International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2000-000X
Vol. 3 Issue 1, January – 2019, Pages: 25-32

IOT Politics, Regulations and Civic Engagement

Arwa Sami Abunohaiah1, Qasem Abu Al-Haija2

1Networking and Telecommunications, King Faisal University, Saudi Arabia
2Electrical Engineering Department, King Faisal University, Saudi Arabia
Qalhaija@kfu.edu.sa2, aabunohaiah@kfu.edu.sa1

Abstract – *The Internet of Things (IoT) describes the connection of any devices to the internet using different type of software and sensors to communicate, collect and exchange data with one another. Today there are a plenty of objects and devices connected to the Internet of Things (IoT), each interaction, reacting, responding and collecting data from every interaction. Although the IoT is still in its early stages of growth, it will shortly become common and the number of connected devices is expected to exceed 40 billion by 2024.To Take the advantage of opportunities that the IoT will provide, media companies need to understand their politics and regulations of using IoT, the key for success factors and the IoT domains that they should operate in.*

Index Terms – Policy and Regulation, IoT in homes, personal data, techniques, civic OS, ICT regulators, IoT.

1. INTRODUCTION

A growing in Internet of Things (IoT) provides a huge socio-economic benefits. Governments and regulators can unlock these benefits and drive digital transformation by implementing consistent policies that rise innovation and investment, and that give confidence to consumers and the industry [1].

Applications in the IoT space are likely involve of two parts that contribute together in function and performance. They are also share of data rights, privacy, security, ownership, and on the commitment and responsibilities of the service providers and intermediate parties, as well as the rights of users and customers. Governments and regulators play a considerable role in how such issues are resolved so that the benefits of IoT technologies can be enjoyed by society in a fair way.

1.1. List of policy and regulation [2]

- Technical enforcement of legal IoT regulations, service level agreements, mutual legal assistance requests, and other instruments.
- Privacy and security in cloud services and IoT
- Internet of Things: data sharing, threats, liability, audit and compliance concerns for cloud supported IoT, fog and edge computing
- Application of cloud computing in regulated sectors Emerging cloud and infrastructure
- Service models (X as a Service)
- Issues concerning the interaction between cloud and IoT technologies, and big data and machine learning
- Emerging cloud technologies (decentralized clouds: cloudlets, droplets; containment mechanisms)
- Compatibility issues between regulation and technical implementation
- Cybercrime: phishing, malware and spam proliferation within cloud computing and IoT
- Encryption, security technologies and responsibility
- Issues of surveillance in cloud and IoT architectures
- Anti-discrimination, human rights, privacy and power issues with cloud and IoT
- Interaction between cloud and IoT and consumer-facing business models, including the transformations towards crowd labor, algorithmic decision making and automation

1.2. The Challenge for ICT Regulators

IoT use traditional industry-specific boundaries (as in figure 1) and challenge governance of industry verticals by respective sector authorities (as in figure 2). In addition, success of the IoT is dependent on collection and use of data to provide customized solutions, which poses a considerable threat to consumers' data privacy and security. So there is a new way to develop regulations. But these regulations are being developed independently. So only New York State has issued a global IoT policy, which not only covers data privacy and security, but also plans to make information about IoT infrastructure public and share IoT infrastructure through public-private partnerships. [3]

Policy-makers already appreciate the strong socio-economic benefits to be realized. But the IoT has broadly been unregulated so far, and is developing on its own, with many countries addressing IoT specific requirements on a case-by-case basis. Most of countries are at a relatively more advanced stage, and are conducting detailed consultations on key aspects related to the IoT. A clear regulatory framework can accelerate development of an IoT ecosystem and make it more potential, through the following key benefits

Figure. 1. Enhanced role for ICT service providers

- Fast development of the ecosystem through progressive market stimulation, such as increasing market clarity and promoting entrepreneurship.
- Improving national security through increased security of the aggregate ICT environment.
- Improving protection of rights and interests of users (individuals, enterprises and government).

Figure. 2. Vertical overlap in use cases

2. POLITICS OF SHARING PERSONAL DATA

Now a day's you have seen a spread of digital technologies throughout our lived environments with an increasing of networking technologies that not just let the people connect together immediately around them but also let them connect with deferent people around the world as well. Thus, we now live in a world where increasingly huge amounts of information about us, or others we know, is shared through the use of computing systems. Sometimes they deliberate sharing information, sometimes it is not. occasionally the people with whom we share information are known to us, sometimes they are not. the information Represented as data. Data is being moved between one and another this movement is somehow being managed, either by people themselves or by the systems that are handling the transposition the data. So, as computing systems become an ever-more spread in our lives and are

increasingly embedded in our environments through enabling platforms such as the Internet of Things, we are beginning to have to come to terms with new ways in which information relating to us might be shared or can be managed. This has led to increasingly widespread regarding the implications of topics such as privacy and data confidentiality. The focus of this section is upon Perspectives on the sharing of personal data through computing systems. this data include text, photos, videos, … etc. [3].

