OMAPLEX
LAW FIRM

DATA PROTECTION AND INTELLECTUAL PROPERTY:

A GLOBAL APPROACH TO DISSECTING EMERGING LEGAL ISSUES

THE NEED FOR DATA PROTECTION IN THE MODERN WORLD

According to **OECD in 2015,** data is seen as the very infrastructure underlying the modern digital economy.

To succeed in the modern economic environment, businesses and technology models heavily rely on huge amount of data to thrive. Top companies like Facebook, amazon and google, some of the world's digital economy leaders, are leaders in the business world due to their access to immense amount of data from their users which they then apply with their algorithms. it helps keep their market at a remarkably high level.

The questions of who owns the data, who gets access to it and whether data is something that can be owned in the first place is yet to be settled. In the same vein, it leaves us with so many questions on intellectual property rights.

Although there exists bits and pockets of legal frameworks for data, the EU's **General Data Protection Regulation** (GDPR) which came in force in 2018 took centre stage and replaced most existing data laws, particularly Directives 95/46/EC (**the Data Protection Directive**) and 2002/58/EC (the ePrivacy Directive). Other new regimes like the **California Consumer Privacy Act** (CCPA) which became operative on the 1st of January 2020 is also a subject of much discourse.

HOW HAS DATA PRIVACY REGULATORY FRAMEWORKS RECOGNISED INTELLECTUAL PROPERTY RIGHTS?

The question that keeps arising is, how much does these laws recognise Intellectual Property rights?

One thing that is certain is that IP rights are not expressly spelt out in most data protection laws and some may even have counter effect on IP. Under the GDPR for example, right owners wishing to take action against domain name owners whose domains have infringed their trademarks, design or copyright, will find it harder to obtain details of a UK domain name owner allegedly infringing their rights due to the consent provision of the GDPR.

Similarly, the GDPR does not recognize company rights but just personal rights. The European Commission (EC) stated that the rules only apply to personal data about individuals and do not govern data relating to legal entities.

The Nigerian data protection regulation (NDPR) also takes a similar approach to data rights. The NDPR defines a 'data subject' as a person who can be identified directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, economic, cultural or social identity. It also defines personal data as information relating to an identified or identifiable natural person which may be a name, address, photo, email address, bank details, posts on social networking websites, medical information, etc. thus,

Giving the restriction of data subjects to majorly natural persons only, the current data protection regime has left a huge void regarding intellectual property rights.

TRADE SECRET PROTECTION: ARE THEY ENOUGH?

Trade secrets arguably enjoy the most protection under the current data protection laws. **The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)** sets out standard minimum levels of protection of trade secrets as Intellectual Property Rights and provides a definition of the information that can be protected, focusing on these three requirements:

(i) Secrecy,
(ii) Commercial value; and
(iii) Reasonable steps to keep the information secret.

Trade secrets regime in the EU has been recently regulated by **Directive (EU) 2016/943 ("Trade Secrets Directive").** As evinced from **Recital 10 and Article 1 of the Trade Secrets Directive,** the aim of the Directive is not to introduce a full EU trade secrets regime, but rather to reach a partial harmonisation through a minimal standard of protection, leaving room for Member States to provide for more far-reaching protection.

TRADE SECRETS UNDER THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

The CCPA particularly provides an interesting cover for trade secrets. Generally, the CCPA allows California consumers to request that a business disclose the specific pieces of personal information (PI) the business has collected. The consumer also may request that the business delete any PI about the consumer that the business has collected. If a business is able to verify the identity of the consumer making the CCPA request, it must comply with the request unless one of the enumerated exceptions applies. Unexcused failure to do so exposes the business to a civil action by the California Attorney General for injunctive relief and civil penalties of up to $7,500 for each violation.

The question now is, what happens if the personal information covered by the consumer request includes information considered as trade secret data? Given the wide meaning of both PI and trade secrets under the CCPA, a conflict in this regard is inevitable.

Although the CCPA does not provide a clear-cut safe harbor to address this dilemma, a potential argument that may support a decision to withhold trade secret data when responding to a consumer request may arise.

HOW TO DETERMINE THE OWNER OF IP PARTICULARLY IN AI DRIVEN TECHNOLOGIES THAT RELY ON DATA?

Seeing that Artificial Intelligence (AI) is already becoming omnipresent in our everyday life, the development raises broad and multi-disciplinary policy questions, including several aspects of intellectual property (IP). Much like the countries in which they operate, an increasing number of corporations are convinced that AI will be essential to maintaining a leading position in the future.

