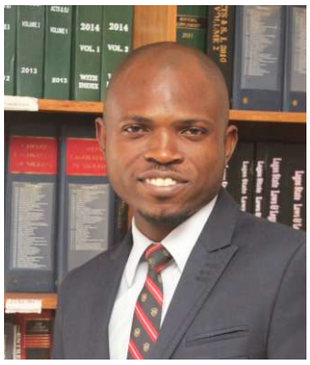
Internet of Things (IoT) and Digital Privacy Rights:

Drawing the Dividing Line in Nigeria

Thought Leadership | By Chuks Okoriekwe (Originally published in *BD Legal Business, 15th February, 2018, p. 25)*



c.okoriekwe@lelawlegal.com

Introduction

The growth of the Information Technology (IT) industry continues to spawn massive investment in research and development of IT products. These research efforts have given rise to Internet of Things (IoT). Simply put, IoT are devices and objects connected to the Internet. These products including: watches, glasses, health indicators, home automation i.e. digital lightbulbs, thermostats and fridges, autonomous vehicles, connected 'smart' cities, etc. have continued to shape the industry across many sectors, thus generating massive data feed into analytics to understand consumer behaviour. However, one of the germane legal issues that arises as a result of IoT is users' privacy: these products could negatively impact users' privacy. To what extent are users willing to open up their daily routine to 'total strangers' in a bid to use a device? Original Equipment Manufacturers (OEMs) may argue that their operation works within the terms of service (usage) of the device. But the reality is that these contracts are usually in standard form, often long, in tiny illegible prints and does not guarantee compliance by OEMs where users/Data Subjects (DS) are unaware of the sets of data strings collected by these devices.

Digital Privacy - A Fundamental Right?

Privacy is defined by Black's Law Dictionary (9th Edition, 2009, pg. 1315) to mean *"the condition or state of being free from public attention to intrusion into or interference with one's acts or decision."* It has also been canvassed that privacy relates to the right or ability of individuals to determine how much or what information about themselves is to be revealed to others. This has necessitated its protection by many countries declaring it a fundamental right in their constitutions. Accordingly, ***section 37, Constitution of the Federal Republic of Nigeria, 1999 (as amended)*** provides, *"the privacy of citizens, their homes, correspondences, telephone conversations and telegraphic communications is hereby guaranteed and protected."* Could it therefore be argued that the right to privacy guaranteed under the Constitution extends to citizen's digital privacy rights?

The rise of IoT has continued to pose a threat to fundamental right to digital privacy across many jurisdictions. In a study conducted by the Global Privacy Enforcement Network (GPEN, a group of national privacy authorities comprising the UK, Canada, Gibraltar, Ireland, Columbia, Australia, Germany, Albania and Norway), it was observed that two-thirds of devices surveyed failed to adequately explain to customers how their personal information was collected, used, stored and disclosed.

Privacy Challenges of IoT

The GPEN further observed that privacy challenges of IoT include: (a) lack of control and information asymmetry where device connectedness results in personal data generation, storage and communication over which the user has no control; (b) quality of user consent - the user's consent to the processing of data carried out by IoT devices must be informed as in many cases the user will not be aware of the data processing carried out by a particular device; (c) secondary use and repurposing - where big data analysis techniques may lead to device data obtained for one purpose being used for a quite different purpose for which no consent has been given; aggregation of data from different devices may reveal specific aspects of individuals' habits, behaviours and preferences in an unduly intrusive manner; (d) limitations on the possibility to remain anonymous when using services; and (e) security risks including physical constraints, for example balancing battery efficiency and device security, may lead to manufacturers reducing security – the implementation of confidentiality, integrity and availability measures – to reduce costs.

These bring to the fore, the following questions: *what is the extent of legal and digital privacy protection granted users /DS of IoT products and services in Nigeria? Does a one-off consent amount to unlimited consent to capture users' data? Can DS hold the developers of IoT products liable for breach of privacy and unlawful access to their digital footprint?* For instance, Mr. A buys an IoT device, a wrist watch which is connected to his mobile phone from where he carries out

his bank transactions. Unknown to Mr. A, by consenting to use the device, the manufacturers of the wrist watch has all his digital footprint from his phone contacts, calls, text messages, account details, etc. This data string is stored with the OEMs/software developers and used for purposes that may not be disclosed to Mr. A. Incidentally, a cursory analysis of the various legislations on cybersecurity in Nigeria, it indicates a dearth in IoT regulation. Notwithstanding, the regulation of IoT could be gleaned from various legislations.