2.1 Perspectives on the sharing of personal data

A perspective discusses uniqueness between data that people may Intentionally to share themselves, for example through personal profiles, applications, preferences and posted content such as social media, and data that is delivered to others on their behalf by human- or machine-based agents. Discussions that move beyond the point at which personal data is somehow transfer and collect, we must understand where the data is stored and how its managed This is where concerns about secure the data. [3]

2.2 Basıc Data Anonymısatıon Technıques

Attribute Suppression: Is refers to the removal of an entire part of data (also referred to as "column" in databases and spreadsheets) In a dataset. We use it When an attribute is not required in the anonymized dataset, or when the attribute cannot otherwise be suitably anonymized with another technique. This technique should be applied at the start of the anonymization process, as it is an easy way to decrease identifiability at this point. Delete or remove the attribute (s), or if the structure of the dataset needs to be maintained, clear the data and probably the header. Note that the suppression should be actual delete permanent, and not just hiding the column. similarity, may not be adequate if the underlying data remains somewhat accessible. Some Tips for this method It is the strongest type of Anonymization technique, because there is no way of recovering any information from such an attribute. In certain scenarios, it may be possible to create a derived attribute that provides utility and it is less sensitive than the original attribute(s) which can be suppressed [4].

Example: In this example, the data set consists of test scores. As the recipient only needs to analysis test scores obtained by students with respect to their various trainers but without analysis on the students themselves, the "student" attribute was removed.

Table 1. Before anonymization:

Student	Trainer	Test Score
John	Tina	87
Yong	Tina	56
Ming	Tina	92
Poh	Huang	83
Linnie	Huang	45
Jake	Huang	67

Table 2. After suppressing the "student" attribute:

Trainer	Test Score
Tina	87
Tina	56
Tina	92
Huang	83
Huang	45
Huang	67

Record Suppression: Record Suppression refers to the delete of an entire record in a dataset. In contrast to most other techniques, this technique affects multiple attributes at the same time. We use it to remove outlier records which are unique or do not meet other criteria such as k-anonymity, and not to keep in the anonymized dataset. Outliers can lead to easy re-identification. It can be applied in deferent stage before or after other techniques. How record suppression is used, we delete the entire record. Note that the suppression should be permanent, and not a hide row function; similarly, redacting may not be sufficient if the underlying data remains accessible. Note that delete of a record impacts your dataset [4].

Character Masking: Is the change of the characters of a data value by using a constant symbol like (*) or (x). Masking is typically partial, and its applied only to some characters in the attribute. We use this type of technique in data value when it is a string of characters and we hiding a part of it is sufficient to provide the extent of anonymity required. It's used depending on the nature of attribute, replace the appropriate characters with any chosen symbol. Depending on the attribute type, you may decide to replace a fixed number of characters such as credit card numbers, or a variable number of characters like what we can found in email

address. There are some tips Related to this method, that masking may need to take into account whether the length of the original data provides information about the original data. Subject matter knowledge is critical especially for partial masking to ensure the right characters are masked. Special consideration also applies to checksums within the data; occasionally the checksum could be used to recover the rest of parts of the masked data. with regard to Complete masking, the attribute could alternatively be suppressed the length of the data is of some relevance. The scenario of masking data in such a way that data subjects are meant to recognize their own data is a special one, and does not belong to the usual objectives of data anonymization.

Instance of this is the publishing of lucky draw results, where by typically the names and partially masked NRIC numbers of lucky draw winners are published for the individuals to recognize themselves as winners. Note that in general, anonymized data should not be recognizable even to the data subject themselves [4].

Example: the example shows an online grocery store conducting a study of its delivery demand from historical data, in order to improve operational efficiency. The company masked out the last four digits of the postal codes, leaving the first two digits, which correspond to the sector code within Singapore.

Table 3. Before anonymization:

Postal Code	Favourite Delivery Time Slot	Average No. of Orders Per Month
100111	8 pm to 9 pm	2
200222	11 am to 12 noon	8
300333	2 pm to 3pm	1

Table 4. After partial masking of postal code:

Postal Code	Favourite Delivery Time Slot	Average No. of Orders Per Month
10xxxx	8 pm to 9 pm	2
20xxxx	11 am to 12 noon	8
30xxxx	2 pm to 3pm	1

Pseudonymisation: The surrogate of identifying data consists of values. That's also referred to as coding. Pseudonyms can be irreversible, the original values are actually disposed and the pseudonymisation was done in a non-repeatable, Reverse by the owner of the original data, where the original values are securely protected but can be retrieved and linked back to the pseudonym, when its need.

