ALLEN & MARYLEBONE
LAW FIRM

INCREASING DATA PRIVACY REGULATIONS: A CATALYST OR BARRIER TO TECHNOLOGICAL INNOVATIONS?

The unmistakable adage making the rounds in the 21st century is that data is the new oil of the internet or the oil of the digital era;[1]whether this is true or false is a debate for another forum. However, just like any commodity of high value, personal data ought to be safeguarded from abuse, misuse, manipulation, theft and unauthorized access. This is where privacy regulation becomes quite crucial to the discussion. Technology has made life easy, affording users the ability to check the status of their home security from smart phones, to start their car with their mobile phone application, and to remotely close or open their garage door anywhere on the planet.[2]Technology is so embedded in our daily lives with both animate and inanimate things connected to the internet. The phrase 'Internet of Things' (IoT)[3] has been touted about as aptly describing this reality. The downside to this seeming easy life is the porous nature of personal data protection and privacy risk involved.

Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) (hereinafter CFRN 1999) provides that the privacy of citizens, their homes, correspondences, telephones conversations and telegraphic communications is guaranteed and protected. Although the constitutional provision is not specific to data protection, one can successfully argue that this could be extended to also include protection of data privacy in the digital age. The right to privacy is recognized by the United Nations (UN) Declaration of Human Rights, European Union (EU) Charter, African Union Charter and the Nigerian Data Protection Act 2023.

Historically, in 1907 the world's first bugging device – the dictograph was invented,[4] while in 1928 a US Supreme Court declared wiretapping private phone calls illegal[5] and after the UN Declaration of Human

[1] Joris Toonders, 'Data is the New Oil of the Digital Economy' (*WIRED NEWS BLOG* 2021) <https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/> accessed 6th September 2021

[2] Marie Helen Maras, 'Internet of Things: Security and Privacy Implications' (2015) 5 (2) IDPL <http://idpl.oxfordjournals.org> accessed 17 February, 2021

[3] **IoT** refers to an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world. OECD, 'The Internet Of Things Seizing The Benefits And Addressing The Challenges; 2016 Ministerial Meeting On The Digital Economy – Background Report' (OECD DIGITAL ECONOMY PAPERS No. 252 OECD Publishing 2016) 4

[4] KPMG, 'Privacy Technology: What's Next? (KPMG International 2021)

[5] Ibid at 11

Rights of 1948 established the Right to Privacy[6], many nations and regional blocs began to take this right seriously. In 1995, the EU adopted the Data Protection Directive setting the pace for other regional blocs in privacy regulation. Unfortunately, in 2013 Edward Snowden[7]made headlines when with the help of wiki leaks he released classified information showing widespread surveillance by Western Intelligence agencies. This incident unleashed an avalanche of questions sparking a global debate about national security versus individual privacy, raising fears that national security would trump individual privacy at any time. In 2016 the European Union (EU) enacted the General Data Protection Regulation (GDPR) 2016 making stringent rules to guarantee privacy of data subjects in processing of their personal data by data controllers.

In Nigeria privacy regulations have always existed all drawing inspiration from chapter four (iv) of 1999 Constitution of the Federal Republic of Nigeria, particularly section 37 afore cited. The Freedom of Information (FOI) Act 2011[8] in its preamble provides that it is: 'An Act to make public records and information more freely available, provide for public access to public records and information, protect public records and information to the extent consistent with the public interest and **the protection of personal privacy,** protect serving public officers from adverse consequences of disclosing certain kinds of official information without authorization and establish procedures for the achievement of those purposes and; for related matters'. From the preamble of the FOI Act 2011, it is clear that the FOI Act 2011 which was set to revolutionize the face of information acquisition and privacy in Nigeria, also sought to regulate privacy of information or data. Section 14 of the FOI Act 2011 went on to exempt production of personal information by providing inter alia that a public institution must deny an application for information that contains personal information. This provision is specifically geared towards privacy regulation. Such disclosure is only subject to the owner's consent[9] or where disclosure is necessary for public interest reasons if the public interest reason for disclosure of such information clearly outweighs the protection of the privacy of the individual to whom such information relates.

The most recent effort at privacy regulation in Nigeria can be seen in the promulgation of the Nigeria Data Protection Regulation (NDPR) 2019 under the auspices and through the instrumentality of the Nigeria

[6] Ibid at 11

[7] He is a former employee and subcontractor of the American Central Intelligence Agency (CIA) who leaked highly classified information from the National Security Agency (NSA) in 2013 revealing widespread surveillance of citizens by the US government.

[8] The Freedom of Information Act was passed into law by the National Assembly on 24th May 2011 and assented to by President Goodluck Jonathan on 28th May 2011.

