Journal of Commercial and Property Law Vol. 4, No1 August 2016

LEGAL RIGHTS OF USERS IN THE LIGHT OF THE INTERNET OF THINGS (IOT): A NIGERIAN PERSPECTIVE.

Monye Ogochukwu
Faculty of Law, University of Benin, Nigeria

Abstract
Internet technology has witnessed a series of advancement, ranging from the evolution of mobile services to the convergence of systems. The Internet of Things (IoT) is the new oil set to take the technology industry by storm. This brain child of Internet technology though envisioned as far back as 1932 by Jay B. Nash as 'the leisure of the Greek citizen', (made possible by mechanical slaves which orchestrate lighting, heating, shoe shining and hair cutting for owners), has only recently witnessed exponential growth due to the availability of enabling factors such as ubiquitous connectivity, sensor technology and availability of smart devices. The IoT is essentially a network of interconnections/communication between machines facilitated by information exchanges that enable devices to make intelligent decisions mostly without human intervention. Although the benefits of the IoT cannot be ignored as it has proven important in several sectors such as in medical diagnosis/patient care and home automation, legal issues such as data and privacy protection, contractual liability, intellectual property rights and consumer protection its use raise some concern. The author analyzes the suitability of existing laws and advocates for the enactment of additional pieces of legislation to adequately cover the field. The overall aim of this work is to explore the potential of the IoT in Nigeria, with a view to ensuring that the value delivery from the IoT does not usher in consumer detriment.

1.0 Introduction
Consumers all over the world are fast becoming part of the connected world, for reason that everyday devices such as mobile phones, home kit appliances, smart systems and wearable gadgets have become commonplace and interoperable. However, the IoT, is taking deep roots worldwide amid near legislative and regulatory vacuity in many jurisdictions including Nigeria. The IoT is essentially the ability of everyday devices, (embedded with technological appliances and tools such as sensors) to improve on tasks and create efficiencies from data gathered from other devices, the internet and observed user preferences; with minimal human interference (if at all). The success of the IoT is predicted to be heightened by the wave of artificial intelligence[1] where individual

[1] Artificial Intelligence (AI) is the discipline that studies how to create software and systems that behave intelligently. AI scientists build systems that can solve reasoning tasks, learn from data, make decisions and plans, play games, perceive their environments, move autonomously, manipulate objects, respond to queries expressed in human languages, translate between languages, and more.

devices become sentient[2] owing to an inbuilt capacity to learn and improve on tasks just as humans.[3] Even though the IoT promises fail safe mechanisms, cutting the risks of human mistakes or inaccuracies, regard must also be had to legal issues sailing beneath these wings of promises. This paper seeks to analyse the legal issues ushered in by the IoT in response to the 1961 pronouncement of Atanda Fatayi Williams J.S.C that, '*The law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of the computer.*[4] This analysis is also important as the industry is already on its heels to roll out embedded smart things equipped with intelligence with little regard to legal standards; in addition to the tacit approval lent to this trend by some national regulators. For example, authorities in the United States have already licensed self-driven cars and drones while the United Kingdom is witnessing a nationwide phase-in of smart meters. This paper advocates for legal and regulatory activism as the reach of the IoT will no doubt be global, necessitating an in-depth consideration of legal implications especially in emerging economies where the technological and legal landscape may be less sophisticated.

2.0 Definition

The Internet of Things (IoT) refers to the ever-growing network of physical objects that feature an IP address for Internet connectivity, and the communication that occurs between objects and other Internet-enabled devices and systems.[5] The Internet of Things extends internet connectivity beyond traditional devices like computers, smart phones and tablets to a diverse range of devices and everyday things that utilize

---

See Bernhard Petermeier, 'AI: how can we manage robot risk? World economic forum. Jan 2015 https://www.weforum.org/agenda/2015/01/artificial-intelligence-how-can-we-manage-the-robot-risk/ Accessed 09/08/2016 at 12.00

[2] Sentience means ability to feel or perceive things, sentience can refer to the ability of any entity to have subjective perceptual experiences. This when put in context with Machines, brings about the core aspect of IoT where the machines with sensors can collect and transmit information that can be processed and packaged for decision making or to follow some predetermined set of instructions if they conform to certain set parameters. See IoT India Congress 2016, 'Machine Sentience' 2016. Available at http://iotindiacongress.com/machine-sentience/ Accessed 9/9/2016 at 12.30

[3] Notable technology experts such as Apple co-founder Steve Wozniak, Bill Gates, Stephen Hawking and Tesla's Elon Musk to warn about the propensity for devices to reach a phase beyond human control- Peter Holley, 'The future is scary and very bad for people' The Switch-Washington Post, March 24, 2015 https://www.washingtonpost.com/news/the-switch/wp/2015/03/24/apple-co-founder-on-artificial-intelligence-the-future-is-scary-and-very-bad-for-people/ Accessed 09/09/2016 at 1.00pm

[4] Festus Sunmola Yesufu v African Continental Bank Limited S.C. 42/1975 per Atanda Fatayi Williams J.S.C

