Privacy, legal and regulatory issues in the management of the internet of things for South Africa

Nomusa Dlodlo[1], Samuel Malinganiso Skosana[2], Zinzile Abigail Dlodlo[3]

CSIR-Meraka Institute[1, 2], University of Pretoria[3]
{ndlodlo[1], smskosana[2]}@csir.co.za, u29368911@tuks.co.za[3]

Abstract

The internet of things (IoT) is a concept which has its roots in sensing, networking and information processing approaches. It enables data exchange between devices, services and people. As a result of the integration of these technologies, big data is generated. Where there is big data involved, there arises challenges in privacy, legal and regulatory issues in the management and security of information within the sphere of IoT. There is no formal legislation yet in South Africa that is linked to IoT. However, there is a framework of pieces of legislation which govern information management and security within which the IoT should operate, for example, The Electronic Communications and Transactions Act and The Electronic Communications Act.

This research paper reports on such legislation, by extracting aspects that would apply to IoT, leading to the formulation of privacy, legal and regulatory issues of IoT for South Africa. Since IoT is an integration of big data, telecommunications, services and people, the identified aspects are those that relate to the information society, that is, the frequency spectrum, regulation of telecommunications, telecommunications policies, universal access, and interception of communications, rights of access to information, ethical issues and consumer protection.

The research came up with the following analyses: (i) that the information collected using IoT technologies should ensure that the privacy of the individual is observed. (ii) that government entities should be regulated within the sphere of IoT while undertaking their responsibilities, (iii) that the constitutional right of the individual to have access to data obtained and processed by the state, organisations and other individuals including the data that has been obtained or processed by the same via IoT is observed, (iv) that the IoT policies should also revolve around the regulation of the market and ethical issues of universal access, development of human resources in the sector and roping in small and medium enterprises (SMMEs) to provide services in the sector, (v) that legislation can be adapted to enable and facilitate electronic communications in the IoT by removing barriers through standardization of communications, combating cybercrime, protection of information through cryptography and monitoring information systems..

Keywords

internet of things; legal issues; regulatory issues; privacy issues

ISBN: 978-1-920508-46-3

• Introduction

The internet of things (IoT) is a vision of a connected world in which people and physical and digital devices are connected and exchange data between themselves, as well as gather information from the environment and make appropriate decisions. The internet of things consists of five components, namely, (1) sensors to collect and transmit data, (2) actuators to trigger a device for a particular function, (3) computing node to process information collected by sensors, (4) receivers to receive messages from other devices or computing node and (5) communicators to pass messages from one component to another (Horrow, 2012). The IoT is built upon the ubiquitous connectivity of smart objects. Smart objects sense the environment around them and communicate with each other over the internet. With the massive deployment of sensors, actuators and everyday objects enhanced with communication and computing capabilities the IoT is closing the gap between the cyber and physical world by weaving technology into everyday life thus giving rise to privacy, legal, security and regulatory issues non-existent before. Weber (2010) argues that the ubiquity of the IoT requires new regulatory approaches to ensure privacy and security.

Rudolf van der Berg from the Expert Group on IoT of the European Commission concludes the following: (i) IoT locks spectrum use in the long run, (ii) There is room for standardisation in IoT, (iii) IoT is about information, (iv) Terms of data sharing in IoT should be defined, (v) Existing laws and regulations on IoT may be sufficient but it needs to be known that they exist and are adequate, (vi) Additional governance schemes of the IoT are required and (vii) The large majority of IoT applications will have a global dimension. This definition identifies the management of the frequency spectrum, regulation of the IoT industry, information management, governance, standardization of IoT, legal aspects of IoT and IoT policy as the requirements to be put in place.

The International Telecommunications Union's (2005) analysis of privacy in ubiquitous network societies emphasizes that three domains must be addressed in tandem when seeking privacy solutions: the sociological, technical and regulatory. Public education about what is desired and acceptable is a key part of the sociological solution. From a technological side, the development of privacy-enhancing technologies is emphasized. It is clear that the present standard of industry self-regulation is not sufficient to constrain the threat to privacy.

