



An Article

DATA SUBJECTS AND THE LIABILITY OF IOT PRODUCTS FOR UNLAWFUL ACCESS TO DIGITAL FOOTPRINT



ABSTRACT

The widespread use and absorption of the Internet of Things (IoT) into our daily lives are drastically altering our global environment and its effect can be seen in the interactions within homes, schools, businesses, the healthcare sector, and other industries who in one form or the other and for a diverse of purpose, make use of these products.

Internet of Things is a system of interrelated and interconnected computing devices that can transfer data over a network with little or no human-to-human or human-to-computer interaction.

As the use of IoT products increases, legal issues such as data protection, software licensing, cybersecurity, and e-contracts arise. This research paper seeks to analyze and review the growth of IoT in the technology space, particularly in Nigeria, the issue of data protection, as well as key regulations. Lastly, the paper attempts to answer the question of who bears liability in the event of a breach of data privacy and unlawful access to the digital footprint.

INTRODUCTION

It is quite evident that the Internet of Things (IoT) is a rapidly developing industry in the technological space globally. Devices such as smart-watches, televisions, fridges, light bulbs, and even smart houses and cities, are changing how we see and interact with the world tremendously.

The processing, exchange, and transfer of data over the internet have made numerous innovations possible. However, some of these devices have little to no security framework against data breaches. There is a need to analyze the concept of the Internet of things, its usage of data, the need for data protection, and the liability arising from any unlawful data breach and access to a Data Subject's digital footprint.

DEFINITION OF KEY TERMS

Data - as defined by the Nigeria Data Protection Regulation (NDPR) 2019, means characters, symbols, and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device¹.

Personal data - is any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, ... but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.¹²

The digital footprint - is a trail or record of activities a person

carries out on the internet. It includes websites visited, emails sent, and information submitted to online services³. Everyone who uses the internet has a digital footprint as a record of online activities are constantly kept by the developers of IoT products.

IoT Developer - means any person charged with the creation of platforms, software and hardware that allows IoT devices to function.⁴

Internet of Things (IoT) - the interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.

THE CONCEPT OF INTERNET OF THINGS (IoT)


Internet of Things or IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors, and communication hardware, to collect, send and act on data they acquire from their environments⁵. It is described as the network of 'smart devices' that communicate with each other to automate and optimize performance. IoT devices share the data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analysed locally.

Sometimes, these devices communicate with other related devices and act on the information they get from one another⁶. The devices are able to function without or with little human interference. Humans can set up the device, give them instructions or access the data stored. Examples of IoT devices include heart monitor implants, smart home security systems, smartwatches, etc.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business⁷.

On the surface level, it is assumed that the IoT has eased the daily activities of consumers and generally made lives easier and simpler for individuals and organizations more so, in instances of ease of access to information, improved communication between connected devices, as well as automation and optimization of tasks.

However, these IoT devices have disadvantages. For instance, the increase in the number of connected devices and the massive amount of data shared between devices, increases the chances of hackers stealing confidential information and committing other cybercrimes.



THE REGULATORY FRAMEWORK OF THE INTERNET OF THINGS

With innumerable IoT devices talking to each other via the internet, the potential for a data security breach is high and as more and more IoT devices are introduced in the market, this issue is projected to become more complex than its current state.

The Constitution of the Federal Republic of Nigeria⁸, the constitutions of several jurisdictions, as well as several international treaties, holds the right to privacy as a salient human right.

In the technological space, this right extends to the Data Subject's personal data and digital footprint. The massive amounts of data processed by IoT devices across various devices over the internet, make the issue of data protection one of the most crucial issues. Without an adequate framework to ensure data privacy, Data Subjects are left vulnerable to numerous cyber-attacks, identity thefts, personal data leaks on the internet, and other unlawful and malicious use of personal data and digital footprint.

Data Protection Laws in the EU

In the European Union ("EU") countries, the General Data Protection Regulation ("GDPR") has been enacted to regulate data collection by IoT and Information Technology Developers and Third-Party Users.

The GDPR is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy⁹.

Personal data is at the core of GDPR. In general, this is information that allows a live individual to be recognized directly or indirectly from publicly available data. Names, addresses, and unambiguous online usernames are all examples of personal information. Personal data can also include information that is less obvious, such as IP addresses and cookie IDs. There are a few unique kinds of sensitive personal data that are given additional safeguards under GDPR. Information regarding racial or ethnic origin, political ideas, religious beliefs, trade union membership, genetic and biometric data, and health information are all examples of personal data.