[5]Forrest Stroud, 'IoT - Internet of Things'. Available at http://www.webopedia.com/TERM/I/internet_of_things.html Accessed 05/05/2016 at 2.00pm

embedded technology to communicate and interact with the external environment, all via the Internet.[6] Daniel Castro notes that with the IoT, the Internet is no longer just a global network for people to communicate with one another using computers, but it is also a platform for devices to communicate electronically with the world around them resulting in a world that is alive with information as data flows from one device to another and is shared and reused for a multitude of purposes[7]

3.0 Scale and Spread of Deployment

As can be gleaned from the success of the mobile phone market, e-commerce and online banking particularly in Nigeria and generally in Africa, it is expected that the IoT has the potential to find uptake in these regions. Cisco postulates that 52 percent of things termed IoT are already in Africa,[8] and 25 billion devices will be connected in the Internet of Things by 2015, rising to 50 billion by 2020.[9] Also, the smart phone which has already gained widespread usage in Nigeria will likely operate as the entry point for IoT deployment in terms of home automation, smart agriculture/crop monitoring and even remote patient monitoring.

Gartner estimates that the Internet of Things (IoT) will support total services spending of $235 billion in 2016, up from 22 percent in 2015 especially in the sphere of professional services for the design installation and operation of IoT systems in addition to connectivity and consumer services.[10] Drones, driverless cars, and smart meters are few of the myriad of devices that already exist. In terms of home automation, smart meters, smart fridges and full range of smart connections have been developed by technology companies such as the Apple home kit and Amazon's Echo which bundle together a connection of music players, lighting, and smart phones to perform tasks. [11] Gartner also predicts that over 6.4 billion web-enabled devices will be connected as part of the Internet of Things at the end of 2016, an increase of 30% from 2015 and

[6] Ibid

[7] Daniel Catro, 'Thirty (Plus) Ways the Internet of Things is Changing the World'. The Futurist Magazine, Nov 19 2013 Available at http://www.theinternetofthings.eu/daniel-castro-thirty-plus-ways-internet-things-changing-world Accessed 03/01/16 at 3.03

[8] Dayo Paul, '52 per-cent hardware for Internet of Things already in Nigeria, others – Cisco' January 4, 2016, Newswatch Times IT/Telecomms. www.mynewswatchtimesng.com Accessed 06/08/2016 at 6.50pm

[9] Cisco, 'The Internet of Things How the next Evolution of the Internet is changing Everything' http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL

[10] Gartner Newsroom STAMFORD, Conn., Press Release- Gartner Says 6.4 Billion Connected "Things" Will Be in use in 2016, Up 30 Percent From 2015.' November 10, 2015 http://www.gartner.com/newsroom/id/3165317 Accessed 05/05/2016 at 6.00pm

[11] Amazon, 'Amazon Echo' Available at https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E 2016, accessed August 2016. See also Apple, 'Homekit' Available at https://developer.apple.com/homekit/ 2016, accessed 09/08/2016 at 6.10m

about 5.5 million new 'things' will be added each day with the total predicted to rise to over 20 billion by 2020.[12]

Verizon data show that "things" such as home thermostats and wearable health, fitness devices, aircraft jet engines and power grids will be added to the internet daily while devices, connectivity, and IT services will make up the majority of the projected $1.3 trillion IoT market in 2019 with modules and sensors comprising 23% of that total.[13]

4.0 Benefits of IoT

From the birth of the first 'thing'- an internet enabled toaster in 1990,[14] the IoT has been successfully used in different areas to provide efficient transport, better health and well being, improved yield in business and agriculture, energy efficiency at home and public safety in smart cities.

In the field of Agriculture, manufacturers can capture data from sensors on agricultural equipments to understand how farmers utilize different product features. This information can be shared with the R&D groups to develop products that best meet customers' needs.[15] Farmers also ensure better yields, output and storage with real time information on crop condition and market rates. An example is the Kaa open-source IoT Platform.[16]

For home automation, devices such as thermometers, washing machines, smart meters, alarms and garage doors can interact efficiently to make energy savings, work optimally and report faults. For instance the Nest thermostat works with August Smart Lock to help home owners view the temperature of the home and keep track of activities in homes.[17]

[12] Rob van der Meulen, Gartner 'Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015' Nov 2015 http://www.gartner.com/newsroom/id/3165317 Accessed 10/08/2016at 12.45

[13] Verizon, 'State of the Market: Internet of Things 2016: Accelerating innovation, productivity and value' 2016 Report. Available at http://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf Accessed 10/08/2016 at 3.00pm

[14] Thomas Newton, 'Internet Connected Toasters: A history' April 2012. Available at https://recombu.com/digital/article/internet-connected-toasters-a-history_M10281.html Accessed 09/09 /2016 at 3.30pm

[15] ibid

[16] Kaa, 'Solutions for smart Farming' Available at http://www.kaaproject.org/agriculture/ Accessed 09/09 /2016 at 3.30pm

