INTERNET OF THINGS (IOT): DATA SECURITY AND PRIVACY CONCERNS UNDER THE GENERAL DATA PROTECTION REGULATION (GDPR)

Olumide Babalola

School of Law, University of Reading,
Whiteknights, Reading, United Kingdom

ABSTRACT

Internet of Things (IoT) refers to the seamless communication and interconnectivity of multiple devices within a certain network enabled by sensors and other technologies facilitating unusual processing of personal data for the performance of a certain goal. This article examines the various definitions of the IoT from technical and socio-technical perspectives and goes ahead to describe some practical examples of IoT by demonstrating their functionalities vis a vis the anticipated privacy and information security implications. Predominantly, the article discusses the information security and privacy risks posed by the operationality of IoT as envisaged under the EU GDPR and makes a few recommendations on how to address the risks.

KEYWORDS

Data Protection, GDPR, Information Security, Internet of Things, Privacy.

1. INTRODUCTION

In its simplest form, Internet of Things (IoT) connotes the seamless interconnectivity, inter-relativity, and interaction of animate and inanimate objects towards the performance of specific tasks. The concept or technology enables the smart communication of two or more objects co-existing digitally or otherwise for a pre-determined or anticipated outcome or set of outcomes.

The IoT - a coinage by Kevin Ashton in 1999, a British technocrat who co-created a global standard for radio-frequency identification (RFID) - has become a household name to describe the functionality of artificial intelligence (AI) deployed to initiate and consummate a wide variety of human related activities or provision of services.[1] The notion of IoT surfaced along with the invention of the worldwide web but was used for the first time in 1999 with the principal objective of developing technologies that would enable the cross communication and interconnectivity of remote digital devices as part of the 'embedded computer system.'[2] Porras, et al however conversely argue that the first modern notion of IoT was rather introduced by Mark Weiser in his 1999 article where he mused about 'interconnected devices that disappear into the background of our everyday lives.'[3]

This article first introduces IoT as a relatively new technology enabling inter-relativity of multiple devices through connectivity-enhancing sensors and control systems while the second part reproduces the various definitions of the concept from academic and technical perspectives and the third describes some practical examples of IoT and the fourth part analyses the data

David C. Wyld et al. (Eds): NLP, MLTEC, CLBD, SEAPP, NeTIoT, VLSIE, ITCS, ARIA, DMS - 2021
pp. 309-320, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.112324

security issues plaguing the functionality of IoT whereas the fifth part analyses the privacy concerns in IoT and then then the sixth provides recommendation on solutions to the issues while the last part concludes with a recap of the issues discussed.

2. CONCEPTUAL DEFINITIONS

The various definitions of IoT are coloured by origins and vision and sometimes the perspectives of the author making such attempt. The concept has been interchangeably referred to or conflated with terms like Internet of Everything (IoE)[4], Machine to Machine (M2M),[5] Cloud of Things, (CoT),[6] Internet of People (IoP)[7] and Web of Things (WoT)[8] which terms have been given similar or divergent connotations with the IoT.[9]

However, a number of authors and stakeholders have attempted defining IoT along the line of divergent interests and proclivities. The International Telecommunications Union (ITU) views IoT as 'a global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT)'[10] and in a similar but not identical attempt, the Internet Oriented Vision defines IoT as 'a global infrastructure that enables connectivity between both virtual and physical object.[11]

Some definitions however compartmentalize IoT only in relation to physical objects as opposed to the inter-relativity between animate and inanimate entities. For example, Al- Fagaha, et al argue that IoT is a technology that allows physical objects to perceive, hear, see, analyse and undertake tasks by having them interact to exchange data and, 'relay information to one another, process the information collaboratively, and take action automatically.'[13] This attempt however limits the operationality of IoT to the Internet thereby disregarding the workability of offline digital platforms and their functionalities. In another attempt that overlooks the (human) users of IoT, Whitmore, et al however view IoT as 'a paradigm where everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the internet to accomplish some objectives.'[14]

