine.

In the exercise of its power under the NBCA, the NBC has issued the National Broadcasting Code 2016 as amended in 2020 (the "NB Code") to further regulate the broadcasting industry. The NB Code makes it illegal for any person to operate or use any apparatus or premises for transmission of sound or vision by cable, television, radio, satellite or other medium of broadcast from anywhere in Nigeria, unless licensed by the NBC.

The NB Code provides that the NBC can grant broadcast licences in the following categories:

- broadcast – subscription DTH (audio and video);
- cable television subscription;
- community (radio and television);
- networking (radio and television);
- FM radio broadcasting;
- internet broadcasting;
- digital TV content aggregation;
- broadcast signal distribution;
- digital terrestrial (free-to-view) TV;
- direct satellite broadcast;
- mobile/handheld (DVB-H);
- digital subscription television;
- electronic programme guide (EPG); and
- over-the-top (OTT)/video on demand (VOD).

Although the NB Code does not define "internet broadcasting", it defines the internet as "an international computer network through which computer users communicate and exchange information" and "broadcasting" as "transmission of programmes, whether or not encrypted, by radio waves or other means of telecommunication for reception by the public by means of a receiving apparatus." A combined reading of both definitions incorporates video platforms with user-generated content to the extent that these platforms are internet-enabled.

Additionally, the National Broadcasting Commission Act (Amendment) Bill 2019 (the "NBC Bill") is presently being debated in the Nigerian Senate. This bill seeks to expand the NBCA's scope of application to incorporate newer forms of broadcasting into Nigeria's broadcasting regulatory framework. Webcasting, which is defined as

"transmitting over the web/internet" and refers to both online and internet broadcasting, is also included in the scope of the bill. In practice, the NBC Bill would have the effect of requiring a licence from the NBC and regulating the provision of online, digital, internet or OTT broadcasting services in Nigeria under the NBC Act.

Eligibility, Fees and Charges

To provide audio-visual media services, the applicant must submit a licence application to request permission to own, establish or operate a radio, sound, television, cable or satellite station. Based on information specified on the NBC's website, the application must be addressed to the Director General of the NBC. For each application, there is an application form fee of NGN50,000. The applicant must satisfy the following conditions:

- be a body corporate registered under the Companies and Allied Matters Act (CAMA) or a station owned, established or operated by the federal, state or local government;
- demonstrate to the satisfaction of the NBC that it is not applying on behalf of any foreign interest;
- comply with the objectives of the National Mass Communications Policy as applicable to the electronic media (that is, radio and television); and
- give an undertaking that the licensed station shall be used to promote national interest, unity and cohesion and that it shall not be used to offend religious sensibilities or ethnicity, or to promote sectionalism, hatred and disaffection among the peoples of Nigeria.

An application must be accompanied by the following:

- a certificate of incorporation;
- a certified copy of the articles and memorandum of association;
- a project study including the engineering design of the system; and
- evidence of the undertaking required under Section 9(d) of the NBCA.

It is important to note that religious organisations and political parties are disqualified from obtaining licences under the NBCA.

After the licence is granted, the applicant would be required to pay the licence fee for an initial term of five years. Subject to renewal, the licence fee for an initial term of five years is as follows.

- Category A – any location in the FCT, Lagos and Rivers State:
  (a) radio – NGN20 million;
  (b) open TV – NGN15 million; and
  (c) cable TV – NGN10 million.
- Category B – any location in all other states:
  (a) radio – NGN15 million;
  (b) open TV – NGN11.25 million; and
  (c) cable TV – NGN10 million.
- Public stations – NGN5 million for five years, or NGN1 million per television or radio channel per annum for five years.
- Direct broadcast satellite (single-channel) – NGN10 million for five years.
- Direct-to-home (DTH) (multichannel) – NGN25 million for five years.
- Dealer (wholesaler) – NGN120,000 per annum.
- Importer (wholesaler) – NGN120,000 per annum.
- Retailer – NGN30,000 per annum.
- Others – 2.5% of income.

Renewal Fees

Renewal fees apply as follows.