[9] Section 14 (2) FOI ACT 2011

Information Technology Development Agency (NITDA). The NDPR 2019 draws inspiration from the EU GDPR 2016, UK Data Protection Act 2018 which has already provided the legal framework for privacy regulations in their respective jurisdictions. Article 1.1 of the NDPR 2019 lays out the objectives of the regulation to include; to safeguard the rights of natural persons to data privacy;[10] to foster safe conduct for transactions involving the exchange of personal data;[11] to prevent manipulation of personal data;[12] and to ensure that Nigerian businesses remain competitive in international trade through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practices.[13]The scope of the Regulation is extended to cover transactions intended for the processing of personal data, notwithstanding the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria. The Regulation applies to all Nigerians residing within or outside the country. The governing principle of the regulation includes the collection and processing of personal data in accordance with specific, legitimate and lawful purpose consented to by the data subject. Consequently, consent is mandatory for processing personal data. Other principles such as accuracy of processing, secure storage, and accountability are also guaranteed under the regulation. Anyone who is entrusted with personal data of a data subject or who is in possession of the personal data of a data subject owes a duty of care to the said data subject.[14]

Sometime in June 2023 President Bola Tinubu as one of his first acts signed into law the Nigerian Data Protection Act 2023. The Nigerian Data Protection Act 2023 has the objective to establish the Data Protection Commission charged with the responsibility for the protection of personal data, rights of data subjects, regulation of the processing of personal data and for related matters.[15]This law provides an efficient regulatory framework for the protection of personal data, regulate the processing of information relating to data subjects, and to safeguard their fundamental rights and freedoms as guaranteed under the CFRN ultimately leading to the regulation of privacy. The new Act effectively replaces the Nigerian Data Protection Regulation (NDPR) 2019.

[10] Article 1.1 (a) NDPR 2019

[11] Article 1.1 (b) NDPR 2019

[12] Article 1.1 (c) NDPR 2019

[13] Article 1.1 (d) NDPR 2019

[14] Article 2.1 (2) NDPR 2019

[15] Data Protection Bill 2020

The prevailing tide all over the world from the EU to the Americas is the increase in privacy regulation especially in the light of the Internet of Things (IoT), machine learning, smart devices and robots. Increasing privacy regulation is a catalyst and not a barrier to technology innovation. Reasons for this position include the continuous increase in technology despite privacy regulations enacted in the EU GDPR and other blocs. The increase in regulation has not stemmed the ebb in innovation; therefore it is our opinion that the increase in data privacy protection regulations is a catalyst and not a barrier to technological innovations. The reverse would be disastrous as non-regulation of privacy would lead to an anarchic situation that removes all integrity from the cyberspace.

In recent times, the right to privacy has been extended to include the right of a data subject to request for their data from a data controller and also the right of a data subject to request for erasure of personal data. The right of a data subject to request for erasure of personal data was upheld by the Court of Justice of the EU in the case of ***Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González***[16], where the Plaintiff sought a court order that would prohibit Google search engine from displaying a link to a newspaper article published in 1998 when his name was searched. Consequently the CJEU held that search engine operators have an obligation to remove links to web pages from their result list if requested by a data subject. Articles 23 and 30 require companies to implement reasonable data protection measures to protect consumers' personal data and privacy against loss or exposure.

In ***Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)***[17] the issue was the refusal of the internet service provider Scarlet to install a system to filter electronic communications that use file-sharing software to prevent file-sharing that infringes copyright protected by SABAM, a management company that represents authors, composers and editors. The CJEU held that users' IP addresses "are protected personal data because they allow those users to be precisely identified". While in the case of ***Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB***,[18] CJEU concluded that IP Addresses are personal data within the scope of EU law. The need to safeguard the processing of personal data is further necessitated by the

[16] CJEU, Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EUC 2014:317

[17] CJEU, Case C-70/10 *Scarlet Extended SA v. Societe belge des auteurs, compositeurs et editeurs SCRL (SABAM)* [2012] ECDR 4 (52) 51

[18] C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB,* [2012] ECLI:EU:C:2012:219

interconnectivity of both animate and inanimate things to the internet. Privacy regulations are necessary and should be sustained as they do not impede development.

It is important for an individual to retain the services of a lawyer as early as possible if they suspect a breach of their privacy, whether directly or indirectly.

REFERENCES:

1. Constitution of the Federal Republic of Nigeria 1999 (as amended)
2. Data Protection Bill 2020
3. C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EUC 2014:317
4. C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB,* [2012] ECLI:EU:C:2012:219
5. C-70/10 *Scarlet Extended SA v. Societe belge des auteurs, compositeurs et editeurs SCRL (SABAM)* [2012] ECDR 4 (52) 51
6. Joris Toonders, 'Data is the New Oil of the Digital Economy' (*WIRED NEWS BLOG* 2021)<https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/> accessed 6th September 2021
7. Marie Helen Maras, 'Internet of Things: Security and Privacy Implications' (2015) 5 (2) IDPL <http://idpl.oxfordjournals.org> accessed 17 February, 2021 Marie Helen Maras, 'Internet of Things: Security and Privacy Implications' (2015) 5 (2) IDPL <http://idpl.oxfordjournals.org> accessed 17 February, 2021
8. OECD, 'The Internet Of Things Seizing The Benefits And Addressing The Challenges; 2016 Ministerial Meeting On The Digital Economy – Background Report' (OECD DIGITAL ECONOMY PAPERS No. 252 OECD Publishing 2016) 4

CONTRIBUTORS

OBINNA AKPUCHUKWU

Partner

+234(0) 906 715 8192.

o.akpuchukwu@allen-marylebone.com

IFATU OGAR

Associate

+2349067158192, +2348035105706

i.ogar@allen-marylebone.com

CONTACT US

Abuja Office: Ventures Park, No 5 Kwaji Close, Maitama, Abuja.

Onitsha Office: No 9 Tasia Road, Off Awka Road by ABS Junction, Onitsha, Anambra State, Nigeria.

Telephone: +234 906 715 8192, +234 803 510 5706

Email: info@allen-marylebone.com

Website: www. allen-marylebone.com