In creating a basis for researchers and academics to further expound on the definitions of IoT, one of the European Commission's intervention initiatives defined the concept as a universally connected network of infrastructure 'linking physical and virtual objects through the exploitation of data capture and communication capabilities.'[15] Flowing from this, Weyrich and Ebert associate IoT with 'innovative functionality and better productivity by seamlessly connecting devices'[16] but in a more elaborate approach, Tarkoma and Katasoner define the concept as 'a global network and service infrastructure of variable density and connectivity with self-configuring capabilities based on standard and interoperable protocols and formats (which) consists of heterogenous things that have identities, physical and virtual attributes and are seamlessly and securely integrated into the internet for clarity.'[17] This definition aligns with notion that socio- technical dimensions to IoT envisages the interaction of the mechanical components with their non-technical counterparts within the same artwork.[18]

3. EXAMPLES OF IOT

Superficially, from the preceding definitions, the concept of IoT appears abstract but with the paradoxical [36] intrusion of technology into homes and private affairs, IoT lives with an average human that envisaged. In this part, I will briefly discuss some contemporary examples or manifestations of IoT around.

3.1. Smart homes or automated homes

These are houses or living environments where technology is used to monitor or control the home appliances remotely in two folds: one consists of the automated home devices and the other relates to their interface, processing and intercommunication.[37] The introduction of IoT into homes remotely controls and coordinates the occupants' individual or joint security needs, medical needs, entertainment preferences, business services, occupational needs and other living needs.[38]

Since smart homes are equipped with ICT which anticipates and responds to the needs of occupants of a house, they necessarily perform their functions after analysing the users' personal information in relation to those needs and the repeated processing activities outside occupants' control raise presumptions of privacy invasion and misuse of such personal data.[39] Within the IoT and Smart homes network, personal data are collected, shared, exchanged and transmitted between several exposed platforms in a manner that robs the users of reasonable control over such personal information and thereby puts them in imminent and imagined risks of privacy violation.[40]

3.2. Wearable devices

Wearable devices are electronic or digital gadgets and software integrated into clothing or worn as accessories for processing information from time to time.

They are manufactured with in-built sensors that enable them track day to day activities of users by syncing them with remote mobile devices. These devices by their operational nature periodically collect users' personal data, share them with other remotely connected devices and ultimately store them in clouds making them vulnerable to attacks, data leakages and breaches with the ultimate end result of privacy invasion. Wearable device like smart bracelets or smart glasses utilize sensors to capture users' sensitive data like pulse, heart rate, blood lipid, blood pressure and other health data and synchronized with health centres' devices to detect early symptoms or supervise health status.[41]

The privacy gaps in the processing activities undertaken by the operators of the wearable devices are accentuated by lack of uniform industry regulation on their transmission formats, encryption and confidentiality especially regarding the further use or indefinite storage of the personal data collected on daily basis. [42]

3.3. Automated vehicles (AV)

Automated vehicles are also referred to as 'fully automated vehicles' or self-driving cars' or 'driver-less cars.'[43] These vehicles are automated to function without human drivers but their navigation is aided by algorithm and sensors using cameras, imaging technology and location-sensitive chips to gather information about the vehicle's location and other information which impart the vehicle owners' expectation of privacy.[44] Most personal data processed during the operationality of AVs are stored in the cloud outside the control of users within the custody of third parties who do not have direct contact with users and provide no guarantees against misuse of such sensitive personal data.

4. INFORMATION SECURITY IN IOT

The ubiquity and dynamism of IoT explicably exposes the technology to a wide array of data security issues.[45] Porras identifies nine primary categories of security concerns raised within IoT as: environmental constraints, vulnerable devices, data security, functional constraints, enforcement mechanism, cross device dependencies, identification, authentication and authorization, control legislation and attacks- threats, modes. [46] However, the concern of this borders on data/ information security – a term often conflated or confused with cybersecurity. While cybersecurity refers to the 'collection of tools, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and users' assets, [47] information security on the other hand is 'the protection of information and its critical elements including the systems and hardware that use store and transmit that information.[48]

In the context of IoT, data security borders on confidentiality, integrity, availability, accuracy, authenticity, utility, and possession of personal information within the confines of the relevant data privacy laws applicable in the respective jurisdictions of the IoT concerned. I shall consider some of this in turn.