- Cable – satellite television (MMDS):
  (a) Category A, any location in the FCT, Lagos and Rivers State – NGN5 million for five years; and
  (b) Category B, any location in all other states – NGN4 million for five years.
- Direct broadcast satellite (single-channel) – NGN10 million for five years.
- Direct-to-home (DTH) (multichannel) – NGN50 million for five years.

NITDA Code of Practice

Video platforms with user-generated content are also required to comply with the NITDA Code of Practice for Interactive Computer Service Platforms (ICSPs) and Internet Intermediaries (IIs) (the "NITDA Code"), as discussed in **2.1 Key Challenges**.

In order to counteract online harm such as misinformation and/or disinformation, and to guarantee a secure digital environment in Nigeria, the NITDA Code specifies best practices required of digital platforms – ie, ICSPs and IIs. According to the NITDA Code, ICSPs and IIs are generally prohibited from using or modifying their platforms in a way that could compromise or obstruct the application and/or enforcement of Nigerian law. Other important compliance obligations include the need to remove illegal content within 48 hours of receiving a complaint from an authorised government agency.

Platform providers known as large service platforms (LSPs) are also required by the NITDA Code to incorporate in Nigeria, and to designate a liaison officer to serve as a conduit of contact with the Nigerian government, among other obligations.

According to the NITDA Code, failure to abide by its rules will be seen as a violation of the NITDA Act 2007, as well as of the National Broadcasting Commission (NBC) Act 2004 and the Nigerian Communications Act (NCA) 2003.

Advertising

Audio-visual media platforms providing advertising services will be regulated by the ARCON Act (see **2.1 Key Challenges**). The ARCON Act seeks to provide a regulatory framework for the advertising, marketing and communications industry. It is applicable to "individuals, organisations, body corporates or agencies of the federal, state or local government(s) that engage in, regulate, sponsor or take benefit of advertising services, advertisements and marketing communication services". It also applies to "any person who sponsors or takes benefit of advertising, advertisements or marketing communications services within the provisions of the ARCON Act".

With respect to licensing, the ARCON Act requires that every person or organisation, including foreigners, that intends to practise or carry out advertising, marketing and communications as a business or profession in Nigeria be registered in accordance with the provisions of the ARCON Act. Furthermore, all adverts directed or targeted at the Nigerian market are required to be vetted and approved by the Advertising Standards Panel (ASP) prior to publication. Thus, if the operations of video platforms with user-generated content in Nigeria involve advertising/marketing business or provide advertising services, they would be required to obtain a licence.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Technologies and Services that Fall Within the Scope of the Local Telecommunications Rules

All activities and operations within the Nigerian telecommunications sector fall within the scope of the local telecommunications rules, either directly or by extension. These include:

- the installation of communication masts and towers;
- international cable infrastructure and landing station services;
- internet services;
- infrastructure sharing and colocation services;
- commercial basic radio communications network services;
- electronic directory services;
- the operation of public payphones;
- internet exchange;
- sales and installation of terminal equipment (including mobile cellular phones and HF/VHF/UHF radio, etc);
- repair and maintenance of telecommunications facilities;
- cabling services; and
- the operation of cybercafes.

Pre-marketing Requirements in the Nigerian Telecommunications Industry

The NCC is the principal regulator in the Nigerian telecommunications sector. Anyone who intends to operate a communications system or facility or to provide a communications service must have been authorised and licensed by the NCC, or must have been exempted from such requirements. A separate licence is usually required for each type of telecommunications activity, although it is also possible for several activities to be undertaken under a single licence.

As detailed in **2.1 Key Challenges**, NCC licences are categorised into two categories – individual licences and class licences. Individual licences are typically bespoke licences where the terms and conditions upon which the licence is granted are specific to the activity undertaken by the licence holder; whereas for class licences, the terms and conditions upon which the licence is granted are common across all licensees.

Any person who provides a telecommunications service in Nigeria without a valid licence shall be liable to an administrative fine of NGN5 million, and NGN500,000 for each day that the contravention persists after an order to desist has been issued by the NCC. Relatedly, it is also an offence for a licensee to continue to provide a telecommunications service after the expiry of a licence duly issued by the NCC, and such offence is punishable by an administrative fine equivalent to the initial fee for the relevant licence, and an additional fine of NGN100,000 for each day that the contravention persists after the expiry of the licence.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Now more than ever, technology transfer has become an integral activity in the increasingly digital global economy. For developing countries like Nigeria, technology transfer agreements are important to ensure the lawful absorption and adoption of technologies created in developed countries for the purpose of boosting the economic performance of the relevant developing country.