[17] Smarter home access with August Home and Nest 2016 http://august.com/nest/ Accessed 03/08/2016 at 11.00am

In terms of public safety, the IoT enables smart bridges and roads to alert the authorities on needed repairs.[18] Additionally, smart cars such as the Google driverless smart car can detect objects, access maps to navigate a journey and choose safe speed and trajectory for self driving.[19] Finally, a smart traffic control light can readjust itself to optimize traffic flows without sticking to pre-fixed timings in addition to providing information to drivers on traffic and street conditions, congestions and parking availability.[20] Dubai is currently being transformed to a smart city where the use of technology to minimize energy, waste and resource consumption is expected to improve the quality of life and ensure better engagement with citizens in the fields of, health care, transport, public utility, education, public safety[21]

Similarly, the combination of sensors, Wi-Fi, and other technologies come handy in the health sector in monitoring the vital functions of patients such as temperature, blood pressure, heart rate, cholesterol levels and to stimulate the heart muscle in case of a heart failure, etc[22]. It will aid better patient care especially in rural settlements where health centers may be sparse. Key beneficiaries will include the ageing population, persons who live alone and the vulnerable. Smart drug dispensers such as the Hero smart pill technology can also monitor drug compliance, order restocking of supplies and report anomalies to family members or medical personnel.[23]

Futuristic as it may seem, some countries have already begun to phase in IoT systems. For example, the Dubai Smart city plan has recently completed its Pilot stage and is currently working on the next phase.

Given the fact that several vulnerabilities have already been discovered in everyday devices such as baby monitors, alarms and TVs,[24] the following section seeks to address explore the IoT in the light of Nigeria's existing laws in order to understand its implication and potential for Nigeria as an emerging economy.

---

[18] Author: Daniel Burrus, 'The Internet of Things Is Far Bigger Than Anyone Realizes,' Burrus Research

[19] Google Self-Driving Car Project, Available at https://www.google.com/selfdrivingcar/how/ Accessed 22/08/ 2016 at 7.05am

[20] The Traffic Lights of Tomorrow Will Actively Manage Congestion: The humble traffic signal is gaining some new responsibilities. Keith Barry Sep 11, 2014 Available at http://www.citylab.com/commute/2014/09/the-traffic-lights-of-tomorrow-will-actively-manage-congestion/379950/ Accessed 11/08/ 2016 at 6.15am

[21] KPMG Consulting, 'Dubai - a new paradigm for smart cities' July 2015 pg 10. Available at https://www.kpmg.com/AE/en/Documents/Dubai%20A%20new%20paradigm%20for%20smart%20cities.pdf Accessed August 2016

[22] Nomusa Diodio: Potential Applications of the Internet of Things technology for South Africa's Health Services

[23] Hero Smart Pill technology Available at https://herohealth.com/ Accessed 15/08/2016 at 8.04am

[24] Popular Internet-of-Things devices aren't secure HP security researchers found 250 security issues when analyzing 10 popular IoT devices By Lucian Constantine http://www.computerworld.com/article/2490587/networking/popular-internet-of-things-devices-aren-t-secure.html Accessed 13/08/2016 8.13 pm

5.0 Core legal concerns

Nigeria is presently the second largest economy in Africa and so naturally a potential hotspot for the emergence of trends. Nigeria has a relatively high broadband and mobile deployment and has collaborated with other African nations to build the largest undersea cable in Africa to improve internet connection. [25] While these heights are commendable, the legal landscape in the area of cyber law is still in its neophyte stage. Important issues such as data Protection and privacy can be mostly found in packets of financial and telecommunications Laws and rules without any comprehensive laws for the Internet and cyberspace.

Nigeria ought to methodically consider the implication of the IoT at the national and subsequently, the global level. Of chief concern should be the suitability of national laws to tackle the issues likely to be raised by the IoT with the view to ensuring that the risks do not outweigh expected benefits. In the United States, for instance, the FTC has released a guidance report on privacy and the security on the IoT[26] with far reaching provisions including proposition for privacy/security by design inputted at the level of manufacturing. Furthermore, data protection principles such as data minimisation, limitation and disposal principles receive emphasis. Again the concepts of notice and choice receive like attention.

Regulators in the European Union have also achieved like strides in recommending consent management features such as sticky-policies[27] and privacy proxies in addition to requiring Privacy Impact Assessment, annonymising or aggregating data, deleting data at the nearest point of collection (not storing raw data), employing user friendly terms, allowing the option to disable sensors and enabling data access and export.[28]
Even the industry has achieved significant feats in self regulation. For instance, alliances such as the All Seen Alliance (with members including LG, Microsoft, Panasonic and Sony) and the Open Interconnect Consortium (with over 150 members

[25] Africa Telecoms utlk 2014: Maximizing digital service Opportunities. www.www.infrmatandm.cm

[26] FTC Staff Report 'Internet of Things: Privacy & Security in a Connected World' January 2015. Available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. Accessed 02/08/2016 at 2.15pm

