AN ETHICS AND PRIVACY FRAMEWORK FOR THE INTERNET OF THINGS

C. P. NNADOZIA[1] O.C OKEKE[2]
[1,2]Department of Computer Science COOU Uli, Anambra State, Nigeria

ABSTRACT
This research is about an ethics and privacy framework for the internet of things. The IoT research is lagging in terms of ethics and privacy frameworks. Existing regulations about IoT and violation of privacy is inadequate. The purpose of this research is to study existing an ethics and privacy framework for their adequacy. The research hopes to answer questions on the ethical and privacy challenges of the IoT and to answer questions on the adequacy of the regulation relating to IoT and adequacy of the existing ethics and privacy framework for the IoT. The related work was reviewed under security challenges, ethics challenges, privacy challenges regulatory legislation and existing frameworks and the inadequacy of existing frameworks were noted while the varied nature of the researchers agreement was noted. The conclusion is that there is a need for an ethics and privacy framework for the internet of things.

Keywords: Internet of things, framework, privacy, ethics, security

1. INTRODUCTION

The internet of things is an emergent technology which is comprised of smart objects and things with sensors able to sense and collect information from the environment and transmits and act based on this information collected. The IoT is seen by researchers as a technology that will disrupt the status quo as it is. A lot of research has gone into the capability, capacity and the ability of the internet of things. The security, ethics and privacy of the internet of things are lagging behind all other aspects of IoT research (Weber 2013). Existing regulation for data from the internet of things are said to be inadequate for the possibilities. Alrawais (2017) asserts that research into security and privacy of the internet of things still in the early stages. Smart objects working together can solve so many existing problems ranging without a framework will routinely infringe on the privacy of the users about who the data is being gathered. The purpose of this research is to study ethical and privacy governance framework for managing the data generated by the internet of things which will prevent ethical and privacy violation. This topic was selected because of its relevance to the development of internet of things today which is ubiquitous and found everywhere from the smart city to personalized health care to just in time manufacturing and inventory control to crime fighting. Without a framework, the internet of things will become a huge tool for routine privacy violations.

1.2 Research questions

The research questions which this research work hopes to answer will be as follows:
RQ1: what are the ethical challenges of the IoT?
RQ2: what are the privacy challenges of the IoT?
RQ3: what are the downsides of the robust security and ethical framework?
RQ4: what is the adequacy of the regulations relating to the IoT?
RQ5: what is the adequacy of the existing ethics and privacy frameworks for IoT?

2. REVIEW OF RELATED LITERATURE

2.1 Security challenges

There are different views and no consensus on the security and privacy challenges of the internet of things. These problems vary from lack of standardization to problems of interoperability of generating sensors and collecting storage media. LeeI and LeeK (2015) sees challenges in IoT development as data management, data mining, privacy, security and chaos challenge.

The ubiquitous internet of things poses challenges both for the security and privacy of individuals on whose data is being collected about their activities including Locations and other various identifiable attributes which can be used to build a personal profile or analyzed to detect patterns not immediately visible. Borgohain and Kumar (2015) classified security challenges of the IOT as threefold; Attacks on secrecy and authentication, silent attacks on service integrity and attacks on network availability.

2.2 Ethics challenges

The ethical challenges of the internet of things are many and varied and researchers are not in agreement. As the technology is still in its infancy as it develops even more ethical issues and quagmires will arise.

The expert group of the European Commission has identified six key ethical issues, namely social justice, trust (exceeding the traditional notions of reliance and confidence), the blurring of contexts (private vs. public), the non-neutrality of IoT metaphors, agency (social contract concept), and autonomy (informed consent vs. obfuscation of functionality) Weber (2013). With the existence of these challenges it is important that any future framework of the internet of things will take all these into consideration.

According to Tzafestas (2018) IoT technologies solve many real-life problems but they create serious ethical concerns and legal and these Challenges relate to: _ Protection of privacy, Data security. Data usability, Data user experience, Trust, Safety, etc... All researchers are in agreement that that there is a need for proper regulations and regulatory framework and as at yet these do not exist. Indeed according toTzafestas (2018), the IoT law and ethics framework should involve the following:

_ Legislation/regulations.
_ Ethics principles, rules and codes.
_ Standards/guidelines.
_ Contractual arrangements.