Persistent pseudonyms allow linking by using the same pseudonym values to represent the same individual across different datasets. otherwise, different pseudonyms used to represent the same individual in different datasets to prevent linking of the different datasets. This can be randomly deterministically created. pseudonyms sometimes provide better utility by maintaining referential integrity across datasets. It is use when data values need to be unique, special and where no character tacit information of the original attribute shall be kept. We use it by replace the respective attribute values with created values. To apply this, we must to pre-generate a list of created values then select random values from this list to replace each of the original values with the created one. There is no connection between the original values and new values, they must be unique. Some tips you have to concern about When allocate pseudonyms, make ensure that not to re-use them a gene, especially when they are randomly generated. As well avoid using the exact same pseudonym generator over several attributes, without any change.

The identity database cannot be shared with the recipient; because it should be secure, save and only used by the organization to resolve any specific queries although, the number of such queries must be controlled, otherwise they can be used to decode the entire pseudonymisation. Like, when you encrypt data you will used encryption key that cannot be shared with any one, it is must be secure and protected from unauthorized access. Security of any key used must be ensured like with any type of encryption. In some cases, special pseudonym generators may be needed to create synthetic datasets, and we considered when creates pseudonyms must have the same format as the original data [4].

Example: shows pseudonymisation being applied to the names of persons who obtained their driving licenses, and some information about them. The names were replaced with pseudonyms instead of the attribute being suppressed, because the organization wanted to be able to reverse the pseudonymisation if it's necessary.

Table 5. Before anonymization:

Person	Pre Assessment Result	Hours of Lessons Taken Before Passing
Joe Phang	A	20
Zack Lim	B	26
Eu Cheng San	C	30
Linnie Mok	D	29
Jeslyn Tan	B	32
Chan Siew Lee	A	25

Table 6. After pseudonymising the Person attribute:

Person	Pre Assessment Result	Hours of Lessons Taken Before Passing
416765	A	20
562396	B	26
964825	C	30
873892	D	29
239976	B	32
943145	A	25

When reversible pseudonymisation, the identity database is save in case there is a future legitimate need to identify individuals. Security controls must be used to protect the identity database.

Table 7. Identity database (single coding):

Pseudonym	Person
416765	Joe Phang
562396	Zack Lim
964825	Eu Cheng San
873892	Linnie Mok
239976	Jeslyn Tan
943145	Chan Siew Lee

To add secure concerning the identity database, you have to code the data twice. Continuing the previous example, this example shows the additional connecting database, which is placed with an authenticate third party. According to this process, the identity of the individuals can only be known when Both parties trusted the third party then the database will connect together. Connecting database securely by only authenticated third party. Note that in both connecting database and identity database, instead of keeping dataset in same order it is better to practice scrambled data.

Table 8. After anonymization:

Person	Pre Assessment Result	Hours of Lessons Taken Before Passing
373666	A	20
594824	B	26
839933	C	30
280074	D	29
746791	B	32
785282	A	25

Table 9. After secure with authenticated third party.

Pseudonym	Interim Pseudonym
373666	OQCPBL
594824	ALGKTY
839933	CGFFNF
280074	BZMHCP
746791	RTJYGR
785282	RCNVJD

Table 10. Identity database after secure it by the organization.

Interim pseudonym	Person
OQCPBL	Joe Phang
ALGKTY	Zack Lim
CGFFNF	Eu Cheng San
BZMHCP	Linnie Mok
RTJYGR	Jeslyn Tan
RCNVJD	Chan Siew Lee

3. EMERGENCE OF A NEW CIVIC OS

Now a day, the Internet of Things (IoT) has been receiving its fair share of attention as the world turns more and more digital. There is no doubt that there is a huge amount of information on the Internet and it is affects many aspects of our lives. This is undoubtedly very useful in the economic sphere. According to the growth of economic sphere this cause a huge change in policymakers, enterprises and citizens are driving to create and steer a truly digital economy. This changes depending on geography, culture, economics and politics in deferent countries. Let's take India as an example of that, it is already has more than 100 smart city initiatives planned not just between humans but also between machine-to-machine (M2M), and machines to humans. The Internet of Things presents an opportunity to transform society and establish a new ecosystem built to serve not merely humans, but humanity. In this new world, people will become more unique by having a new personality as they want. The Organization for Economic Co-operation and Development (OECD) compares IoT's importance and potential ubiquity to the advent of household electricity and study the extending technology and commerce to redefine our social life, cultural and relationships. We have to understand the new live with IoT. To create idle environment, we have to concern about impact of IoT in our life and spread higher awareness of the technologies to be able to enjoy using technology in All aspects of our lives and how it can shape our daily lives. the idea of Civic OS is the ability of humans and machines to coexist and to cohabit and communicate seamlessly.