Determining the owner of an IP right in AI driven technologies are quite complicated. Biometrics, as an AI initiative provides a brilliant case study. The GDPR includes specific provisions for biometric data. In particular, the GDPR covers the processing of biometric data for the purpose of uniquely identifying a natural person. Biometric data is data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

A company that is desirous of collecting the biometric (or other prohibited data) of an EU citizen, the company must be able to demonstrate that it has met an exception to the GDPR's general prohibition. A non-exhaustive list of these exceptions include: that the EU citizen has given explicit consent for a specified purpose for the data; that processing the data is essential to protect the vital interests of the individual and he or she is incapable of giving consent; or that processing the data is necessary for the purposes of preventive or occupational medicine, and subject to the conditions and safeguards referred to in the GDPR.

In addition to meeting one of the exceptions, a company must also comply with data protection requirements and obligations. For example, a company must provide EU citizens with the right to be forgotten, meaning that an individual shall have the right to withdraw his or her consent at any time. This can lead to severe penalties for the company for failure to comply. The question then arises, at the point where consent was yet to be withdrawn, who owned the intellectual property right? If it is the company, do they lose that ownership when the data subject decided they want to be forgotten?

In this regard, it could be argued that ownership of IP rights in big AI resides with the data subjects and only upon certain exceptions can companies use it.

INTELLECTUAL PROPERTY AND ARTIFICIAL INTELLIGENCE: FOCUS ON COPYRIGHTS.

The global technology transition brings into question several fundamental IP concerns. Seeing that most IP laws were written at a time when only natural and human intelligence were contemplated, AI challenges many traditional IP

legal notions such as originality, copying, author, designer, and inventor among others. Arguably, when AI systems are engaged to perform creative or other cognitive tasks, the prevailing humanistic approach to IP is not well suited to protect the generated results.

Let's look at copyrights for example. Under EU and American copyright law, copyright protection applies to the expression in any form of a computer program, provided that the program is original in the sense that it is the author's own intellectual creation. In respect of the criteria to be applied in determining whether a computer program meets the originality requirement, no tests as to the qualitative or aesthetic merits of the program should be applied.

However, ideas, methods and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright. Only expressions of intellectual efforts are protected. In addition, since no registration is neces-sary for copyright protection to arise (with varying exceptions), collection of evidence may sometimes be difficult.

In conclusion therefore, from an economic standpoint, the scope of copyright protection (and other IP protection including trademarks and trade secrets) for an AI system is insufficient. Seeing that copyright will not protect the creativity, skill and inventiveness devoted to the development of the functional concept behind an AI system, it may be recommended not to rely solely on copyright law and data protection laws. The current data regime completely ignores this possible insufficiency. These insufficiencies for the main time are best circumvented via a robust contractual agreement, although it has its inadequacies, especially when dealing with a large number of data subjects.

DATA RIGHTS AND DATABASE RIGHTS: ACHIEVING AN EQUILLIBRIUM BETWEEN DATA RIGHT PROTECTION AND INTELLECTUAL PROPERTY PROTECTION UNDER NIGERIAN LAWS.

On the back of several reports of privacy violations against Facebook, the United States Federal Trade Commission imposed a $5,000,000,000(Five-Billion Dollar) fine on the company in July, 2019. Earlier in January, 2021, social media giants – Twitter, permanently suspended the account of Former American President, Donald Trump for inciting violent protests at the Capitol (the Nation's legislative building) via his tweets on the platform.

What indeed is the nexus between these narratives? Simply put, the former narrative on the fine imposed on Facebook encapsulates the importance placed on the need to protect data rights as contained in databases. The later relays the great extent to which the owner of an intellectual property can exploit his powers (in this instance, it was exercised to outlaw a President from social media). Moving forward, it is without doubt that in several jurisdictions the world over, various laws have been put in place to uphold various rights and more importantly in this discuss – data rights and intellectual property rights.

This paper seeks to open a conversation on the need to ensure that the exercise of database rights by an intellectual property owner, does not infringe on the data rights of others.

DATABASE RIGHTS: MEANING AND PROTECTION UNDER THE NIGERIAN COPYRIGHT LAW

Although no Nigerian legislation defines database rights, in Nigeria, it can be regarded as a literary work eligible for protection under **Section 1, of the Copyright Act, 2004**. For the purposes of clarity however, the definition of a database under the United Kingdom's **Copyright and Rights in Databases Regulations, 1997,** may be adopted. **Regulation 6** of the Regulation defines a database as 'a collection of independent works, data or other materials which are arranged in a systematic or methodical way, and are individually accessible by electronic or other means.

Therefore, in basic terms, a database right refers to the intellectual property right accorded to a person in recognition of the effort put in forming/creating a database.