[27] A sticky policy is Policies that attach conditions and constraints to data to define allowed usage and obligations are called sticky policies. See definition by Shuyu Li, Tao Zhang and Jerry Gao, Younghee Park, 'in A Sticky Policy Framework for Big Data Security' Mar 23, 2015. Available at https://www.researchgate.net/publication/273635349_A_Sticky_Policy_Framework_for_Big_Data_Security

[28] Article 29 Data Protection Working Party 14/EN WP 223: 'Opinion 8/2014 on the on Recent Developments on the Internet of Things.' Adopted on 16 September 2014. Available at www.dataprotection.ro/servlet/ViewDocument?id=1088 Accessed 15/08/2016 at 2.05pm

including Intel, Cisco, GE, Samsung and HP)[29] are working together to develop open interoperable standards between members. Apple has also sought collaborations from Google, Philips Hue, and Samsung for its smart home product range.[30]

Unfortunately, Nigeria has barely made significant inroads into considering the impact of the IoT on consumers and the nation as a whole. Clearly, the IoT raises core concerns as regards data protection, consumer protection, privacy, intellectual property protection/ Digital Rights Management, spectrum allocation, standardisation and competition that need to be addressed at first opportunity in order to ensure that the country is not at the receiving end of unfair business practices or a dumping ground for services that fail to meet acceptable standards. To help put Nigeria's perspective in context, it is important to consider the legal landscape in place with a view to ascertaining adequacy to cushion any negative effects of the IoT.

5.1 Data Protection

Data protection laws ought to address core universally acceptable principles such as data adequacy, relevance, accuracy, necessity, accessibility and transferability. Also data should be obtained lawfully and fairly, should recognize the rights of data subjects, be anonymised/pseudomised[31] and be protected from unlawful processing and transfer.[32] The importance of proper processing of data will be heightened in the light of the IoT as interactions especially between personal things such as mobile phones, home appliances and other wearable gadgets can provide a deeply revealing digital picture of individuals. Unfortunately, in the sphere of data protection, Nigeria has no general data protection law, even though there exists some packets of protection within some telecommunications and financial regulations that mandate the protection of data.

[29] Consumers International, 'Connection and Protection in the Digital Age: The Internet of Things and challenges for consumer protection' April 2016. Available at http://www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf Accessed 30/09/2016 at 11.03am

[30] Amazon, 'Amazon Echo' Available at https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E 2016. Accessed 15/08/2016 at 4.00pm

[31] Care must be taken with anonymized data which is data that does not itself identify any individual and that is unlikely to allow any individual to be identified through its combination with other data. See in Information Commissioner's Office, 'Anonymisation: managing data protection risk code of practice' https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf November 2012. Accessed August 2016 as Even if data is anonymized, evidence has been led to the fact that connecting large amounts of diverse data, could still result in the identification of individuals. Morana Miljanovic, 'The not-so-new false promise: putting the puzzle together' Feb 2015. Available at https://myshadow.org/false-promises-data-anonymisation Accessed 23/01/2016 at 12.00 pm

[32] These Principles have been enshrined in the laws of several countries including the European Union Data Protection Directive 1998 revised 2014 which spells out eight core principles for efficient data protection.

One of such provisions is the Nigerian Communications Commissions Act 2003 Consumer Code of Practice Regulations 2007. Section 35 of this regulation provides that data on consumers can be collected by licensees for reasonable business purposes provided that collection is-

(*a*) fairly and lawfully collected and processed;
(*b*) processed for limited and identified purposes;
(*c*) relevant and not excessive;
(*d*) accurate;
(*e*) not kept longer than necessary;
(*f*) processed in accordance with the Consumer's other rights;
(*g*) protected against improper or accidental disclosure; and
(*h*) not transferred to any party except as permitted.

A Licensee must also imbibe fair information principles including notice, choice, access security, enforcement and redress mechanisms[33] and apply data rules to all recorded information whether received verbally or written manually.[34] Section 36 further provides that a licensee shall ensure that exchange or disclosure of information is only between entities that have adopted and implemented an appropriate protection of Consumer information policy. Licensees must also provide an accessible and easy to read policy clearly stating what information is being collected, the use of that information, possible third party exchange or disclosure of that information, the choices available to the consumer regarding collection, use, disclosure and access to the collected information, the consequences if any, of a consumer's refusal to provide information and available complaints mechanism.[35] By the provisions of section 38, individually identifiable consumer information shall be accurate, relevant and current for the purposes for which it is to be used and Licensees shall establish appropriate processes or mechanisms to correct so that inaccuracies in individual consumer information, including out of date information.

Furthermore, the Central Bank of Nigeria Guidelines on Electronic Banking in Nigeria, 2003, mandates all banks by section 3(d) to protect the privacy of the customer's data by ensuring that customer's personal data are used for the purpose for which they are compiled, consent of the customer is sought before the Data is used, and data user's request for blocking or rectification of inaccurate data is honored free of cost. Further, children's data must only be processed with the consent of the parents (through regular mail verification). Default attracts strict criminal and pecuniary sanctions.