There is no formal legislation yet in South Africa that governs the IoT. However there are pieces of legislation in South Africa which govern information management and security within which IoT should operate. These are (i) The Constitution of the Republic of South Africa (Constitution of the Republic of South Africa, 1996), (ii) The Promotion of Access to Information Act No. 2 of 2000 (The Promotion of Access to Information Act, 2000), (iii) The National Credit Act (The National Credit Act, 2005), (iv) The Electronic Communications and Transactions Act No. 25 of 2002 (The Electronic Communications and Transactions Act, 2002), (v) The Regulation of Interception of Communication and (vi) Provision of Communication-related Information Act No. 70 of 2002 (RICA) (Regulation of Interception of Communications Act, 2002), (vii) The Protection of Personal Information Bill (Protection of Personal Information Bill, 2009), (viii) The Telecommunications Policy (White paper on Telecommunications Policy, 2014) (ix) The Independent Communications Authority of South Africa Act 2000 (Independent Communications Authority Act, 2000), (x) The Independent Broadcasting Authority Act 153 of 1993 Independent Broadcasting Authority Act, 1993), (xi) The Broadcasting Act 4 of 1999 (Broadcasting Act, 1999), (xii) The Electronic Communications Act 2005 (Electronic Communications Act, 2005) and (xii) The Sentech Act (Sentech Act, 1996). The Protection of Access to State Information Bill (Protection of Access to State Information Bill, 2010) has been submitted to the President of South Africa for enactment. The legislation spans the area of information security and privacy, telecommunications policies and regulations and legal issues. This document shall therefore report on privacy, legal and regulatory issues in the management of IoT for South Africa. It identifies a number of South African legislation that should be applied to IoT in South Africa.

• Problem Statement

Current legislature only provides protection for the broad definition of the internet but specifically does not cover for the IoT. Therefore this research asks the following questions

a. What are the relevant aspects of IoT that need to be investigated from privacy, legal and regulatory points of view?

b. Which current legislation is addressing these aspects and are they doing this in an adequate manner?

c. Is the current legislation sufficient, does it need enhancement or is new legislation needed?

ISBN: 978-1-920508-46-3

The research conducted a desktop study on South African legislation. Some of the information was collected from experts on regulatory issues. All this information was analysed to identify the link with IoT

• Data Privacy in IOT

The emergence of the IoT has created big data. The legal questions of big data include in particular the ownership of data, the limits of such data, the legality of their processing and the contracts needed between the suppliers and clients. A great deal of personal information, related to both one's health and identity might be inferred from one's aggregate data, for example, erroneous personal data from distributed databases could be linked to an individual. Data mining is prone to inaccuracies. Surveillance in public places highlights the blurring boundary between public and private space. Usually, individuals do not benefit from access to such information, highlighting an imbalance in power that emerges from the act of surveillance. Mining of data, invasive target advertising, loss of autonomy through marketing profiles tip the balance between consumer benefit and corporate gain. Protecting the privacy of individuals is also difficult in the internet age. The internet makes it possible to store and transfer large amounts of data at little cost and at the same time, vast amounts of personal information are searchable, linkable and traceable.

In the IoT domain, the collection of data and profiling are can be interpreted as an intrusion of privacy. The intention of data collection might be positive, as it enables governments and companies to provide services and better target citizens. However an excessive use of these technologies leads to practices for commercial or other purposes. Like other technologies that collect personal data, the focus should be on ensuring only data related to achieving the stated business objectives is collected. Moreover data collectors should make certain collected data is protected with the same rigorous privacy standards applied to personal data collected from other sources.

Information may be owned or free. It belongs to someone if it is protected by intellectual property. It may also be given in the form of a free licence. Therefore with the IoT we cannot dispense these old theories of ownership. Most countries have adopted regulations on the internet that limit liability of internet actors such as infrastructures, ISPs or hosting providers. These limited liabilities cannot work with IoT since the actors will have to account for technical performance of the IoT.

The 1980 OECD fair information principles (FIPPS) on privacy address the following (Massit-Follea, 2009)

- Consumers should be given notice of an entity's information practices before any personal information is collected from them
- Consumer choice means giving consumers choice to decide on how any personal information about them is used
- An individual must be able to access data about him/herself
- Data must be accurate and secure
- Principles of privacy protection can only be effective if there is a mechanism to enforce them
- The European principles of "proportionality and transparency' should be applied to IoT. "Proportionality" requires a balanced analysis of assessing risk and mitigating risk based upon threat to privacy. "Transparency" ensures IoT is not used to secretly collect data.
- In order to achieve transparency, individuals should receive reasonable and appropriate notification of the type of data collected and how the data will be shared and used.