The Civic OS represents a fundamental change in norms and mores in society this change in the way we conduct both our businesses and our relationships, as well as our daily lives. This new civic society will be full of data that optimized by machines collaborating together for the benefit of citizens. This change will contain public and commercial services that can be delivered directly to individuals in specific range of connected devices [5].

3.1 THE CIVIC OPERATING SYSTEM

There are 7.6 billion people on Earth about 3.7 billion are connected to the Internet. India is one of the key countries poised for large-scale implementation of IoT projects - not only to be able to set new roles but also as a key geography to anticipate the emergence of a humanism embracing people and devices. This emergence of a new societal operating system reflects technology impact and evolving concept of citizenship that's mean change in citizen's access way to services. This is the fundamental basis of Civic OS. IoT will role the society, because of control both humans and machines.

This change causes a new collection of protocols and behaviors to be able to apply technology functions. The new operating system, controlled by IoT will enable economies to grow more in security, productively and efficiently. Diagram below shows technology and infrastructure in global economies [5,6].

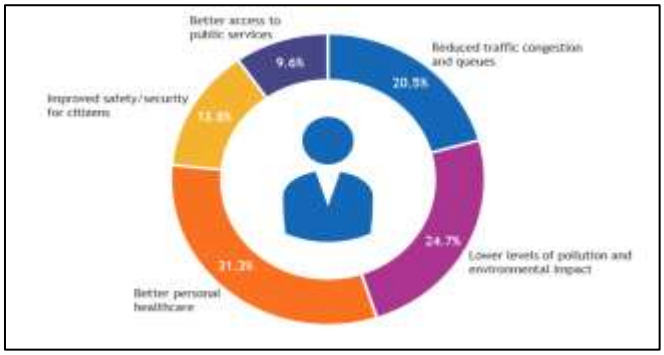

Figure. 3. Consumer Expectations from IoT

3.2 CONNECTED DEVICES

One of research Show that (34.6%) of Indians support IoT firstly with smartphones. Small ratio Represent public services (14.5%), smart homes (14.1%) and smart cities (11.4%). (14.2%) Represent the ratio of using all devices and appliances with IoT [5].

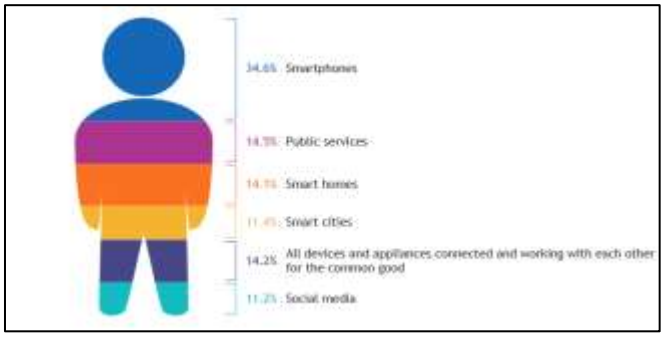

Figure 4. Consumer Insight | IoT by association

India has growth in wearable technology, with IoT utilized in the fitness, healthcare and lifestyle. As shown, smartphone has the largest impact. India IoT market growth with a CAGR of 28.2% in 2016 to2022. 60% of India's think that it is being imperative to driving a competitive advantage and about 50% of companies heads believe that IoT is imperative to remaining digital fit. IoT need to advance through educate society to create idle ecosystem in the future. India have the biggest economy. The real case of IoT in India become better beyond the smartphone otherwise, population don't understand that. Only 14.5% of public services take advantage from the technology [5].

3.3 IoT IN HOMES

Most of the respondents believe that they forget to buy important things like yogurt almost once a month. About 75% of the respondents attract to buy any type of technology which meant that they would never have to worry about running out of groceries again.