This notwithstanding, in Nigeria technology transfer comes with its own challenges, which include the following.

Registration Difficulties

Foreign technology transfer agreements are subject to registration requirements under the National Office for Technology Acquisition and Promotion (NOTAP) Act. The effect of not registering a registrable contract is that the parties are restricted from making payment through, or on the authority of, the Central Bank of Nigeria, or a licensed bank in Nigeria. The challenge here is that the registration process with the NOTAP is typically protracted and, in most cases, involves a lot of exchanges between the applicant and the NOTAP regarding the terms of the contract, especially where this has been executed by the parties prior to submission for registration. Other specific application requirements which may pose challenges to the registration process include the following.

- The requirement for certain applications such as trade mark licence agreements to be accompanied by evidence of the registration or pending registration of trade marks. Where such evidence is not available, compliance with this requirement may be a challenge, especially for time-sensitive agreements and projects.
- The requirement that all technology transfer agreements involving projects of and/or by the Nigerian government be mandatorily governed by the Nigerian laws of arbitration, with Nigeria being the seat of arbitration. This requirement poses difficulty, especially for transferors of technology who would prefer that such agreements be governed by other arbitral rules.
- Registration of the relevant contracts with the NOTAP is also cost-intensive as, upon approval of registration, applicants are required to pay a registration fee which varies depending on the value of the underlying contract.

Lack of Funds to Adapt the Transferred Technology to Local Conditions

For efficient use of the transferred technology, it is ideal that the transferee has enough financial capacity to fund the purchase of the technology as well as local research and development for the adaptation and improvement of the transferred technology. However, this is rarely the case in Nigeria as transferees often barely have the required funds for research and development for the adaptation of the technology or to train the relevant members of staff on the workings of the technology.

Lack of Local Technical Know-How

The skills and technical know-how of the recipient in a technology transfer agreement are essential for the valid utilisation and optimal performance of the foreign technology. However, the dearth in sufficient skills and know-how for the efficient adoption and utilisation of foreign technologies is a limiting factor in Nigeria.

Local Legal Framework

Generally, the procurement of technology products and services is subject to the laws of contract. As mentioned previously, the transfer of technology into Nigeria must be done within the context of the local regulatory framework, and as such the following rules and restrictions will apply.

Registration of the technology transfer agreement with the NOTAP

The NOTAP may refuse to register technology agreements:

- where the underlying technology is obsolete;
- where the underlying technology already exists in Nigeria;
- where the price is not commensurate with the value of the underlying technology sought to be transferred; and
- in instances where such transfer of technology imposes limitations on technological research or development by the transferee.

Non-registration of the relevant technology transfer agreement restricts the repatriation of funds (foreign exchange) through the official foreign exchange market. Importantly, technology agreements must be registered with the NOTAP within 60 days of the execution or signing of the contract. Agreements in the following titles and substance are required to be registered:

- technical know-how;
- technical know-how and management services;
- technical services;
- consultancy;
- management services;
- software licence;
- value-added services;
- trade mark licence;
- R&D;
- franchise;
- hotel management agreement; and
- consultancy and technical know-how.

Competition considerations

Competition issues may arise within the context of technology transfer agreements. The Federal Competition and Consumer Protection Act (FCCPA) 2018 and the Abuse of Dominance Regulations 2022 prohibit all such agreements, including technology transfer agreements, which have the effect of stifling competition.

However, where a local organisation occupies a position of dominance or attains a position of dominance in the relevant market by virtue of a technology transfer agreement, the actions of such organisation which stifle competition and/or constitute an abuse of the dominant position would be excused where such actions or conduct are indispensable for the achievement of technological or economic progress in Nigeria. Alternatively, such conduct would be excused where the anti-competitive effects of the abusive conduct are reasonably necessary for the achievement of technological or economic progress.