[33] Section 35(2) The Nigerian Communications Act 2003 No. 19 Consumer Code of Practice Regulations 2007
[34] Ibid at 35(3)
[35] Ibid at section 37

Additionally, data Protection is covered by the CBN Guidelines on Agent Banking and Agent Banking Relationship 2013 which provides that all information or data collected by bank agents shall be kept confidential[36] including all relevant records, data, documents or files[37]

As can be gleaned from the foregoing, data protection in Nigeria is sector specific and not consolidated. One disadvantage of this therefore is that only specific data controllers or processors[38] such as banks, bank agents and telecommunications companies are mandated to protect consumer data. A comprehensive Data Protection Act is therefore needed to guarantee principles that safeguard citizens' data from collection to disposal over a myriad of IoT connected systems.

5.2 Privacy and Security

The most apparent legal issues surrounding the IoT involve privacy and security. This is because the plethora of connection between devices within the IoT ecosystem will generate a data lake beyond imagination introducing the opportunity for mistake or abuse.[39] The IoT's potential to generate large amounts of personal information has serious implications for users which must be particularly addressed as unwarranted revelations of an individual's identity, location, medical records, sexual orientation, socioeconomics or political profile[40] could have grave detrimental effects on citizens. By the joint provisions of section 37 of the Nigerian Constitution, 1999, Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) the privacy of family life, home and correspondence is guaranteed. These instruments however barely set the imperative for protection without the needed depth as to specifics.

Other privacy provisions in Nigeria include, The Nigerian Communications Act 2003 No. 19 Consumer Code of Practice Regulations 2007 Part VI which provides in section 34 for the protection of the privacy of consumer information by licensees except for authorized interception of communication by the commission within section 147 of the Act.

---

[36] Part 3, section xv, CBN Guidelines on Agent Banking and Agent Banking Relationship, 2013

[37] Ibid at xxii

[38] A data controller determines the processing of data including the collection, use, transfer and disposal of such data while a data processor processes data under the instruction of the data controller e.g. employees. See the EU Data Protection Directive 1998 revised 2014 and the ICO explanation of the Data Protection Act. See at https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/?q=data+controller Accessed 15/08/2016

[39] Phillip Blum: 'Internet Of Things' 101: Legal Concerns, Law 360'. Available at http://www.law360.com/articles/526266/internet-of-things-101-legal-concerns Accessed 05/17/2016 at 2.33

[40] Ibid

The Child Rights Act 2003 which regulates the protection of children i.e. persons under the age of 18 years also makes general provisions for the protection of children's' privacy including privacy of family life, home, correspondence, telephone conversation and telegraphic communications[41]. The Freedom of information Act No. 4 of 2011 (the FOI Act) also compels the protection of the information of Nigerians. 14 of the FOI Act, permits a public institution to deny an application for information that contains personal information unless the data subject[42] consents to the disclosure, or where such information is publicly available. The Act defines 'Personal information' as "*any official information held about an identifiable person but does not include information that bears on the public duties of public employees and officials*".[43]

Furthermore, the CBN Regulatory Framework for Mobile Payment Services for Mobile Payment Services in Nigeria provides for privacy trust and security of transactions as rights of users[44] Also, the Guidelines on Operation of Electronic Payment Channels in Nigeria, 2016 makes provision for privacy by design and installation features which means that privacy must be considered at the point of product or service design or at the time of installation and not as an afterthought.[45]
Finally, the Guidelines for the Regulation of Agent Banking and Agent Banking Relationships in Nigeria 2013 mandates the protection of appropriate consumer protection systems against risks of fraud, loss of privacy and loss of service[46]

Obviously, a higher and more encompassing standard is required for privacy protection within the sphere of the IoT, than is provided by the abovementioned pieces of legislation. Nigeria should therefore propound far-reaching privacy standards that safeguard citizens in addition to objecting to practices that put privacy and security at risk. In the Netherlands for instance, the privacy authorities objected to a project for the introduction of smart metering due to the potential for intrusion into people's lives.[47]

---

[41] Section 8 Child's Right Act

[42] A data subject is one of is the individual whom particular personal data is about but not an individual who has died or who cannot be identified or distinguished from others. ICO Guidance on the EU Data Protection Act 1998. https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/?q=data+subject Accessed 22/08/2016 at 6.14pm

[43] See also Patrick Wallace: Data Privacy Protection in Nigeria: An overview of the Data Privacy Protection Laws in Nigeria. Feb 2015 http://www.elexica.com/en/legal-topics/data-protection-and-privacy/16-data-privacy-protection-in-nigeria Accessed 22/08/2016 at 6.14pm

[44] 6.2.3

[45] 1.2.k

[46] Guideline 15

[47] Eric Barbry, 'The Internet of Things, Legal Aspects What Will Change (Everything)…' 2012 Digiworld Economic Journal, no. 87, 3rd Q.
2012,http://repec.idate.fr/RePEc/idt/journl/CS8705/CS87_BARBRY.pdf Accessed 22/08/2016 at 6.14pm