4.1. Data confidentiality and integrity

Confidentiality and integrity are one of the universal principles of data protection. The EU General Data Protection Regulation (GDPR) mandates data controllers to ensure appropriate security of personal data against accidental loss, destruction or damage through formidable technical or organization measures. [49] By the nature of IoT, massive complex processing activities take place simultaneously necessitating appropriate data confidentiality and integrity mechanisms to prevent loss or destruction of personal information. Contemporary and modern techniques must be employed to shield access to personal data from authorized third parties or malicious destruction. In this light, Chanal suggests some confidentiality-preservatives like Message-Digest (M05), Ellipte Curve Cryptography, Advanced Encryption Standard (AES) and Algorithms for efficient communication in IoT without the fear of eavesdropping, theft of personal data or compromise of the information in any form. [50]

While access control and cryptography have been suggested as mechanisms that reduce the risk of data manipulation, unauthorized access or misappropriation in IoT, their protective coverage do not extend to already disseminated or transmitted personal data but Minch alternatively advises the use of confidential policy in IoT to analyze information flow which ought to culminate in information policies for the networked systems.[51]

4.2. Data accuracy

This is another principle of data protection deeply rooted in the OECD principle of data quality.[52] It stipulates that personal data stored by entities must reflect the true and correct information of data subjects and where they are outdated, such data must be updated or deleted completely. For the IoT, data accuracy is regulated by the source of collection of data and ultimately the storage mechanism which ought to facilitate periodic and necessary updates.

Personal data is the lifeblood of IoT, because they provide the link between the connected devices on one hand and clarity on the nature of expected outcome via the intercommunication of the entities involved, hence, the quality and accuracy of the personal information transmitted within the interconnected entities must not only be verified but sustained.

Karkouch however notes that while data quality or accuracy in IoT is vitiated by: deployment scale, sensors, constrained resources and intermitted loss of connection, these negative effects can be cured by various relevant data cleaning techniques. [53] Inaccurate (personal) data processed within the IoT system does not only violate data protection principles and users' rights, it compromises the objectives and outcomes of the IoT processing activities making it unreliable of unfit for purpose. In exercise of the right of access [54] to their personal information processed in IoT, users can request from the operators of such technologies, copies of their personal data processed to ensure accuracy of data and as well as ensuring transparency of processing activities involved in the IoT ecosystem when it is ultimately, considered that, IoT could constitute problems to their operators or users where personal data used are inaccurate or outdated.

4.3. Misuse or unauthorised possession of (personal) data

The main objective of data security is prevention of data breach in the form of data loss-(availability breach) or misuse of personal data (utility breach). The risks of data breach vary for different kinds of devices in a IoT network, hence, the need for appropriate and befitting IoT security measures for the respective systems. IoT security is 'a technology area that addresses the protection of the security and privacy of data and information in the physical world as well as in the digital world.' [55]

The IoT functionality involves some external and exposed cross-transmission of personal data on various platforms which may be intercepted by middlemen and third parties through the use of sniffing stations.[56] Other security issues such as robustness, reliability, safety, resilience, performability and survivability may also plague data IoT but it must however be noted that while all these issues impact vehicular data, they do not all relate to personal data as far as IoT security is concerned.[57]

5. (INFORMATION) PRIVACY IN IOT

The functionality of IoT thrives in a multitude of data processing activities. Personal data are used to assess users' preferences, lifestyle, social activities and to ultimately create a profile for marketing or other purposes. Informational privacy is the shade of privacy that interplays with IoT when users' information are shared between several interconnected devices to provide certain services, thereby exposing the users to privacy risks. While one concedes that the IoT's utility of personal data ultimately improves service delivery by making them unusually seamless, however this advantage ought to be balanced against the essentiality of right to privacy especially where the data are amassed without (informed) consent or legal basis. [58]

Consent, in this context is, any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her [59] while informed consent in IoT refers to 'the process by which a fully informed user participates in decisions about his or her personal data.' [60] Like found in some online transactions, the ubiquity of IoT however sometimes makes it impracticable for informed consent to be sought and obtained especially since consent envisages an affirmative indication of agreement to surrender data for certain purposes.

Privacy of IoT always raises the issue of trust since the network of devices utilize massive personal data which processing ought to align with users' expectations of privacy and other freedoms. In IoT, the personal data processed may reveal information on users' location, financial data, health data, home, family, sexuality etc. hence the paradigm requires protection of

these sensitive data to guarantee users privacy even when exchanged on varying platforms over which the users do not have reasonable control. [61] Ziegeldorf et al argue that 'the increasingly invisible dense and pervasive collection, processing and disseminating' of users' personal data raise serious privacy concerns for IoT enablers like RFID, wireless sensor networks (WSN), web personalization and mobile application platforms. [62]

Privacy in IoT guarantees tripod protection for users to wit: (a) transparency risks posed by AI in IoT (b) personal autonomy over personal data collected and (c) knowledge and control of future utility of personal data, all through five different type of information flows of interaction, collection phase, processing, dissemination, and presentation phases. [63] Even though all the phases technically constitute data sharing and processing phases, they depict the IoT's cycle of personal data handling in the light of magnitude of personal data surrendered by users' to IoT and their consequential exposure to privacy risks.