The regulations for IoT should include:

_ Regulations for the devices connected.
_ Regulations for the networks and their security.
_ Regulations for the data associated with the devices.

2.3 Privacy Challenges

Privacy as a universal human right was enshrined in the Universal declaration of human rights in article 12 (united nations 1948). However the existing laws in most countries to protect against privacy violations by the internet of things and smart objects are inadequate.

Ziegeldorf (2013) sees privacy in the IoT as a threefold guarantee to the subject for awareness of privacy risk imposed by smart things, individual control over collection and processing of personal information, awareness and control of personal information. Indeed, this captures the privacy dilemma posed by the internet of things. There is a lot of ignorance ranging from lack of awareness on the part of users posed by the data collected and generated and exchanged by the smart and interconnected devices.

Interestingly Ziegeldorf(2013) approaches this from the perspective of informational self-determination by enabling the subject to access his personal privacy risk , to take appropriate action and to protect his privacy and to be assured that it is enforced beyond his immediate control sphere. In this sense information and education of the user s about any IoT enabled device must be explicit. This is to be the case if the user is to know and understand this personal privacy risk. The subject must also be able to opt out of the information being collected and most importantly he should be informed of what the data being collected will be used for.

2.4 Regulatory Legislation

The European Union is most advanced in having regulations and laws which serve to provide regulatory legislation to the challenges of privacy that emanates from the internet of things. The

European Union general data protection regulation (GDPR) enacted in 2016 is the closest to all-encompassing the privacy issues raised by the internet of things. Not all OECD countries have adequate privacy laws. The United States n does not have an all-encompassing law for data privacy, various aspect of health and financial privacy is managed with the health insurance portability and accountability act (HIPAA) and the Gramm-Leach-Bliley act (GLB) respectively. The privacy law in Canada is the personal information protection and electronic documents act (PIPEDA) enacted in 2000. It relates to data privacy and governed how personal information is collected and used. There is no national data privacy law existing that is designed with the internet of things in mind. Australia for example does not have any sort of privacy law that can serve in this era of the internet of things. Indeed according to Caron*et al*., (2016) Australia has no law that addresses individual privacy. While the need for regulation and laws for regulating the internet of things cannot be over emphasized Weber (2010) affirm that the choice is between national regulation, international agreement and self-regulation. The current situations a mixture of all three with international agreements exists at the European Union level. Different corporations implement different levels of privacy regulation which is a form of self-regulation without input of governments and states. Policies and regulations are urgently needed (Suo et al., 2012)

Research has mostly focused on the technical side of the internet of things especially as applies to the smart city. Weber (2013) points that while the technical aspects are being discussed in detail a legal framework does not exist so far. There is a need for an encompassing framework which will guide the way IoT applications services and artefacts are delivered and deployed. Any framework which is going to be designed for the internet of thing will need to address issues of IoT privacy, data protection, and data security. Weber (2013) identifies these as keys issues of any regulatory frameworks which might exist in future.

The first supranational organization trying to work out an IoT governance framework has been the European Commission by appointing a large group of experts to examine the relevant aspects of a possible IoT governance regime (Weber 2016)

2.5 The Existing Framework

There is no uniformly agreed set of guidelines that exist that is agreed on that any regulatory framework for the internet of things must address. Different researchers have come to different conclusions about what the internet of things must address. Perera advocates adopting Privacy by design (Perera*et al*., 2016) based on minimizing data acquisition , number of data sources , raw data intake, knowledge , data storage , data retention among others.

Berman*et al*., (2017) policy in IoT safety, security and privacy a legal framework for determining appropriate behavior, focus on human right and ethical behavior, and sustainable development of the IoT. A framework for privacy protection proposed by Baldini *et al*.,(2013)

should take into consideration, digital identity, and trust and usage control. Weber (2010) asserts that future legislation encouraging privacy and data protection should have five goals which he stipulated as right to know, prohibition regulation IT security utilization legislation and task force legislation