The IoT generates a range of data such as health parameters, location data, lifestyle, etc. Pachube proposed an 'Internet of Things Bill of Right", i.e. a set of rights that it hopes to become an industry standard. It is intended to give people access to and control over their data created and gathered via IoT devices. In South Africa on the other hand the information security and privacy legislation include The Protection of Personal Information Bill (POPI), Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA), Promotion of Access to Information Act (PAIA) and the National Credit Act (NCA).

ISBN: 978-1-920508-46-3

3.1. Protection of Personal Information Bill

The Protection of Personal Information Bill (Protection of Personal Information Bill, 2009) aims to give effect to the right to privacy, by introducing measures to ensure that the personal information of an individual (data subject) is safeguarded when it is processed by responsible parties. It is about the protection of information processed by both public and private bodies with a view to privacy of information in the collection, retention, dissemination and use. Personal information must be processed lawfully in a manner that does not infringe on the privacy of the data subject. The information must be collected directly from the data subject unless the data subject has given consent for the information to be collected from other sources. The subject should be aware of the purpose of collection. The records must not be retained longer than necessary for achieving the purpose. A responsible party must ensure the integrity of the information in their possession. The data subject may request the responsible party to delete or correct the information. A person's personal information can only be processed by medical professionals, insurance companies, schools and child protection services for child/learner support, and employers on behalf of pension funds. Information cannot be transferred to foreign bodies unless the recipient is subject to a law or the subject consents to the transfer. This means that information collected via IoT technologies should ensure privacy of the individual.

3.2. RICA

Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) (Regulation of Interception of Communications Act, 2002) does not regulate the telecommunications infrastructure in the manner of the Telecommunications Act. Rather, it sets out the circumstances under which government entities or other persons may or must intercept or monitor communications. No person may intercept a communication in the course of its transmission unless they are authorised to execute interception. Any person may intercept a communication if they are party to the communication, or if one of the parties to the communication has given consent. Any person may in the course of carrying on any business, intercept any indirect communication. Any law enforcement officer may intercept communication to prevent serious bodily harm. Communication can be intercepted for the purposes of determining location in case of an emergency. Any person who is lawfully engaged in duties relating to the monitoring of signal for the purposes of installation or maintenance of equipment, facilities or devices may monitor the related signal for purposes of these duties. An employee may monitor signals and radio frequency spectrum for purposes of managing the radio frequency spectrum. No telecommunication service provider or employee may provide communication-related information to any person other than the customer of the telecommunication service provider, except when authorised by the customer. This legislation simply means that government entities should be regulated. This means that the government entities should be regulated as well within the sphere of IoT while undertaking their responsibilities to ensure safety and security.

3.3. Promotion of Access to Information Act 2000

The Constitution provides that everyone has the right to access any information held by the state. The Promotion of Access to Information Act 2000 (PAIA) (The Promotion of Access to Information Act, 2000) gives effect to the constitutional right of access to any information held by the state and any information that is held by another person and that is required for the exercise or protection of any rights. A requester must be given access to a record of a public body if that requests complies with all the procedural requirements in this Act relating to a request for access to that record and access to that record is not refused in terms of any ground for refusal contemplated. This Act does not apply to a record of the cabinet and its committees, the judicial functions of a court, special tribunal or a judicial officer.

The grounds for refusal of access to records are:

- Protection of privacy of a third party who is a natural person
- Protection of records or certain records of the South African Revenue Service
- Protection of commercial information of a third party such as trade secrets of a third party, financial, commercial, scientific or technical information of a third party, or information provided in confidence by a third party
- Protection of confidential information of a third party

ISBN: 978-1-920508-46-3

- Protection of safety of individuals and protection of property
- Commercial information of private body
- Protection of research information of third party and research information of private body
- Protection of police dockets in bail proceedings and protection of law enforcement and legal proceedings
- Protection of information whose disclosure will prejudice the defence and security of the republic
- Economic interests and financial welfare of the republic
- Protection of information on the operations of public bodies, disclosure of which is likely to frustrate processes in the public body or policy formulation processes

This means that the constitutional right of the individual to have access to data obtained via IoT should be observed as long as access to the data does not infringe on the rights and privacy of others and does not prejudice safety and security of the state.