6. MANAGING PRIVACY AND SECURITY RISKS IN IOT UNDER THE GDPR

Many authors [64] have proffered technical solutions for addressing security and privacy risks in IoT but our concern here relates to the legal or regulatory management of information privacy and security in the networked technology. The GDPR which now represents the global benchmark for data privacy [65] is applicable to IoT in so far as it processes the personal data of EU residents or operated by an EU-based entity or targeted at EU customers.[66] Operators or manufacturers of IoT (as data controllers) are obligated under the GDPR to take certain measures to ensure data security and privacy of users of their products.

6.1. Identifying the controller(s) in IoT systems

The whole essence of data protection laws especially the GDPR is the apportionment of liabilities and responsibilities to the stakeholders in every relevant data processing eco-system. Under the GDPR, while the 'controllers' determine the purpose(s) and means of processing personal data, the 'joint controllers' are two or multiple controllers that jointly determine means and purpose of processing and then 'processors' are engaged under contract with definitive terms to process personal data on behalf of controllers, while 'recipients' are either employees or other entities to which personal data are disclosed and 'third parties' are entities who does not qualify as any of the preceding parties listed here.[67]

In IoT systems a decision on the party responsible for ensuring privacy and data security must necessarily begin with an inquiry into whether or not the developer or manufacturer or seller of IoT is the controller, joint controller or processor. Recital 78 and article 25 GDPR requires a controller to consider and implement the principles of data protection at the point of determination of the means of processing and its implementation and with respect to processors, article 28(1) (b) also requires the implementation of 'appropriate technical and organizational measures' to protect personal data.

The complex nature of processing activities undertaken by independent developers of certain components [68] of IoT systems render them liable to qualify as joint data controllers or independent controllers except in rare cases where they may not process personal data in the developmental stages.[69] Hadzovic however identifies a host of other players in the IoT network with varying data processing roles to wit: data manager, service providers, IoT data provider, IoT framework provider, IoT data application provider, IoT data carrier etc.[70] Ultimately, every developer of a component in an IoT network is independently or jointly responsible for ensuring protection of privacy by implementing the GDPR principles except personal data was not

processed during developmental stages. The table below illustrates the apportionment of responsibilities under the GDPR but for this purpose of this paper, we are only concerned with the systems developers, components developer, IoT users and IoT managers.

Actors	Designation undo GDPR	Responsibility under the GDPR
IoT systems developer	Controllers	Design IoT to incorporate data protection principles like data minimization storage limitation, lawfulness of processing & transparency, confidentiality and integrity etc. (GDPR, art.24)
IoT component developer	Controllers, joint controllers, or processors (depending on terms of engagement)	Comply with the obligations of controllers, and/or as processor provide sufficient guarantees to implement appropriate threshold and organizational measures (GDPR, art. 28)
IoT Users/ consumers	Joint controllers/ independent controllers	Ensure the utility of IoT does not violate others' data privacy rights and fulfil obligations under the GDPR.
IoT managers	Controllers/processors. (Depending on the stage they come into the picture.)	Ascertain the compliance of IoT with GDPR principles and ensure the regulatory measures are implemented to minimize risk of data privacy rights violation.

6.2. Use of privacy statements

IoT collect information round the clock for intermittent use and sometimes store them indefinitely hence, users of IoT platforms are entitled to information on how, why and when their personal data are collected, stored and used. Article 13 GDPR guarantees data subjects right to information on: (a) identity (b) identify of controller, details of data protection office, purpose of process (c) legitimate interest (d) recipients etc.