GDPR also applies to enterprises situated outside of the EU. GDPR may apply if a Nigerian company does business in the EU, as well as if the data controller is a citizen of an EU nation-state.

The GDPR is built on seven main principles outlined in Article 5 of the Act, which are intended to regulate how people's data is treated. Lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability are the seven principles of GDPR.

While data controllers and processors face the most severe penalties under GDPR, the regulation is intended to safeguard people' rights.

Data Protection Laws in Nigeria

The Constitution of the Federal Republic of Nigeria, 1999 (as amended) sets the pace for the protection of the privacy of Data Subjects in Nigeria. Section 37 guarantees and protects the privacy of citizens, their homes, correspondence, and telegraphic communications¹⁰. Although the provision above does not specifically mention "data", it is arguable that information on homes, correspondences, and telephone conversations are captured in the definition of personal data, hence, the above provision can be used to safeguard such breaches¹¹.

The Nigerian Information Technology Development Agency ("NITDA") created the Nigerian Data Protection Regulation ("NDPR") 2007 pursuant to Section 6 (a) and (c) of the National Information Technology Development Agency Act (NITDA Act), to secure and protect the personal information of Data Subjects.

This Regulation was made in recognition of the fact that many public and private bodies have migrated their respective businesses and other information systems online. These information systems have thus, become critical information infrastructure that must be safeguarded, regulated, and protected against personal data breaches¹².

In the wake of the passage of the NDPR, the Federal High Court, sitting in Abuja, in the case of **Incorporated Trustees of Paradigm Initiative for Information Technology (PIIT) & Sarah Solomon-Eseh v National Identity Management Commission (NIMC) & Anor**¹³ reaffirmed the privacy rights of Nigerians as it ordered the Nigerian Information Management Commission to implement adequate steps to safeguard the privacy rights of Nigerian citizens beyond merely having spurious security policies which it had prior to the suit, and failed to implement.

More so, in **Suit No. FHC/IB/98/2020** between **Digital Rights Lawyers Initiative v. N.Y.S.C.**, filed at the Federal High Court, Ibadan, the Plaintiff is seeking amongst other things¹⁴– a declaration that the filing of a 'Data Subject Consent Statement' as a condition for the issuance of a discharge

certificate does not qualify as freely given consent required under Article 1.3(iii) of the NDPR, 2019 for the obvious reason that in refusing to waive one's right by filling the said form, a discharge certificate would not be issued.

The NDPR Regulation stipulates the guidelines for the lawful collection and processing of data and impose on IoT developers and data controllers the duty to ensure that data collected through the devices or platforms are secured against cyber-attacks and data breaches.

The NDPR provides that the processing of personal data is governed by general principles that personal data must be collected and processed in accordance with a specific, legitimate, and lawful purpose consented to by the Data Subject¹⁵.

According to this Section, access to digital footprint must be in accordance with the law. Also, Article 2.2 of NDPR provides principles that must be followed for data processing. These principles are lawful processing of data, data minimization, accuracy, reasonable storage and retention period, confidentiality and security, adherence to the rights of the Data Subjects, and lastly, compliance and enforcement of all guidelines as stipulated by the Regulation.

To fully protect and safeguard the personal information of Data Subjects, the Regulation provides several rights for the benefit of Data Subjects. These rights include:

- a. The Right to be Informed of the Actual Or Intended Processing Activity;
- b. The Right to Rectify the Personal Data;
- c. The Right to Object to the Processing of Personal Data;
- d. The Right to Request the Deletion of Personal Data;
- e. The Right to Request the Restriction of the Processing of Personal Data; and
- f. The Right to Request that Personal Data be Transferred to Another Platform or Person (natural or artificial).

Apart from the NDPR, the Credit Reporting Act (CRA) No. 2, 2017 enacted by the Federal Government aims to promote access to accurate, fair, and credible credit information, though sector specific, offers protection to Data Subjects.

Section 9 (1) provides:

“Except this Act provides otherwise, Data Subjects shall have the right to the privacy, confidentiality and protection of their credit information”.

This section gives rights to Data Subjects to protect their privacy and to withhold or give consent when they so desire¹⁶.

Other laws that regulates data privacy and unlawful access

to digital footprint include

- i. The Nigerian Communications Commission Code of Practice Regulation 2007,
- ii. The Nigerian Communications Commission Registration of Telephone Subscribers Regulation 2011,
- iii. The Freedom of Information Act, 2011,
- iv. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015,
- v. The Childs Right Act 2003,
- vi. The Consumer Protection Framework 2016,
- vii. The National Identity Management Commission (NIMC) Act 2007,
- viii. The National Health Act (NHA) 2014; and
- ix. The Federal Competition and Consumer Protection Act, 2019.