The industry has to also be proactive in manufacturing devices and applying the principle of privacy by design to ensure that access and purpose of data collection will be decided at the stage of manufacturing[48] and not as an afterthought. For example, Pachube (Cosm) has proposed an "Internet of Things Bill of Right", which is expected to serve as an industry standard[49] Also, Netatmo Welcome facial recognition camera claims to store information only on the device's memory card rather than online.[50] Individuals should also be empowered with Personal Information Management Systems (PIMS) to track and manage data.[51]

5.3 Liability

As is to be expected, within the IoT ecosystem, the nature and consequences of offences will likely change e.g. identity theft will go beyond individual targets to vulnerabilities in machines and connections.[52] With reference to liability, the difficulty will lie in identifying 'who' or 'what' bears the liability. E.g. where a device malfunctions or gives out wrong information that causes damage down the chain of connections, where will liability lie? Would it be the German device manufacturer, Chinese installation engineer, American IoT software developer or Norwegian information aggregators/transmitters, Nigerian Internet Service providers or even the individual owner for not updating software or downloading malware from unsecure sites?[53]

Devices within the IoT ecosystem will largely depend on settings and communications to which the humans will have no control.[54] For instance in a smart car scenario where autonomous vehicles must weigh the risks of injury to passengers against the risks to

[48] Taylor Wessing, 'Privacy by design – essential for the growth of the Internet of Things?'Feb 2014 https://united-kingdom.taylorwessing.com/download/article_privacy_design.html Accessed 22/08/2016 at 6.14pm

[49] ibid

[50] https://www.netatmo.com/en-US/product/camera

[51]A personal information manager (PIM) is a software application that uses tools to manage contacts, calendars, tasks, appointments and other personal data. See Techopedia, 'Personal Information Management System definition' Available at https://www.techopedia.com/definition/24752/personal-information-manager-pim Accessed 20/09/2016 at 11.14 am

[52]Eric Barbry, 'The Internet of Things, Legal Aspects What Will Change (Everything)…' 2012 Digiworld Economic Journal, no. 87, 3rd Q. 2012,http://repec.idate.fr/RePEc/idt/journl/CS8705/CS87_BARBRY.pdf

[53]Wilson Elser, 'The Internet of Things: The Inevitable Collision with Product Liability' Product Liability Blog, lexology. January 2015 http://www.lexology.com/library/detail.aspx?g=d2011572-dd37-4709-a283-0f2171ab7c3d Accessed 22/08/2016 at 6.14pm

[54] Eric Barbry, 'The Internet of Things, Legal Aspects What Will Change (Everything)…' 2012 Digiworld Economic Journal, no. 87, 3rd Q. 2012,http://repec.idate.fr/RePEc/idt/journl/CS8705/CS87_BARBRY.pdf page 14 Accessed 22/08/2016 at 6.14pm

pedestrians[55] Laws addressing liability at this stage will therefore be difficult to propose as regulators grapple with unfurling problems that open new vistas for legislation and regulation. Traditionally, a consumer could bring a product or service liability claim for defective products or shoddy services but it still has to be determined whether product malfunction or transmission of wrong information by devices will entitle one to a valid claim under the law especially where there is no subsisting contract to lay a claim upon. However, the industry must consider consumer protection in enabling IoT connections and regulators must watch out for signs of consumer detriment.

Remarkably, the first IoT class action (Cahen v. Toyota Motor Corporation, U.S. District Court of Northern California, San Francisco Division)[56] was brought against Toyota Motor Corporation, Ford Motor Company and General Motors LLC. in March 2015 prompted by a report uncovering threats in automobiles that made them vulnerable to hacking and remote manipulation of functions such as the braking, steering and acceleration in breach of the warranty that the vehicles were free from defects. The action though still pending is indicative of the fact that IoT device manufacturers need to employ utmost caution to prevent threats to users.[57]

5.4 Ownership of Intellectual Property Rights (IPR) and Digital Rights Management (DRM)

The IoT will call in questions of who owns what information within the network of connections and the legal responsibility for unauthorised use of Intellectual Property Rights (IPR). The IoT will witness the interaction between several actors in terms of data ownership such as users, manufacturers, data analysts, software developers, data controllers, 'things' etc. with no clear cut ownership rights. Given the potential of data for targeted advertising, marketing, understanding consumer preferences and restructuring company strategy, rules for ownership will require urgent regulatory attention.[58]

---

[55] Bernhard Petermeier, AI: how can we manage robot risk? World Economic Forum. Available at https://www.weforum.org/agenda/2015/01/artificial-intelligence-how-can-we-manage-the-robot-risk/ Accessed 30/08/2016 at 11.21 am

[56] See Cahen, et al. v. Toyota Motor Corporation, et al., U.S. District Court of Northern California, San Francisco Division, Civil Action No. 4:2015cv01104.