3.4. National Credit Act

The National Credit Act (NCA) (national Credit Act, 2005) is designed to protect consumers in the credit market and make credit and banking services more accessible. With relation to information this Act is meant to achieve the following:

- To improve the standards of consumer information
- To prohibit unfair credit and credit marketing practices
- To regulate credit information.

The NCA does all this by simplifying and standardising credit agreements and information disclosure, regulating credit bureaux in terms of consumer information and records. On the issue of confidentiality, personal information and credit records, this Act advocates for the following:

- Right to confidential treatment
- National register of credit agreements
- Credit bureau information
- Removal of record of debt adjustment or judgement
- Right to access and challenge credit records
- Verification, review and removal of consumer credit information

The Act requires all credit bureaus to be registered and ensure data is accurate at all costs and that inaccurate information is immediately removed without cost to the customer. The NCA regulations stipulate how credit bureau information is obtained, used and for how long it should remain on a consumer's profile. Consumers are eligible for one free credit report

ISBN: 978-1-920508-46-3

from each credit bureau each year in order to effectively manage their credit profiles. These same regulations should apply to data obtained and processed via IoT technologies.

3.5. Protection of Access to State Information Bill

Although the bill has not been enacted yet, it states that for security reasons classified information should not get out to the public. There have been arguments that public rights of access to information will be violated. There have also been arguments that it will promote corruption since individuals will conceal information under this bill. The Constitution of the Republic of South Africa states that everyone has the right of access to any information held by the State, and any information that is held by another person for the protection and exercise of any rights. Freedom of expression is also enshrined in the constitution. However, according to this bill classified information cannot be expressed in public. The IoT is affected in that people's access to information will be curtailed.

• Regulatory and Legal issues of IOT

The internet of things is defined as: "... a network that enables to identify digital entities and physical objects, directly and without ambiguity, via standardised and unified electronic identification systems and wireless mobile devices, and thus makes it possible to retrieve, store, transfer and process data relating to them, without discontinuity between the physical and virtual worlds" Mossit-Follea, 2009).

The advantage of the above definition is to contain most of the keywords symbolising the legal issues surrounding IoT (Barby, 2012):

- "network of networks" implies topics such as ownership and standards
- 'identification system" implies topics such as traceability and monitoring
- "physical objects" implies topics such as quality and related matters
- "data' implies topics such as quality and ownership
- "processing of data" implies topics such as relevance and liability

The European commission has passed legislation that IoT devices are expected to be in the radio-frequency group (i.e. 100kHz) and operate with very low power, unlikely to produce significant levels of exposure to electromagnetic frequencies (EMF).

The principles underlying the internet of things require that each object is uniquely identified and identifiable inside the network. Currently there are three types of identifiers: a machine identifier (e.g. MAC address), a product identifier (e.g. bar code) and a digital identifier (e.g. IP address). With IoT identity is a key issue. There are two options; changeover from IPv4 to IPv6 or to come up with a new solution. The issue with the second option is the ownership of the future new addressing system and who will run the new system.

The main reasons advanced for regulation of telecommunications are:

- To maintain control over the use of valuable natural resource, namely the radio frequency spectrum
- To control anti-competitive behaviour by dominant players in the market, this in turn will lead to the realisation of universal access and to increases in quality and choice
- To ensure the development and implementation of effective universal services policies

ISBN: 978-1-920508-46-3

Due to the ease of which data is collected, shared, analysed and stored leads to a proliferation of databases. Individual access to remedy incorrect data is a challenge. Computer, network infrastructure or process failures can lead to a paralysis of the overall automated IoT vision. To make this failure even more severe is the excessive reliance on technological infrastructure that is characteristic of this envisaged environment. Failure of smart devices, loss of functionality due to IT infrastructure, cyber-attacks, devices' weak access control will lead to overall systems failure. With the systems integrated the failure will have a far-ranging impact.