As earlier stated, these rights are accorded protection under the Copyright Act of Nigeria. Consequently, the owner of a database enjoys the protection of the following rights as a copyright owner:

1. **Economic rights:** These rights aim at safeguarding the financial interests of a copyright owner by conferment of an exclusive right to exploit the work commercially. They consequently provide the following benefits:
    - Enhance the market value of a business by leveraging on the goodwill provided by ownership of IP.
    - A source of earning as they can be licensed/assigned
2. **Moral rights:** These seek to protect the integrity of the author's work as it encapsulates the reputation of a copyright owner. To this end, the law will operate to prevent a copyright owner's work from being used in a manner contrary to the owner's wishes or without his prior approval.

THE STRENGTHS OF THE NIGERIAN DATA PROTECTION REGULATION (NDPR), 2019 IN PROTECTING DATA RIGHTS.

As earlier established, database rights under Nigerian law enjoy the benefit of copyright protection which enable a copyright owner to exploit the benefits therein. However, whilst the law will recognise and afford protection to the ingenuity of an author (copyright owner) who has exerted effort in compiling such a database, such a compilation must be done in a manner that does not infringe on the rights of others. It is indeed in this regard, that the issue of Nigeria's data protection regime comes to fore.

Whilst they exist pockets of industry specific legislations on data protection in Nigeria, **the Nigerian Data Protection Regulation (NDPR), 2019** constitutes the only comprehensive and holistic piece of data protection in Nigeria. The regulation principally seeks to ensure that the processing of the data of Nigerians is carried out lawfully in a manner consistent with the privacy rights of Nigerians.

Since its coming into force, the NDPR has strengthened the nation's data protection framework by ushering in a number of laudable developments as follows:

1. **Enhanced Privacy Rights:** The NDPR most importantly, has articulated the privacy rights of Nigerian citizens guaranteed under **Section 37 of the 1999 Constitution as amended.** In a landmark decision, the Federal High Court in Abuja, in 2019, affirmed the data privacy rights of Nigerians and ordered the Nigerian Information Management Commission to protect the data rights of Nigerians beyond merely having bogus security policies which it had prior to the suit, failed to implement. [See **Incorporated Trustees of Paradigm Initiative for Information Technology (PIIT) & Sarah Solomon-Eseh v National Identity Management Commission (NIMC) & Anor)].**

    Essentially, the NDPR preserves the data rights of Nigerians by requiring all data controllers (organisations processing the data of Nigerians) to ensure that in processing (making use of) the data of Nigerians:
    - consent must be obtained;
    - it must be in the interest of the data subject or in public interest;
    - for the performance of a contract which the data subject is a party to, amongst others.
2. **Commitment to Ensuring Data Protection:** The NDPR also solidifies the commitment of the Nigerian government in ensuring that all cybercrimes and associated threats

linked to breaches in data bases are addressed. **Article 2.6 of the NDPR** places a duty on all data processors to put in place security measures to protect data which amongst other things include setting up firewalls, protection of emailing systems and employing data encryption technologies.

Reports indicating that 588 businesses have filed data audit reports with the National Information Technology Development Agency (NITDA) as at August, 2020, as opposed to a near zero compliance level before the inception of the NDPR is indeed a silver lining in the quest for data protection in Nigeria.

3. **Expansion of Nigeria's Job and Wealth Creation Potential:**
In Nigeria, the National Information and Technology Development Agency (NITDA) licenses Data Protection Compliance Officers (DPCOs) to not only provide data audit services, but to provide general training on data compliance which obviously comes at a cost to data controllers patronizing such DPCOs thereby fuelling wealth and job creation. In a similar vein, an avenue is created for the government to generate funds through licensing fees for DPCOs and applicable fines for breach of data rights.

In capturing the wealth and job creation potential available via the NDPR, Isa Pantami, Nigeria's Minister of Communications and Digital Economy in an interview in September, 2020, observed succinctly:

> "One of my greatest sources of joy on the Regulation is its job creation potential. Over 1.5 million businesses and non-governmental organisations would need to file Data Audit Reports on or before March 15 every year. Each of these reports must bear a Verification Statement, sign and seal of a licensed DPCO. If each DPCO provides service for an average of 50 Data Controllers, we would need over 300,000 professionals to meet this need." **[Available On: Premium Times, 'The Huge Prospects of Nigeria's Data Protection Regulation 2019, By Isa Ali Ibrahim Pantami' (Premium Times, 16 April 2019) accessed 7th September 2020].**

THE CHALLENGES OF THE NDPR IN PROTECTING DATA RIGHTS

Although, the provisions of the NDPR are laudable and set the tone for much potential in Nigeria's efforts at achieving a world class data protection status in which all data rights are protected, nonetheless, there exist few challenges:

1. **Scope:** The NDPR only guarantees data protection for Nigerians in Nigeria **(Article 1.2 NDPR)**. Consequently, the regulation does not extend protection to non-residents. In contrast, the General Data Protection Regulations, GDPR (applicable to countries in the European Union) has extra-territorial provisions governing such outsourcing needs. **See Article 3 of the GDPR.**

2. **The Status of the NDPR:** It has been submitted, that the efficacy of the provisions of the NDPR is watered down as it is not a legislation. Consequently, in the event of a conflict between the regulation and statute, the later shall prevail. For example, the provisions of the **Cyber Crimes Act, 2015,** on the release of personal data pursuant to Court orders and statutory fines, will take precedence over the NDPR. In sharp contrast however, the provisions of the General Data Protection Regulations (applicable to the European Union) is a substantive legislation of parliament.

3. **Deterrence Measures:** In light of the serious damage privacy infringement may occasion and the huge profits earned by infringing companies doing business, it is observed that the penalty imposed by the regulations should be made weightier. **Article 2.10 of the NDPR** imposes a fine of 2% on domestic gross annual revenue or 20 Million Naira, whichever is greater on companies (handling above 10,000 data subjects) in breach of the regulation. With

the combined values of the top tech companies Facebook, Netflix, Google and Amazon placed at 2.3 trillion dollars in 2018, the 20 Million Naira fine under the NDPR should be increased to deter violations.

THE WAY FORWARD: RECOMMENDATIONS

Nigeria's quest to achieving a compliant data protection status capable of securing database rights and indeed all other ancillary intellectual property rights cannot be achieved overnight. Nonetheless, the above issues discussed are cardinal and must be tackled as a first step:

1. **Need to Improve Capacity:** It is germane that NITDA as the principal body for data protection in Nigeria consolidates on its successes and takes steps to improve further. Whilst the agency must be applauded for opening investigations into a number of alleged data breaches, notably breaches by **TrueCaller, Surebet247 and the Lagos Inland Revenue Service**, the absence of sanctions or the non-publicity of same must be addressed. The agency must begin to impose sanctions on defaulting organisations. The NITDA should take a cue from countries within the European Union which have imposed a minimum **€114,000,000** in fines since the inception of the GDPR in 2016.

2. **Scope of the Act:** The definition of data under the NDPR must be reviewed to explicitly include non-electronic data. This will ensure that data not electronically stored is also afforded protection. Such an amendment must also include an obligation on data controllers to inform data subjects of data breaches thus affording such subjects the opportunity to take extra precautionary measures and further ultimately bring the NDPR into conformity with international best practices on data protection.

3. **Increased Licensing Capacity:** Lastly, it is firmly believed that by licensing more competent data compliance officers, market forces would operate to dictate cost of data audit reports and associated due diligence on data compliance. This would remedy the effect of the current regime were high compliance costs currently cripple the efforts of data controllers at achieving compliance.

4. **Passage of the Digital Rights Bill:** The Nigerian Government must take steps in ensuring that the Digital Rights Bill is passed into law. Following President Buhari's non-assent to the Bill, the National Assembly must take the bull by the horn to ensure passage by addressing the reasons for the President's decline of assent (for e.g. the failure to address specific digital rights extensively). The Act, if passed will not only crystallise the data rights of Nigerians it would also allay all fears pertaining to the genuineness of Nigeria's data protection regime.

CONCLUSION

This Legal content appraises the role of the intercourse between Data protection and intellectual property rights from a global and ever evolving purview, while succinctly addressing the need for an improvement in the Global and Nigeria's data protection framework with a view to ultimately ensure that a balance is achieved in the protection of data rights and database rights.

OMAPLEX
LAW FIRM

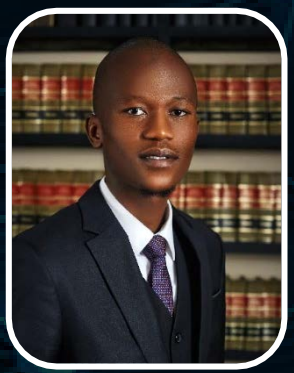
Author

O. M. Atoyebi, SAN
Managing Partner, Omaplex Law Firm
atoyebi@omaplex.com.ng

Contributors

Caleb Echoga
Member, Data & Security Privacy Team
Omaplex Law Firm
caleb.echoga@omaplex.com.ng

Isaac Adeyanju
Member, Technology Law Team
Omaplex Law Firm
isaac.adeyanju@omaplex.com.ng



Ibrahim Wali
Member, FinTech Team
Omaplex Law Firm
Ibrahim.wali@omaplex.com.ng