Operators of IoT can fulfil their obligation to provide information by utilizing privacy statements. These are either designated as privacy notice or policies that fully explain entities' collection purpose, use, storage, and overall management of personal data and therein giving the users a choice over their preference for processing activities on their personal data. These statements enable users develop trust in the IoT systems and reduce the apprehension of privacy risks more so through the data controllers' transparency as clearly spelt out in the statements. Ultimately, to achieve optimum result, privacy policies/notices in IoT ought to be summarized to aid comprehension, categorized, well organised, and automated into the respective systems.[71]

6.3. Data protection by design and default

This is one of the hallmarks of the GDPR which introduced an additional obligation on data controllers (IoT manufacturers in this context) to integrate, at the point of construction 'Privacy-Enhancing- Technologies' (PETs) and throughout the life cycles of the IoT.[72] Article 25 GDPR

imposes a duty on IoT manufacturers and operators to integrate technical and organizational measures in the system, to fulfil the data protection of personal data and privacy of users.

In integrating privacy by default and design in IoT, manufacturers must identify and ascertain the legal basis to process users' information, ensure security of information collected and prevent misuse of such personal data which must not be stored for more than necessary and minimize the quantum of irrelevant data collected by the devices in the network. Article 29 Working Party recommends the utility of 'shielding techniques' or 'kill commands' to address unauthorized or unanticipated tracking of personal data belonging to users of IoT. [73] For enhancement of privacy in IoT, Larrieux suggests the use of other PETs like 'thresholding the transmission of information based on signal strength, protecting passwords and using hash-locks or metalDs.'[74]

7. CONCLUSION

With the rise in human dependence on IoT comes privacy and security challenges associated with the intrusive and invasive tendencies of the ubiquitous technology. Of all issues militating against IoT, privacy and security concerns rank top in spite of the seaming wilful surrender of personal information by users – this underscores the privacy paradox of IoT platforms.

In this article, I have briefly discussed the origin of IoT as well as the various academic definitions of the concept to show its nature, objectives and nuances. I have also analysed how privacy and data security constinue to pose threats to the seamless utility and operationalism of IoT and here, I have also proffered some quick or long fixes to the process.

REFERENCES

[1] Keyul K. Patel & Sunil Patel, (2016) 'Internet of Things - IoT: Definitions, Characteristics, Architecture Enabling Technologies, Application and Future challenges' 6(5) IJESC, VOL. 6 NO. 5, p 6122.

[2] Jorge E. Ibara-Esquer et al, (2017) 'Tracking the Evolution of Internet of Things Concept Across Different Application Domains' Sensors Journal, Vol. 17, p1.

[3] Jari Porras, et al, (2018) 'Security in the Internet of Things- A Systematic Mapping Study' Proceedings of the 51st Hawaii International Conference on System sciences.

[4] Langley et al argue that IoE is an expanded and broadened version of IoT by throwing people, business and other processes into the mix. They describe IoE as 'a network of connections between smart things, people, processes, and data with real-time data/information flows between them.' See David Langley, (2021) 'The Internet of Everything: Smart Things and their Impact on Business Models' Journal of Business Research, Vol. 122, pp853 – 863.

[5] Kalyani et al view M2M as an application of IoT which utilizes sensors to enable communication between devices of same type. In other words, the IoT's functionality is aided by M2M via merger of wireless technologies and smart sensors. See Vijay Laxmi Kalyani et al, (2015) 'IoT: 'Machine to Machine' Application A Future Vision' Journal of Management Engineering and Information Technology, Vol. 2 No. 4, p15. Chen emphatically says, IoT is also known as M2M. See Yen-Kuang Chen, (2012) 'Challenges and Opportunities of Internet of Things' 7th Asia and South Pacific Design Automation Conference, pp. 383-388, doi: 10.1109/ASPDAC.2012.6164978.

[6] This is the integration of cloud computing and IoT. See D. Vaishnavi, (2018) 'Towards Cloud of Things from Internet of Things' International Journal of Engineering & Technology, Vol. 7 No. 4, p112-116.

[7] Proposed as 'a radically new human-centric approach to Internet data and knowledge management' with emphatic focus of the users of the paradigm as opposed to the orthodox IoT that is quite distant from humans but more fixated on the inanimate players in the network. See Marco Conti and Andrea Passarella, (2018) 'The Internet of People: A Human and Data-Centric Paradigm For the Next Generation Internet' Computer Communications, Vol. 131, p51 – 65.

[8] This 'invention' enables 'physical devices to connect to the Internet as well as provide their services as a resource on the web' with the principal purpose of linking physical objects to the web. See Muhammad Rehan Faheem, Tayyaba Anees, & Muzammil Hussain, (2019) 'The Web of Things: Findability Taxonomy and Challenges' IEEE Access, 1.