From an international perspective, as shown in the first part of this section, issues of universal access policies, control and regulation of the market, legislation of the radio frequency spectrum, data quality and ownership, regulation and monitoring of infrastructure, security of the infrastructure and standardization are identified. In South Africa, the legislations that would cover these identified issues include The Independent Communications Authority of South Africa (ICASA) Act, The Telecommunications Act, The Telecommunications Policy, The Electronic Communications and Transactions Act, The Electronic Communications Act and the Sentech Act.

4.1. ICASA Act

The Independent Communications Authority of South Africa (ICASA) (Independent Communications Authority of South Africa, 2000) is an independent regulatory body of the South African government, established in 2000 by the ICASA Act to regulate both the telecommunications and broadcasting sectors in the public interest. Traditionally, telecommunications and broadcasting services operated separately and so has the regulation of the sectors. Broadcasting in South Africa was regulated by the Independent Broadcasting Authority (IBA), whereas telecommunications was regulated by the South African Telecommunications Regulatory Authority (SATRA). Rapid technological developments have led to the convergence of broadcasting and telecommunications services. This also had an influence on the convergence of regulation resulting in the merging of the IBA and SATRA. ICASA functions under the Department of Communications (DoC).

ICASA is empowered by the Telecommunications Act to make regulations on telecommunications service licences, fees for these licences, the way in which telecommunication service licencees keep accounts and records. ICASA also prepares a frequency band plan. Telecommunication systems all require a certain amount of electromagnetic bandwidth to operate. In different parts of the world, different organizations allot parts of the overall electromagnetic spectrum to different uses. In many parts of the world, international agreements are required so that communications systems in neighbouring countries are not interfering with each other. So, the spectrum, that is, the full frequency range, is allotted to various purposes: analog TV broadcasts get a certain slot (from 54 to 88 MHz, 174 to 216 MHz and 470 to 806 MHz), FM radio gets a certain slot (88 to 108 MHz), AM radio gets a certain slot (535 to 1700 kHz), cellular communications (mobile phones) get certain slots There are lots of these as little gaps in the spectrum have been given over to cell phone use. As the world becomes increasingly wireless (with cordless phones, cell phones, wireless internet, GPS devices, etc), allocation of the available spectrum to each technology becomes increasingly contentious. Each user community (usually manufacturers of the wireless equipment) wants more bandwidth in order to be able to sell and service more units. For any given slot of bandwidth, there is a limited amount of data that can be shared in that bandwidth, so vendors want more bandwidth so they can handle more devices in a given area.

Under ICASA socio-economic regulations, the licencing conditions for different sectors and areas differ. So do the licence fees. For example licences for disadvantaged dividend areas, that is, those areas without the penetration of digital communications, are subsidised.

Spectrum is a scarce commodity. Telkom and the military have monopoly over the South African spectrum. Not all spectrum is utilised and hence there is a lot of spectrum which can be allocated to other operators to render new services. Licencing of operations does not automatically mean that an entity qualifies for spectrum. The role of ICASA is to allocate frequencies to these spectrums. Wi-Fi, microwave, GSM all comes in different frequencies.

Under ICASA ethical issues, each ICASA area determines frequencies that work without interference from other areas. For example, amplification of signals results in signal amplitude increasing and interfering with other frequencies. Therefore it is necessary to put more base stations within a given radius in order to cover more areas as hand over occurs. For interoperability between systems technologies, interfaces should be standardised, e.g., user radio to send to fibre-optic or a physical network, free and open source framework for open standard applications.

Under ICASA regulatory issues, security of a network can be built into any layer of the ISO Reference Model. If it is built into the application layer, it can easily be hacked into. At the physical layer security uses IP addresses. Security at this

ISBN: 978-1-920508-46-3

layer can be enhanced through physical-edged addresses that cannot be broken into. The physical layer 1 and the network layer 2 provide more security in a network.

The architecture of the technology affects regulatory issues. In a GSM network you have a base switch, a base station controller and the base station itself. At the base station controller level is attenuation. The switch gets a number, puts you to a route, e.g. 00 for international calls, and then puts you to the next switch, etc. The architecture is built around logic. Broadband cannot be transmitted through a switch though. Attenuation is caused by resistance to the signal strength. For broadband networks the cells are smaller, hence there are no attenuation loops. The LTE base station operates a broad pie and a radius of 500 metres to 1 kilometre, so you can get signal strength. The regulations on fibre, wireless will be different.