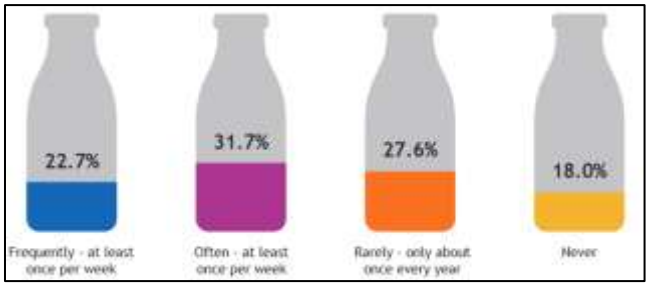

Figure 5. Consumer Insight | Essential Supplies

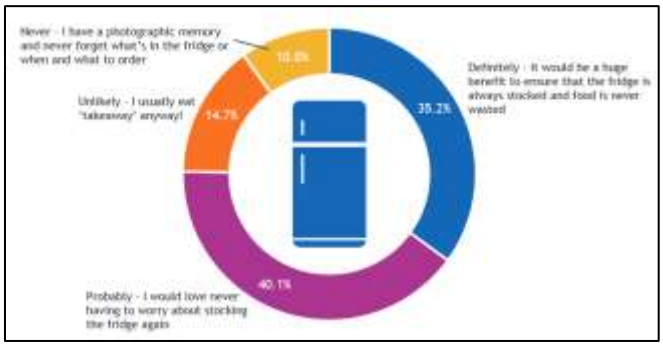

Figure. 6. Consumer Insight | Acceptance of new technology

Note that 35.2% of the respondents cited that manage food as one of the key takeaways from such a purchase. Almost 9 out of 10 Indians are open to experimenting with a gadget that helps them monitor their home appliances in real-time [5].

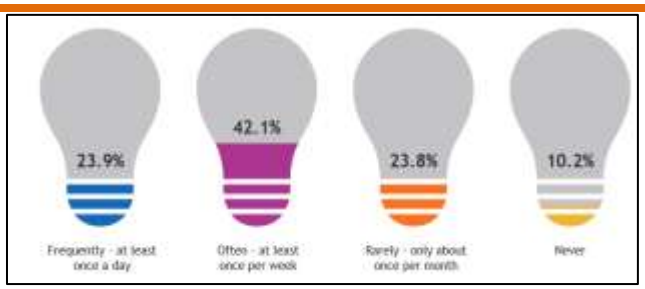

Figure. 7. Accepting FOLO (Fear of Lights On)

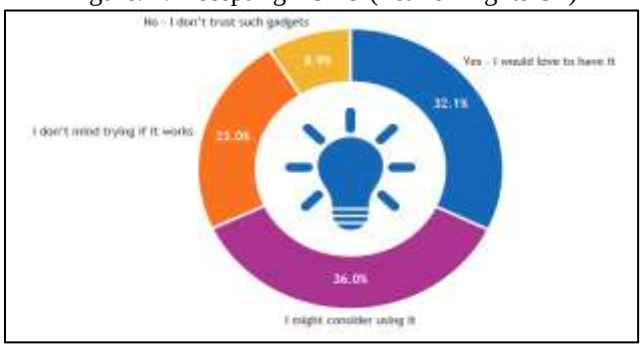

Figure**. 8.** Acceptance of technology in managing FOLO

4. Conclusions and Remarks

Internet of things is a new technology which let many applications and devices to be connected to the internet and between each other. Each objects in the world can be identified, connected to each other through internet controlled independently. There is some challenge that Faces the interconnected world of the IoT because of that IoT needs a new role, policy and regulation to control the relationship between world and the internet of things. Our life changes by the IoT many smart applications will appear. In addition, this new technology will enable us to reach and contact with every things This means that all aspects of life will be easier than in the past. IoT is a new approach of technology which describes the connection of different kind of applications and devices that let them communicate with each other by sending and receiving multiple type of data also allow humans to communicate with smart machines. This communication takes short time to stratify specific order according to their appetites with massive advantages. But anything new needs laws and controls to be used in a useful and harmless way so they create a policy and regulations Especially for internet of things (IoT). And if we Commitment with this policies and regulations This will lead us to enjoy using the Internet in good way.

REFERENCES

[1] 4th IEEE World Forum on Internet of Things (WF-IoT 2018), http://wfiot2018.iot.ieee.org/files/2017/04/IEEE-WF-IoT-2018-CFPs-Final-2.pdf.
[2] With the Internet of Things (IoT) everywhere ,can regulation be far behind?, http://www.adlittle.com/sites/default/files/viewpoints/adl_iot.pdf
[3] Peter Tolmie , Andy Crabtree : The practical politics of sharing personal data. Artical (2017).
[4] GUIDE TO BASIC DATA ANONYMISATION TECHNIQUES, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf.
[5] EMERGENCE OF A NEW CIVIC OS, http://www.communicationstoday.co.in/images/reports/20180222-IoT-Report-Final.pdf.
[6] World ometers , http://www.worldometers.info/world-population/