[9] Alem Colakovic and Mesud Hadzialic, (2018) 'Internet of Things (IoT). A Review of Enabling Technologies, Challenges and Open Research Issues' (2018) Computer Networks, Vol. 114, pp17-39.

[10] Global Information Infrastructure (2021) Internet Protocol Aspects and Next Generation Networks. Next Generation Networks- Frameworks and Functional Architecture Models: Overview of Internet of Things ITU- Recommendation Y. 2060 server Y.

[11] Colakovic and Hadzialic (n 9) pp17-39.

[12] A. Al-Fuqaha, Mohsen Guizani, Mohammed Aledhari and Moussa Ayyash, (2015) 'Internet of Things: A survey on Enabling Technologies Protocols and Applications' IEEE Communication Surveys &Tutorials, Vol. 17 No.4, 2347.

[13] See Yen-Kuang Chen, (2012) 'Challenges and Opportunities of Internet of Things' 7th Asia and South Pacific Design Automation Conference, pp. 383-388, doi: 10.1109/ASPDAC.2012.6164978.

[14] Andrew Whitmore, (2015) 'The Internet of Things - A Survey of Topics and Trends' Information System Frontiers, Vol. 17, p261-274.

[15] CASAGRAS Partnership (2009) Final Report: RFID and the inclusive Model for Internet of Things: EU Project (216803) European Commission, London UK.

[16] Michael Weyrich and Christof Ebert, (2000) 'Reference Architecture for the Internet of Things' IEEE software, 1.

[17] Sasu Tarkoma and Artem Katasanov, 'Internet of Things Strategic Research Agenda (IoT- SRA) Finish Strategic Centre for Science, 1.

[18] Theo Lynn et al, (2000) 'The Internet of Things: Definition, Keep concepts and Reference Architectures' in Theo Lynn, John G. Mooney, Brain Lee and Patricia Takako Endo, (eds) *The Cloud to thing Continuum, Opportunities and Challenges in Cloud, Fog and Edge Computing*, Palgrave Macmillan, 1.

[19] Luigi Atzori, (2010) 'The Internet of Things: A Survey' Computer Networks, Vol. 54, p2787-2805.

[20] Sachin Kumar et al, 'Internet of Things is a Revolutionary Approach for Future Technology Enhancement: A Review, Journal of Big Data, Vol. 6, No. 111, p1.

[21] Somayya Madakam et al, (2015) 'Internet of Things (IoT): A literature Review' (2015) Journal of Computer and Communications, Vol. 3, 164-173.

[22] Owais Ahmed, (2019) 'Internet of Things (IoT) A Review' International Journal of Research in Engineering Application & Management, Vol. 4, No. 10, p2454.

[23] Mohd Muntjir et al, (2017) 'An Analysis of Internet of Things (IoT): Novel Architectures, Modern Applications, Security Aspects and Future (2017) IJERT, Vol. 6, No.6, p422.

[24] Jaimon T. Kelly, (2020) 'The Internet of Things: Impact and Implications for Health care J Med Internet Res. Vol. 22, No. 11, 1.

[25] Kenyur Patel and Sunil M. Patel, (2016) 'Internet of Things – IoT: Definition, Characteristics, Architecture Enabling Technologies, Application and Future challenges' IJESC, Vol. 6, No. 5, 6122.

[26] R. Nandhini, R. Aparna and P. Srilakshmi, (2018) 'Study on Security Issues in Internet of Things' International Conference on Social Impact of Internet of Things (IoT), p130.

[27] I.C.L. Ng and S.Y.L. Wakenshaw, (2017) 'The Internet-of-Things: Review and Research Directions' International Journal of Research in Marketing, Vol. 34, No.1, p3-21.

[28] Poornima Chanal and Mahabaleshwar S. Kakkasageri, (2021) 'Preserving Data Confidentiality in the Internet of Things' (2021) SN Computer Science, Vol. 2, p53.

[29] Charith Perera, '(2006] Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms' < https://www.researchgate.net/publication/307967586_Privacy-by-Design_Framework_for_Assessing_Internet_of_Things_Applications_and_Platforms/link/5a42776eaca272d29458fe8e/download> accessed 2 August 2021.