Data localisation requirements

Parties to a technology transfer agreement which involves personal data must ensure compliance with the localisation requirements of the data privacy laws in Nigeria. These data localisation laws provide specifically for the following:

- all ministries, departments and agencies (MDAs) of the Federal Government of Nigeria are required to host all sovereign data locally on servers within Nigeria;
- all data and information management companies are required to host all sovereign data in Nigeria;
- all network service companies in Nigeria are required to host all subscriber and consumer data in Nigeria;
- all telecommunications companies are required to host all subscriber and consumer data in Nigeria; and
- all companies that produce functional computer devices from component parts brought from other organisations are required to assemble all hardware in Nigeria and maintain fully staffed facilities for that purpose.

Importantly, the localisation laws apply to all MDAs across all tiers and arms of government, private sector institutions, multinationals and individuals to the extent that they process sovereign data.

The Public Procurement Act

The procurement of technology products and services by government or public bodies is regulated by the Public Procurement Act (PPA) 2007. The Act covers procurement of all goods and services by the federal government, public bodies and all entities which derive 35% of the funds appropriated for any type of procurement, from the Federation's share of the Consolidated Revenue Fund. The PPA focuses primarily on ensuring transparency and accountability in all procurement processes by public sector bodies.

Industries Subject to Greater Restrictions

The banking sector

In the context of technology transfer agreements, banks are subject to more restrictions due largely to the need to protect the interests of the public whose funds they deal in. Specifically, fees payable by banks for management or technical support services, which they receive from expatriates, should be tied to the actual costs of the services rendered by the expert and not to the profit or sales of the bank.

A further restriction in this regard is that expatriate staff of banks can only be paid in the local currency – ie, Naira. However, remittance abroad, in foreign currency, can be effected through the Personal Home Remittance.

Nigeria's federal government ministries, departments and agencies (MDAs)

As mentioned above, public sector entities are subject to procurement requirements under the PPA.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The COVID-19 pandemic changed global realities and led to the introduction of digital identity schemes and trust services such as electronic signatures and teleconferences. While there are no specific laws which speak to the legality, permissibility or otherwise of electronic signatures and other digital identity schemes, some major laws have been amended to accommodate these new realities. Examples of these laws, rules and regulations are listed as follows:

- the Companies and Allied Matters Act 2020 recognises the validity of an electronic signature for the authentication of a document or proceeding by a company and further provides that the signature may be by a director, secretary or other authorised officer of the company;
- the Evidence Act 2011 provides that an electronic signature would suffice where the relevant law requires a signature;
- the Nigerian Data Protection Regulation (NDPR) 2019 and the accompanying Implementation Framework recognise and govern the collection, protection, storage and processing of personal data, which is defined broadly and thus includes digital identities and electronic signatures; and
- the CPPA 2015 provides that electronic signatures appended in respect of purchases of goods and any other transactions shall be binding.

Notwithstanding the above, certain transactions and documents cannot be validly concluded and executed using electronic signatures. These

transactions and agreements include the following:

- the creation and execution of wills, and other testamentary documents;
- death certificate;
- birth certificate;
- divorce, marriage, adoption and other related matters;
- the issuance of court orders, notices and official court documents such as affidavits, pleadings, motions and other related judicial documents and instruments;
- any cancellation or termination of utility services;
- any instrument required to accompany any transportation or handling of dangerous materials either solid or liquid in nature; and
- any document ordering the withdrawal of drugs, chemicals and any other material either on the grounds that such items are fake, dangerous to people or the environment, or expired.

Considerations Arising from Trust Services, Electronic Signatures and Digital Identity Schemes

Other than the aforementioned laws, there is presently no specific and comprehensive legal framework governing electronic signatures and trust services in Nigeria. However, by the existing laws referenced above, the following elements are relevant.

Legal liability

Trust services and electronic signatures present varying levels of risks, including the risk that the electronic signature or digital identity is not authentic. Here the current legal position is that whenever the genuine nature of an electronic signature is in question, the burden of proving that the signature does not belong to the purported originator of such electronic signature shall be on the contender. Indeed, for many evidential issues in Nigeria, the general legal position is that he who asserts must prove.