3. DISCUSSION

There is a need for rules and regulations and by extension frameworks which will guide design of internet t of things enabled devices to ensure they are secure by design. This is because if they are not secure they can be hacked and customer data can be exposed and privacy rights compromised. as lot of problems exist as a result of the race to market where manufacturers are producing internet enabled devices at break neck speed most of them with poor security . Another problem that exists is the situation where manufacturers are trying to make every object internet enabled. This raises questions as to whether it is necessary and whether security has been given consideration in doing all of this. an ethical and privacy framework is necessary for reasons of privacy to ensure that sensitive information like spending habits , medical records and other such sensitive information is to hacked and exposed . . In this regard, there exists problems with existing regulations, they are not just inadequate, and this is exacerbated by the pace at which technology is moving with, frameworks and regulations just playing catch-up. It is thus essential that the right regulations and frameworks are put in place to ensure that these catastrophic risks do not occur. However while frame works are being developed adequate care should be taken to ensure that the frameworks and regulations do not get in the way of technological progress.

3.1 Future Research

The future research into the internet of things should be mostly focused on development of a quasi-rules of engagement, and as internet enabled devices become more common place the need for an ethical framework will become more apparent, future research should focus on the development of an ethical framework for the internet of things, this framework will guide design and use to ensure all rights are respected and privacy is preserved

4. CONCLUSION

The opportunities and prospects of internet of things can only be realized if there are adequate privacy and security frameworks to prevent abuse by those collecting the data. The framework of smart objects and internet of things must be user centered with an aim to protecting privacy. This framework will contribute to existing knowledge of the internet of things.

REFERENCES

Alrawais A ; Alhothaily A ; Hu C ; Cheng X (2017)Fog Computing for the Internet of Things: Security and Privacy Issues IEEE Internet Computing (Volume: 21 , Issue: 2 , Mar.-Apr. 2017)

Baldini G., Kounelis I., Fovino I.N., Neisse R. (2013) A Framework for Privacy Protection and Usage Control of Personal Data in a Smart City Scenario. In: Luiijf E., Hartel P. (Eds) Critical Information Infrastructures Security. CRITIS 2013. Lecture Notes in Computer Science, vol 8328. Springer, Cham

Berman and Cerf V (2017), Social and ethical behavior in the internet of things communications of the ACM February 2017vol. 60 no 2.

Borgohain, Tuhin & Kumar, Uday& Sandal, Sugata. (2015). Survey of Security and Privacy Issues of Internet of Things. International Journal of Advanced Networking Applications. 6. 2372-2378.

Caron X, Bosua R,Maynard SB and Ahmad A.(2016)The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective Computer Law & Security Review Volume 32, Issue 1, February 2016, Pages 4-15 Internet society (2015) the internet of things : an overview

LeeI and LeeK (2015), The Internet of Things (IoT): Applications, investments, and challenges for enterprises Business HorizonsVolume 58, Issue 4, July–August 2015, Pages 431-440

Perera C , Cairn Mc, Cormick C, Bandera AK, Price BA Nuseibeh B (2016) Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms IoT'16 Proceedings of the 6th International Conference on the Internet of Things Stuttgart, Germany — November 07 - 09, 2016

Sadeghi A, Wachsmann C; Waidner M (2015) Security and Privacy Challenges in Industrial Internet of Things DAC '15, June 07 - 11, 2015, San Francisco, CA, USACopyright 2015 ACM 978-1-4503-3520-1/15/06

Suo H , Wan J, Zou C, Liu J (2012) Security in the Internet of Things: A Review 2012 International Conference on Computer Science and Electronics Engineering

The United Nations (1948) Universal Declaration of Human Rights.

Tzafestas s (2018) Ethics and Law in the Internet of Things World Smart Cities 2018, 1, 98–120; doi: 10.3390/smartcities1010006.

Weber R (2010) Internet of Things – New security and privacy challenges comp u t e r law & s e c u r i t y r e v i e w 2 6 (2 0 1 0) 2 3 – 3 0.

Weber R (2013)Internet of things e Governance quo vadis? Computer law & security review 29 (2013) 341e347.

Weber RH (2016)Governance of the Internet of Things—From Infancy to First Attempts of Implementation Laws 2016, 5, 28; doi:10.3390/laws5030028

Ziegeldorf JH, Morchon OG, Wehrle K(2014) Privacy in the Internet of Things: threats and challenges - Security and Communication Networks, 2014 Security Comm. Networks 2014; **7:**2728–274