[30] Aimad Karkouch et al, [2015] Data Quality Enhancement in Internet of Things Environment' IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA).

[31] Vijay Laxmi Kalyani et al, [2015] 'IoT: 'Machine to Machine' Application A Future Vision' Journal of Management Engineering and Information Technology, Vol. 2, No. 4, p15.

[32] D. Vaishnavi, (2018) 'Towards Cloud of Things from Internet of Things' International Journal of Engineering & Technology, Vol 7, No.4, p112-116.

[33] Lo'ai Tawalbeh, (2020) 'IoT Privacy and Security: Challenges and Solutions' Applied Sciences, Vol 10, p1.
[34] Jan H. Ziegeldorf et al, (2014) 'Privacy in the Internet of Things: Threats and Challenges' Security and Communication Networks, Vol. 7, No.12, p2728.
[35] Baoan Li, et al, (2011) 'Research and application on the smart home based on component technologies and Internet of Things' Procedia Engineering, Vol. 15, p2087.
[36] In this context, privacy paradox refers to the 'documented fact that users have a tendency towards privacy-compromising behavior online which eventually results in a dichotomy between privacy attitudes and actual behavior' See Susanne Barth, (2017) 'The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behaviour – Asystematic Literature Review' Telematics and Informatics, Vol. 34, p1038.
[37] Jyotsna Gaghane et al, (2011) 'Smart Homes System Internet of Things: Issues, Solutions and Recent Research Directors' International Research Journal of Engineering and Technology, Vol. 4, No.5, 1965.
[38] Baoan Li, (n. 35) p1.
[39] Frances K. Adrich, (2003) 'Smart Homes: Past Present and Future' in R. Harper (ed) *Inside Smart Homes*, Springer, London, pp17-39
[40] Nadine Guhr, et al, (2020) 'Privacy Concerns in the Smart Home Context' (2020) SN Applied Sciences, Vol. 2, No. 247, 1.
[41] Dawei Jiang, et al (2021) 'Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare' Journal of Healthcare Engineering, Vol. 2021, 1.
[42] Ibid.
[43] Wolfgang Gruel et al, (2016) 'Assessing the Long-Term Effects of Autonomous Vehicles: A Speculative Approach' Transportation Research Procedia, Vol. 13, 18 - 29
[44] Rushit Dave et al, (2019) 'Efficient Data Privacy and Security in Autonomous Cars' Journal of Computer Science and Application, Vol. 7, No.11, p31-36; T.K. Chan, CS Chin, 'Review of Autonomous Intelligent Vehicle for Urban Driving and Parking' (2021) 10(9) Electronics, 1021, T. K. Chan, et al, 'A Comprehensive Review of Driver Behaviour Analysis Utilizing Smartphones' (2020) 21(10) IEEE Transations on Intelligent Transportation System, 4444-4475.
[45] In this article information security is used interchangeably with data security.
[46] Porras (n 3).
[47] Rossouw von Solms and Johan van Nickerk, (2013) 'From Information Security to Cybersecurity' (2013) Computers & Security, Vol. 38, p97-102.
[48] M.E. Whitman & H.J. Mattord, (2009) *Principles of Information Security*, 3rd ed. Thompson Course Tech., 8.
[49] GDPR, recital 39, 49, 75, 83, 85 article 5(1)(f).
[50] Poornima Chanal and Mahabaleshwar S. Kakkasageri, (2021) 'Preserving Data Confidentiality in the Internet of Things' SN Computer Science, Vol. 2, p53.
[51] See Tri Ngo Minh, 'Confidentiality and integrity for IoT/Mobile Networks' (2019) < https://www.intechopen.com/chapters/68117> accessed 15 September 2021.
[52] Fred H. Cate, Peter Cullen, and Victor Mayer-Schonberger, (2014) 'Data Protection Principles for the 21st Century, Revising the 1980 OECD Guidelines' < https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf > accessed 6 May 2021.
[53] Aimad Karkouch et al, (2015) Data Quality Enhancement in Internet of Things Environment' IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA).
[54] GDPR, art. 15(1).
[55] Nina Olinder, et al, (2020) 'Personal Data Protection in the Internet of Things' Advances in Economics, Business and Management Research, Vol. 171, p227.
[56] Carsten Maple, (2017) 'Security and Privacy in the Internet of Things' Journal of Cyber Policy, Vol. 2, No. 2, p154.
[57] James Sterhenz et al, (2010) 'Resilience and Survivability in Communication Network, Strategies, Principles and Survey of Disciplines' Computer Networks, Vol. 54, No. 8, p1245.
[58] Maple (n 55).
[59] GDPR, art. 4(11).
[60] T. van der Geest et al, (2005) 'Informed Consent to Address Trust, Control and Privacy Concerns in User Profiling' Privacy Enhanced Personalization, 23-34.