[57] The Internet of Things and the Inevitable Collision with Products Liability PART 2: One Step Closer By H. Michael O'Brien (NY Metro) on July 15, 2015
Posted in Product Liability, Technology and electronic products
http://www.productliabilityadvocate.com/2015/07/the-internet-of-things-and-the-inevitable-collision-with-products-liability-part-2-one-step-closer/ Accessed 22/08/2016 at 6.14pm

[58] Taylor Wessling, 'Who owns the data in the Internet of Things?' Feb 2014 https://united-kingdom.taylorwessing.com/download/article_data_lot.html Accessed 05/02/2016

Digital Rights Management will be an offshoot of ownership determination. Detrimental practices already existing within the e-book industry that debar digital consumers from owning e-books will find escalation in the light of the IoT as interactions between users' devices will enable e-book platforms monitor the use of e-books by consumers and compel compliance with company policies and rules beyond copyright exceptions. A similar trend is taking root in regard to patent claims by John Deere tractor manufacturers who insist on carrying out all customer repairs on tractors after purchase in view of the assertion that they own the software in the tractors. John Deere asserts that customers own the vehicles subject to the company's ownership of the Electronic Control Unit Software.[59]

5.5 Standardization and Compatibility

The success of the Internet of Things depends strongly on the existence of smooth and effective operation of national and global standards to ensure compatibility between systems. Products will need to interact seamlessly with other IoT products. In 2015 Google also announced the Weave and Brillo initiatives to create both a common language and a common operating system for the Internet of Things.[60] There are also several moves towards security and platform standardisation, with some collaborative efforts occurring between market players such as the AllSeen Alliance established in 2013 by the Linux foundation, which is working on the possibility of having an open interoperable standard between its members (including LG, Microsoft, Panasonic and Sony). The Open Interconnect Consortium is another alliance established in 2014 with over 150 members including Intel, Cisco, GE, Samsung and Hp.[61] Nest is also working with some companies, including appliance makers LG and Whirlpool and lighting companies Osram and Philips, to ensure products can 'talk to each other'.[62] Regulators must however be on the guard to ensure that standardization blocs do not metamorphose into formidable cartels that lock consumers into specific device manufacturer/service provider circles.

In Nigeria, standards' setting is the core responsibility of the Standards Organization of Nigeria which applies the Standards Organization of Nigeria Act 2015. Section 4 of the Act gives the standards Council, wide powers to formulate rules on standards and

[59] John Deere, Long Comment Regarding a proposed exemption under 17.U.S.C 1201. Available at http://copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf Accessed 30/09/2016 at 11.32 am

[60] https://developers.google.com/brillo/

[61] See https://allseenalliance.org/ and http://openinterconnect.org/ Accessed 30/09/2016 at 11.32 am

[62] Paul Otto, 'NIST Releases Draft Framework on the Internet of Things'. Posted in Consumer Privacy, Cybersecurity & Data Breaches. 25/09/2015 http://www.hldataprotection.com/2015/09/articles/consumer-privacy/nist-releases-draft-framework-on-the-internet-of-things/ Accessed 30/09/2016 at 11.32 am

specification for commodities, processes and related matters, in collaboration with stakeholders. Default attracts a fine not exceeding NI, 000.00 or imprisonment for a term not exceeding one year or to both such fine and imprisonment. (2) Where a person is convicted under this section, the court may make such order as to the forfeiture or destruction of the material or document in issue at it may think appropriate in the circumstances.- section 15 (1and 2).

5.6 Spectrum Availability

Spectrum management which is the process of regulating the use of radio frequencies to promote efficient use[63] will be pivotal to the IoT. This is because the IoT will certainly require much more internet data than is presently in use. The expected demand of IoT devices must necessarily be matched with sufficiently large spectrum bandwidth that accommodates the array of devices within the IoT ecosystem. Spectrum though regarded as infinite resource is prone to interference by neighboring use[64] and so is rationed by the International Telecommunications Union (ITU) Radio Regulations under the international framework for the utilization of the radio frequency spectrum. Unfortunately, this is detrimental to many emerging nations as allocation is according to present needs and technological capability to the detriment of developing.[65] Nigeria as a developing country needs to challenge this practice to guarantee the nations procures as much spectrum bandwidth as is needed for the IoT.

5.7 Consumer Protection

Consumer protection will be at the centre of the IoT regulation. Consumer protection issues such as lock-in, transparency of terms, insistence on arbitration rather than litigation, disclosure/consent, unfair contract terms, exemption clauses, incessant notifications and enforcement of unfavourable End User Agreements,[66] are just some of the consumer protection issues that regulators will strive to tackle. Obviously, it will be impossible for consumers to read, understand and consent to all data collection requests, terms of use and privacy policies, leading consumers to accept pre-set default options that agree to every request to necessitating therefore that regulators ensure that

[63] Martin Cave, Chris Doyle, William Webb, Modern Spectrum Management, Cambridge University Press, 2007 ISBN 0-521-87669-9

[64] See Anne Flanagan, 'Telecommunications Law and Regulation' Edited by Ian Walden, Oxford University Press 2013. Pg 358

[65] Ibid at page 370

[66] Analysis undertaken in 2008 calculated that it would take 76 working days to read every privacy policy an Internet user encounters in the course of a year. Research shows the median time users spend on license agreements was only six seconds; that 70 per cent of users spend less than 12 seconds on the license page; and that no more than 8 per cent of users read the License Agreement in full. Indeed, this has led some legal scholars to question whether they are actually valid, since consumers do not read them. 101 http://www.bbc.co.uk/news/technology-22772321 Accessed 05/02/2016

terms offered to consumers are acceptable. A balance between the IoT innovation and consumer protection/convenience must be sought.