In order to ensure the privacy and protection of data collected, and in compliance with the various regulatory laws, the IoT service provider specifically drafts a privacy policy detailing the private information that is collected by the service provider, the scope and extent of use of such information, the details of any third-party with whom such information will be shared, and the steps taken to ensure that the information collected is secured against cyber attacks and illegal usage.

PRIVACY ISSUES ARISING FROM THE USE OF IoT PRODUCTS


Increase in Communication Pattern

One of the major challenges of this interconnectivity is that the IoT device communication pattern might increase the likelihood of data breaches. IoT devices could communicate in several ways, such as: device – to – device communications, device to an internet cloud service or a device to a gateway communication.

In the latter instances, the IoT device would have to connect to a data analytic service in a cloud computing setting. In those situations, a company would have to ensure the security of the cloud platform.

Furthermore, the consent of e-users, forms one of the legal basis for processing any personal information. However, some IoT devices have no mechanism for user interface and so may be unable to obtain the consent of users. This may be problematic, as it does not afford visitors the opportunity to read privacy notices or information usually presented on a computer or a mobile device, requesting for the consent of the users.

In addressing this seeming gap, an option is to obtain the consent of the Data Subject or enter into an agreement with the Data Subject at the point of using the device. However, because various devices might interact with one another, the information accessed by a device may not have been



anticipated by the manufacturer.

Consequently, although permission might have been obtained at the initial point, the legal basis for processing additional information might not have been established thus, exposing the developer to liability in respect of the additional data.

Cross-Border Transfer of Data

Another issue is the cross-border transfer of data. The IoT devices connected to the internet may collect information from a country and transmit same for storage or processing in another country. In this situation, the entities processing the personal data are to ensure that they establish the legal basis for the transfer of the data and establish adequate security measures for the personal data.

The data protection regulations earlier mentioned have set out regulations guiding the cross-border transfer of data. Failure to follow the laid down guidelines results in liability on the part of the developer in the event of data breach.

Ultimately, companies involved in the processing of information from IoT devices are expected to recognize the rights of consumers to use, access, and store their personal data. The right of consumers to data portability allows them to access and reuse their data. The right to erasure also allows them to be forgotten. Consumers are also given the right to object to automated decision-making for use in scenarios, when a potentially damaging decision could be made without human intervention⁷.

Data Ownership

The issue of data ownership can also pose a problem for IoT products due to the involvement of multiple stakeholders/IoT users, involvement of third parties, and the multitude of sources of the data, the data may come into possession of many data processors.

The IoT service provider, being the data controller would essentially determine the scope, extent, manner, and purpose of the use of the personal data, whereas the service provider may have different third-party data processors, functioning to process the data on the instance and under the control of the data controller.

Therefore, an aspect worth noting, is that since there are numerous channels of dissemination of the data/information and multiple stakeholders involved, the IoT service provider (data controller) at all times should ensure that the line between data controller and data processor does not get obscured.

Additionally, the Machine Generated Information (MGI) and

Machine to Machine Communication (M2M) generated in an IoT environment would also pose ownership and liability issues.

In light of the above, the allocation of risk and responsibilities between the parties must be defined precisely in particular, which party bears the liability for any damage caused to the user of an IoT and which party owns the information generated by the IoT project.

Hence, warranties and indemnities regarding data protection, security and privacy will become important to help draw the line between data controller and data processor, which are made all the more complex by the large number of stakeholders involved in an IoT environment. The question of who owns the data will be purely based upon the agreement between the two entities.

The issues pertaining to data ownership, security and privacy in an IoT environment can be reasonably addressed by contracts between device manufacturers/ IoT service providers and IoT users. These contracts may be entered by way of clickwrap and shrink-wrap contracts which are basically End User Licensing Agreements (EULA), governing the terms and conditions of use of the software or device. Like any normal contract, an e-contract can form a valid and binding relationship between the parties if it fulfills the essentials of a valid contract.

In an IoT environment, there is no privity of contracts between multiple IoT users which may lead to complexity in case of a dispute. Therefore, the draft agreement should contain express provisions regarding third party liabilities and dispute resolution.

Possible Protection for IoT Developers

IoT manufacturers/developers are advised to cover themselves with product liability insurance, to minimize the liability which may arise from device malfunctions, software compromise or data loss/breach. These issues could result, not only from device defect but also failure on the part of network providers to ensure necessary communication.

