

# ÆLEX

## DATA PROTECTION AND THE INTERNET OF THINGS



SEPTEMBER 2019



# INTRODUCTION

The introduction of the internet in the late 20th century has changed how we live, work and carry out transactions.

Although internet usage began with computers, it has now extended to other devices such as cellphones, watches, coffeemakers and even smart buildings.

The Internet of Things (“IoT”) has been described as “a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-human or human-computer interaction.”[1]

Put simply, IoT is the connection of devices to the internet; it involves the use of sensor enabled devices designed to collect data about their environment, which frequently includes data related to people.[2]

For instance, Amazon introduced the Amazon Echo, a voice-controlled device that is activated with the voice of the owner of the device and responds to voice commands.[3]

The International Data Corporation has forecasted that there will be 41.6 billion connected IoT devices, or “things,” generating 79.4 zettabytes (ZB) of data by 2025.[4]

## INTERNET OF THINGS AND DATA PROTECTION LAWS

The core data privacy law in Nigeria is the Nigeria Data Protection Regulation (“NDPR”), issued by the Nigerian Information Technology and Development Agency (“NITDA”), and it regulates the processing of personal data.

It is noteworthy that the NDPR specifies the legal basis for which an entity can process personal data and imposes the obligation for security and protection of personal data on such data processing company.[5]

You may read our article on the NDPR here for more details. It is assumed that the IoT will ease the life activities of consumers and on the flip side, companies will be able to see how customers are using their stores, online services and even their products.[6]

However, 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,[7] 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.[8]

[1] <https://qa-platforms.com/importance-of-internet-of-things/> accessed on 30th August 2019.

[2] Karen Rose, Scott Eldridge, Lyman Chapin - The Internet of Things: An Overview – October 2015 – The Internet Society.

[3] Nicole Lindsey- Data Privacy in the Era of Internet of Things- <https://www.cpmagazine.com/data-privacy/data-privacy-era-internet-of-things/> accessed on 30th August 2019

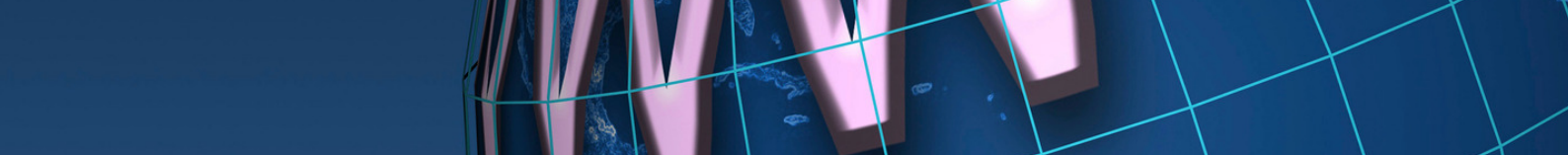
[4] The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast – June 18, 2019 - <https://www.idc.com/getdoc.jsp?containerId=prUS45213219> accessed on 30th August 2019.

[5] Article 2.2 of the NDPR.

[6] Internet of Things - <https://www.intel.com/content/www/us/en/internet-of-things/iotalliance.html> accessed on 30th August 2019.

[7] Internet Architecture Board (IAB) - networking of smart objects (RFC 7452), <http://www.rfc-editor.org/rfc/rfc7452.txt> accessed on 30th August 2019.

[8] Karen Rose, Scott Eldridge, Lyman Chapin - The Internet of Things: An Overview – October 2015 – The Internet Society



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.[9]

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.

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 to 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. [10]

Ultimately, companies involved in the processing of information from IoT devices are expected to recognise the rights of consumers to use, access, and store their personal data.[11]

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 intervention.

## CONCLUSION

Although IoT devices have the tendency to push the limits of privacy in their operations, the protection of consumers' data must be foremost in delivering IoT solutions.

[9] Lara Veigh, The Internet of Things in the Era of GDPR, <https://eugdprcompliant.com/internet-of-things-era-of-gdpr/>, October 24, 2017 accessed on 30th August 2019

[10] Article 2.6, 2.11 and 2.12 of the NDPR

[11] Article .1 of the NDPR



# ÆLEX



Florence  
Bola-Balogun  
ASSOCIATE



Davidson  
Oturu  
PARTNER

ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana. A profile of our firm can be viewed here. You can also visit our website at [www.aelex.com](http://www.aelex.com) to learn more about our firm and its services.'

**COPYRIGHT:** All rights reserved. No part of the publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means without the prior permission in writing of ÆLEX or as expressly permitted by law.

**DISCLAIMER:** This publication is not intended to provide legal advice but to provide information on the matter covered in the publication. No reader should act on the matters covered in this publication without first seeking specific legal advice.

ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana.

Contact us at:

4th Floor, Marble House,  
1 Kingsway Road, Falomo Ikoyi,  
Lagos, Nigeria

Telephone: (+234-1) 4617321-3, 2793367-8, 7406533,

E-mail: [lagos@aelex.com](mailto:lagos@aelex.com)

Click here [www.aelex.com](http://www.aelex.com)

to follow our social media handles  
click below



@aelexpartners