Fundamental rights considerations

While the introduction and general acceptance of electronic signatures and other trust services have brought ease to cross-boundary transactions and communications, the possibility of forgery of electronic signatures and digital identities has raised concerns about the potential breach of the rights of private citizens to their privacy and digital identity.

Although the Constitution of the Federal Republic of Nigeria contains a generic provision for the protection of the privacy of citizens, their correspondence, telephone conversations and telegraphic communications, the NDPR contains a more comprehensive provision safeguarding the rights of natural persons resident in Nigeria to the protection of their personal data, which by its broad definition includes electronic signatures and digital identities.

Data protection

Data protection is a major concern regarding the manner in which electronic signatures are collected, processed and stored by relevant host companies. Considering that electronic signatures validly constitute personal data, it is important that the process of collection, storage and processing in this regard complies with local data processing laws.

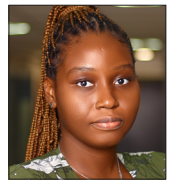
Templars is a full-service commercial law firm with offices in the cosmopolitan cities of Lagos, Abuja, Port Harcourt and Accra. The media, entertainment, technology, and intellectual property (METI) practice at Templars is renowned for the services it provides traversing the full range of issues in the technology sector, including: e-commerce, data protection, intellectual property licensing, patenting and protection; cloud services arrangements; cybersecurity; fintech regulation and compliance; technology licensing; acquisition; international joint ventures in the telecommunications industry; and advice on start-ups. The firm's recent experience includes: advising YouTube on its USD100 million Black Voices Fund, a global racial-justice initiative aimed at supporting black content creators and artists across different countries; advising Apple on the launch of a number of first-to-market products that are connected with its online services (including the online provision of original video-on-demand content via Apple Music); and advising American Tower Corporation (ATC) on its business entry into Nigeria through its USD1.05 billion acquisition of approximately 4,800 tower sites across Nigeria from Bharti Airtel.

Authors

Ijeoma Uju is a partner in Templar's corporate and commercial practice group. She has almost two decades' experience in providing general corporate advisory services to clients, and in advising clients on compliance requirements applicable to the operation of their businesses in the technology ecosystem, regarding data protection, financial technology, cryptocurrency regulations, blockchain, artificial intelligence, tech policy, and start-up/organisational development. In addition to her transaction-specific work, Ijeoma regularly conducts regulatory compliance seminars and workshops for leading Nigerian and multinational tech companies. Ijeoma has also written and published articles on regulatory compliance, corporate governance and business formation in legal journals.

Oghomwen Akpaibor is a managing counsel in Templar's corporate and commercial practice group and METI practice group. She has a wealth of experience in media and technology law, general corporate advisory and general regulatory advisory. Oghomwen manages the government-relations aspects of clients' regulatory compliance engagements. She also advises the various players in the tech ecosystem (locally and internationally) on subject matter-specific queries arising in respect of their businesses, including regarding labour and immigration, intellectual property, anti-corruption and privacy.

Tomisin Olanrewaju is an associate in Templar's finance practice group and METI practice group. She has been admitted to the Nigerian bar and has experience advising on regulatory compliance, data protection and intellectual property. Tomisin provides legal support to Nigerian entities and MNEs to ensure they achieve their business objectives and remain in legal compliance with the requirements of relevant Nigerian authorities, particularly in relation to data protection, corporate restructuring, intellectual property protection, and the establishment of businesses by foreign and indigenous companies.



Victoria Oloni is an associate in Templar's corporate and commercial practice group and METI practice group. Victoria is a Certified Information Privacy Professional (CIPP/E) with the International Association of Privacy Professionals (IAPP), where she also served as the Young Privacy Professional for the 2022 leadership cohort of the IAPP Nigeria Knowledge chapter. Victoria has written and published articles on privacy and data protection, cybersecurity, the digital economy, and general intersections of technology and law.

Templars

Fifth Floor
The Octagon Building
13A, AJ Marinho Drive
Victoria Island
Lagos
Nigeria

Tel: +234 1 270 3982
Fax: +234 1 271 2810
Email: info@templars-law.com
Web: www.templars-law.com

TEMPLARS

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com