CONCLUSION

Whether or not Data Subjects can hold IoT developers for breach of data privacy and unlawful access to digital footprint will be a matter of facts rather than of law. It might be difficult to determine who should be held accountable for breaches of privacy and unauthorized access to digital footprints. For example, in a situation whereby a patient⁹ is being monitored by a cardiac monitor in a hospital, who is the owner of the data stored on the machine? the developer of the machine, the hospital, the health insurer or the

patient and who can be held liable in the case of breach of data privacy?

The answers to this issue are open, as various individuals will have different opinions and views. To ascertain ownership of the data, recourse must be given to the terms and agreement in the contract between the developer of the machine and the hospital, the health insurer, the patient and the hospital.

Also, to determine who is liable for the breach, we will have to consider which party is at fault for the negligence. It is safe to state, that each issue of data breach will be handled by

the courts objectively and with consideration to the specific facts.

The legal wisdom regarding the IoT is inadequate due to the lack of awareness in this regard. Also, the law is still very unclear about the use of IoT products and the protection of data stored on and shared through them. The IoT environment continues to evolve at an unprecedented rate and it will not be long before the legal system catches up. Although IoT devices tend to push the limits of privacy in their operations, the protection of consumers' data should be the foremost concern in delivering IoT solutions.

END NOTES

1. Article 1.3- iv, *Nigeria Data Protection Regulation, 2019*
2. Article 4(1) of the NDPR
3. 'Digital footprint' TechTerms.
https://techterms.com/definition/digital_footprint
4. A. DiFranza: "How to Become an IoT Developer"
<<https://www.northeastern.edu/graduate/blog/iot-developer/#:~:text=An%20IoT%20developer%20is%20one,and%20connect%20to%20other%20devices> (Last accessed at 8:56pm 20th June, 2021)
5. Gillis, A. 'Internet of things'. TechTarget: IoT agenda.
<https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT> accessed on 6th June, 2021.
6. *ibid*
7. *ibid*
8. Section 37 of the Constitution of the Federal Republic of Nigeria, 1999.
9. Palmer, D. 'What is GDPR? Everything you need to know about the new general data protection regulation' [July 5, 2021]. ZDNet. Retrieved from <https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/>
10. Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) provides "the privacy of citizens, their homes, correspondence, telephone conversation and telegraphic communications is hereby guaranteed and protected"
11. Olumide Babalola, 'Nigeria: Data Protection And Privacy Challenges In Nigeria (Legal Issues)', [July 5, 2021] Retrieved from: <https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues->
12. Article 1.3 of *The National Data Protection Regulation 2019*
13. Caleb Echoga, *Is Africa's data protection in crisis? The Nigerian Experience* https://omplex.com.ng/wp-content/uploads/2021/01/Thought_Leadership-Is_Africa_Data_Protection_in_Crisis_The_Nigerian_Experience.pdf; accessed July 5th, 2021
14. Unini Chioma, 'NGO Sues NYSC for Violating Corp Members' Privacy by Forcefully Publishing and Selling Their Personal Data in A Yearbook' < <https://thenigerialawyer.com/ngo-sues-nysc-for-violating-corp-members-privacy-by-forcefully-publishing-and-selling-their-personal-data-in-a-yearbook/> > Accessed 04 July 2021.
15. See article 2.1 of NDPR
16. Okoriekwe, C. 'Internet of Things (IoT) and Digital Privacy Rights: Drawing the Dividing Line in Nigeria' [2020]. Lexology.
<https://www.lexology.com/library/detail.aspx?g=9670c2e6-1b58-4140-8042-2bc6a3aaaf21> Accessed on 6th June, 2021.
17. Davidson Oturu and Florence Balo-Balugun; September 11, 2019; Data Protection and Internet of things
<https://www.mondaq.com/nigeria/privacy-protection/844216/data-protect3050n-and-the-internet-of-things>
19. Radcliffe, M. 'Internet of things: understanding the legal framework'. CIOReview. Retrieved from <https://networking.cioreview.com/cxinsight/internet-of-things-understanding-the-legal-framework-nid-10493-cid-9.html>

Authors

Raimi Khadijat Opemipo
Ajao Humomot Temitope
Iremia Favour
Arogundade Hikmat



Contributor

John Oladipo
Member, Technology, Financial Technology and Intellectual Property Group,
Omaplex Law Firm
John.oladipo@omplex.com.ng