The Changing Paradigm in Digital Privacy Right Protection

The ***Electronic Transaction Bill, 2017*** provides an extensive protection of digital privacy rights of Data Subject (DS) and succinctly makes provision for liability for breach. The absence of Presidential assent since its passage in May, 2017 means the legislature undergoing the whole legislative process over again - ***National Assembly v. President & Ors. [2003] 9 NWLR (Pt. 824) 104***. This delay in putting in place a proper legislative framework for data protection has continued to increase DS' risk exposure to digital privacy breach by Data Processors (DP) within and outside Nigeria who deploy bespoke technologies to capture digital footprint without express consent.

The Federal Government (FG)'s efforts at enacting the ***Credit Reporting Act (CRA) No. 2, 2017*** with equivalent data protection provisions is however worthy of commendation. The ***CRA*** aims to promote access to accurate, fair and credible credit information, though sector specific, offers protection to DS. Some experts have argued that rather than have a single legislation on data protection, it would be preferable to have sectoral legislation, given the complexity as well as sector-relevance of some of the issues.

Section 9(1) CRA reads: *"Except this Act provides otherwise, Data Subjects shall have the right to the privacy, confidentiality and protection of their credit information."* Thus, affording DS the right to privacy and disclosure of data to Credit Information Users (CIU) is only permitted upon written consent - with the exception of banks, court orders and where discloser is required under applicable law, and such is only valid for the purpose for which it was granted – ***section 9(4) CRA***. Although the ***CRA*** is silent on the means of information exchange, it could reasonably be argued that usage of IoT devices (in the form of Credit Reporting Managing System), would not preclude its application since its basis is the regulation of credit reporting.

In cases of breach of DS' digital privacy rights especially where DS' credit information was wrongfully or fraudulently used, ***section 13 (8) CRA*** provides, *"…Credit Information Users shall be held liable in the event of wrongful or fraudulent use of Credit Information."* This provision could arguably be interpreted to create liability for data misuse or breach against CIUs thereby paving way for DS to institute action in court against CIUs. On the other hand, it could also be argued that the liability of CIU is to the regulator with the regulator having the right to impose sanctions, thereby excluding any potential claim by DS. Notwithstanding the foregoing arguments, DS whose digital privacy rights has been breached could approach the court under the ***Fundamental Rights Enforcement Procedure (FREP) Rules, 2009*** for the enforcement of his fundamental right to privacy.

Stemming the Tide of IoT Digital Privacy Breach: EU Example

The European Union (EU) remains one the most advanced jurisdictions regulating IoT. It imposes high responsibility on DPs whilst protecting digital privacy rights of DS, within its jurisdiction. With its most recent regulation, ***European General Data Protection Regulation (GDPR)*** due to become effective in May 2018, it seeks to further strengthen the gains in digital privacy protection through fines and increased compliance requirements for EV Dps.

The ***GDPR*** proposes an extra-territorial application to companies that process or control data from the EU regardless of the company's location or where the actual processing is carried out. By implication, if a company is based in Nigeria for instance, but processes or controls data from EU DS, it would be bound by the ***GDPR***. Where a company fails to adhere to the standards in the ***GDPR***, it could be liable for maximum fine of up to 4% of the company's annual global turnover or €20 million (whichever is greater). The ***GDPR*** further strengthens the requirement for consent. It requires Data Controllers (DC) and DPs to seek consent from DS using an intelligible and easily accessible form indicating the purpose for which the data is required. An innovative requirement for DC/DP is the inclusion of privacy protection in the design of their systems, rather than an 'add-on' when the need to protect DS arises and appointing data protection officers for the purpose of compliance notification.

In addition to the responsibilities on DC and DP, the ***GDPR*** created DS rights. Accordingly, where a breach occurs, there is an incumbent responsibility on the DC/DP to notify the DS within 72 hours of becoming aware of the breach, otherwise omission would constitute an infraction of the ***GDPR***. Also, the DS is guaranteed the right to access whatever information is being processed about him. This is to be provided upon request, free of charge and in electronic format leading to data transparency. Right to erasure is further guaranteed under the revised ***Article 17, GDPR.*** By implication, DS can request the total deletion or stop further processing of his data by simply withdrawing consent. DS also have the right to transfer their personal data from one controller to another.

Conclusion

Although, the use and deployment of IoT is of global significance, its impacts could be felt by direct users who reside within the jurisdiction of its use. As the EU has sought to protect the privacy of its residents through the ***GDPR***, it is prescient that the FG put similar regulations in place to protect millions of users of IoT devices and software - considering the amount of data of Nigerians captured on a regular basis by these devices. Undoubtedly, the ***CRA*** is in the right

direction. But the pending ***Electronic Transaction Bill, 2017*** could concretise digital privacy protection offered DS in Nigeria and same could be applicable to multinationals such as; Facebook, Google, Apple, etc. that captures, controls and process data from Nigeria, whilst promoting in-country data centres as opposed to 'outsourcing' Nigerian users' data to third party countries.