[61] S. Sicari et al, (2015) 'Security, Privacy, and Trust in Internet of Things: The Road Ahead' Computer Networks, Vol. 76, p146-164.
[62] Ziegeldorf (n 34).
[63] Ibid.
[64] W. H. Hassan, (2019) 'Current Research on Internet of Things (IoT) Security: A Survey' Computer Networks, Vol. 148, p28
[65] Christoper Kuner et al, (2020) *General Data Protection Regulation (GDPR). A Commentary,* Oxford University Press, London, p2.
[66] GDPR, art. 2 and 3 provide for material and territorial scopes of the regulation.
[67] See GDPR articles 4(7), 26, 4(8), 4(4) and 4(10) respectfully.
[68] These consist of the device, IoT area network, gateway, access network is network, IoT platform and IoT application server. See International Telecommunication Union, 'Requirement of the network for the Internet of Things' (2016) < https://www.itu.int/rec/T-REC-Y.4113/en> accessed 15 September 2021.
[69] Jiahong chen et al, (2020) 'Who is responsible for data processing in smart houses? Reconsidering joint controllership and the household exemption' International Data Privacy Law, Vol. 10, No.4, p279.
[70] Suada Hadzovic et al, 'Identification of IoT Actors' (2021) 21 Sensors, 2093.
[71] Julia B, Earp, (2005) 'Examining Internet Privacy Policies within the Context of User Privacy Values' IEEE Transactions on Engineering Management, Vol. 52, No.2, p227.
[72] Lee Bygrave, (2017) 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' Oslo Law Review, Vol 4, No.2, p106, Woodrow Hartzog, (2018) *Privacy Blueprint: The Battle to Control the Design of New Technologies,* Harvard University Press.
[73] See Article 29 Data Protection Working Party. 'Working Document on Data Protection Issues delated to RFID Technology' (2005) < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf> accessed 15 September 2021.
[74] Aurelia Tamo – Larrieux, *Designing for Privacy and its Legal Framework, Data Protection by Design and Default for Internet of Things,* Springer Nature, Switzerland, 2018.

AUTHOR

Olumide Babalola, the author of Casebook on Data Protection (Nigeria's first and only law textbook on data protection) is a prolific and consummate digital rights, consumer rights, privacy and data protection lawyer. His rich and diverse digital rights litigation experience spans across all superior courts of records in Nigeria and regional courts in Africa including ECOWAS Community Court of Justice. He has specifically litigated on Privacy and Data Protection, Cybercrime, Hate Speech, Freedom of Information, Online Freedom of Expression, passage of laws protecting digital rights among others. Olumide is a seasoned Conference speaker at local and international fora. In 2019, he spoke at the RightsCon (The 8th Annual Summit on Human Rights in the Digital Age) held in Tunis and UN Internet Governance Forum in Berlin, 2019, among others.

Olumide has five published books to his credit: the first is a historical piece on the office of the attorney general of the federation and its occupants in Nigeria; the second being a casebook on Labour and employment law - which work was propelled by the volume of legal opinions (on Nigerian Labour regime especially the decisions of the courts on the peculiar issues) he had to write for his multi-national company on regular basis while the third is another casebook on corporate law and practice; Babalola's Law Dictionary, is reputed as Nigeria's first law dictionary (strictly so called) and his latest being a Casebook on Data Protection.

Olumide is the managing partner of Olumide Babalola, LP - his flagship full-service law office with particular bias for digital rights, consumer rights litigation, class actions, employment and corporate commercial litigation et al. The awardee of the "Nigerian Rising Star Award" is a member of the Nigerian Bar Association, Secretary of NBA Lagos Human Rights Committee, British Nigeria Law Forum, Internet Society, Internet Governance Forum Support Association (IGFSA), Chartered Institute of Arbitrators (UK), World Litigation Forum, International Bar Association, International Association of Privacy Professionals and International Network of Privacy Law Practitioners. (INPLP)