Consumer Protection Council Act 1992 is the principal legislation on consumer protection in Nigeria.[67] The Act deals mostly with preventing consumer harm occasioned by hazardous products. The council is charged with the responsibility of providing speedy redress for consumer complaints and mandating erring companies to compensate injured consumers. The council must also publish a list of harmful products and organise and undertake campaigns and other forms of activities that improve public consumer awareness[68] . The Act does not however cover such expected IoT areas in depth and will therefore have to be updated to embrace the realities of the IoT trend.

5.8 Competition Law and Lock In

Effective competition is a healthy recipe for consumer protection. However, the IoT will likely reduce the function of competition for users if left unchecked as companies can effectively develop 'things' that only communicate within select circles, thereby shutting out devices of competitors. This will invariably force consumers to acquire devices that can communicate with already existing purchases or face a lock-out technically, resultantly whittling down the essence of the IoT.

The Nigerian Communications Act Competition Practises Regulations, 2007 (2003 No. 19) makes extensive provisions for competition regulation. These Regulations provide further guidance on the standards and procedures for determining substantial lessening of competition[69], anticompetitive acts,[70] abuse of dominance[71] and restriction on mergers by telecommunications licensees[72].

The Consultation Guidelines of the Nigerian Communications Commission Act 2003 should be invoked at this point in Nigeria's technological history. The objectives of this Act clearly require the commission to consult with stakeholders, regulatory and industry professionals and the general public on any issues of the public interest in order to consumer understanding, participation and confidence in regulatory processes. Undoubtedly, The IoT will affect individual consumers and will be ignited by the industry. Therefore a public consultation on the topic is needed to ensure that the

[67] Consumer Protection Council Act 1992 Chapter C25 (Decree No 66 of 1992) Laws of the Federation of Nigeria

[68] Section 2 Consumer Protection Council Act, 1992

[69] Sections 2, 6 and 8 Nigerian Communications Act Competition Practices Regulations, 2007 (2003 No. 19)

[70] Section 11 Nigerian Communications Act Competition Practices Regulations, 2007 (2003 No. 19)

[71] Section 16 Nigerian Communications Act Competition Practices Regulations, 2007 (2003 No. 19)

[72] Section 26 Nigerian Communications Act Competition Practices Regulations, 2007 (2003 No. 19)

industry standards conform to consumer protection and consumers derive value from the trend while guarding against any risks.[73]

6.0 Recommendations

- For the IoT to thrive, the industry must employ user-friendly privacy policies and practices including privacy by design, Privacy Impact Assessment, notice and consent, disclosure and must allow privacy management by consumers through the use of Personal Information Management Systems (PIMS)
- International cooperation on best practises is also key to the proper functioning of the IoT. Concepts such as standardisation, compatibility and better spectrum allocation must be upheld to drive the trend.
- Again, robust data management and analytics should be adopted. Data controllers should enable such practices as data portability, data minimisation, anonymisation and the deletion of raw data to safeguard personal and sensitive information from getting into the wrong hands. The consent of data subjects must also be sought before data is processed and data controllers must be transparent enough to give all relevant information on data collection, purpose and use of data and any exchanges or transfer with third parties. Data controllers must also allow data subjects to view and object to the processing of data from collection to disposal.
- Advance consumer protection principles such as the right of return when company policy is unacceptable and empower consumers to be aware of and enforce consumer rights.
- Regulators and legislators must also ensure that the fast pace of the IoT deployment is matched by activism that predicts and cushions consumer detriment.

7.0 Conclusion

From the foregoing, it can be deduced that the IoT will usher in both benefits and detriments for consumers. Regulators must therefore be proactive in the sphere of the IoT to ensure that the benefits of the concept come to consumers without (or at least with minimal) risks. The IoT will certainly help Nigeria to leapfrog some stages of technological development especially in the fields of agriculture, health care, congestion management, home automation and public safety. It is also clear that without suitable laws, Nigeria will sooner become a destination for low quality, invasive and unfavourable practices unlike other high end countries with more sophisticated laws. Clearly information on the Internet will move up from that inputted by humans such as through uploads and recordings to that gathered and uploaded by devices. Beyond this there will be a higher number of endpoint vulnerabilities and opportunities for security invasions e.g. through hacking. Regulators must therefore at first opportunity demand standards that safeguard consumers and protect data. Standards on IPR, compatibility and competition must be spelt out in addition to a

[73] Section 4 The Consultation Guidelines of the Nigerian Communications Commission Act 2003

targeted clamour for increased spectrum allocation to match the demands of the IoT ecosystem.