Frequencies can be categorised into ultra-low, medium, low, high and very high frequency. LTE and TV spaces have a low frequency of between 700 and 900MHz. Low frequencies can penetrate walls. High frequency cannot go through walls. High frequency resonates with the wall and creates interference. The capacity for propagation or transmission of signals is determined by the material used. Therefore to understand the properties of these frequencies one needs to understand these materials. Low frequency materials are in high demand. Laser is high frequency hence it resonates.

2.4 GHz and 5 GHz are bands which are not regulated. 2.4 GHz is used for testing technology more than to put up a service. Systems are then migrated to regulated frequencies. Direct point-to-point optical technologies are not regulated. They are good in short distance communications and high capacity carriers. Intra-township can use these point-to-point optical technologies while out-of-township can use microwave or fibre-optic technologies. Fibre is light and hence there is no interference. On the other hand microwave has interference and a line of sight is required to avoid a reduction in strength.

4.2. Telecommunications Act

The Telecommunications Act (Telecommunications Act, 1996) does 3 things: (1) it sets out fundamental rules for the telecommunications industry, e.g. that one may not provide a telecommunications service without a licence, that no one may transmit a signal by radio or receive a signal by radio without a licence, (2) it initially established the telecommunications regulator called SATRA which was later merged into ICASA through the ICASA Act, (3) ICASA must establish other rules for the telecommunications industry.

The Telecommunications Act covers for radio regulations and telecommunication regulations including mobile cellular communications. Radio dealers are expected to keep records of all radio apparatus sold, hired, supplied and the apparatus should be tuned to the right frequency that the licencee is allowed to use. Sections 95 and 96 of the Telecommunications Act empower the regulator, ICASA, to make regulations which must be approved and published by the Minister of Communications. The Telecommunications Act also empowers ICASA to issues licences and makes orders in relation to disputes.

This Act regulates telecommunications infrastructure, and regulates the market and controls unfair practices. The same should be adapted to IoT.

4.3. Telecommunications Policy

The Telecommunications Policy (Weber, 2010) deals with the universal service, market structure and independent regulator. The White paper on Telecommunications Policy set out that there should be an initial period of exclusivity for Telkom. The Telecommunications Policy should accommodate new services and technologies, e.g., international call-back services and internet telephony services. At the beginning of the exclusivity period additional market segments would be open up for competition, that is, local loops, public payphones and national long distance and metropolitan area networks. The policy provided for a second national operator to compete with Telkom and the amendment of the Sentech Act to provide international communication gateway services and multimedia services. SMMEs would be licenced to provide services in under-serviced areas. The policy required the Minister of Communications to develop an ICT strategy to be reviewed every 2 years and a national e-strategy to be reviewed every year. The national strategy is to deal with universal access, development of human resources and facilitating use of electronic communications by SMMEs. One of S.A.'s international obligations is in terms of GATS. GATS provides that any signatory country should treat service providers from other countries as favourably as it treats service providers from its country.

ISBN: 978-1-920508-46-3

The policy is on the regulation of the market and ethical issues of universal access, development of human resources in the telecommunications sector and roping in SMMEs to provide services in the sector. These policies can also be adopted in South Africa's IoT sector.

4.4. Electronic Communications and Transactions Act 2002

The objective of Electronic Communications and Transactions Act (Electronic Communications and Transaction Act, 2002) is to enable and facilitate electronic communications and transactions in the public interest. It does not regulate telecommunication infrastructure in the manner of the Telecommunications Act. Rather, it removes the legal uncertainties regarding electronic communications and transactions and facilitates the use of telecommunications. It serves the following:

- Development of a national e-strategy
- Remove barriers to electronic communications
- Encourage the use of e-government services
- Observe international standards
- Encourage investment in the telecommunications sector
- Promote SMMEs to transact electronically
- Promote HR development in skills relevant to the telecommunications sector
- Ensure efficient use and management of the .za domain
- Keeping a directory of cryptography providers
- Protection of personal information collected via telecommunications
- Protection of critical databases
- Appointment of cyber inspectors to monitor information systems
- Combat cyber crime

The Electronic Communications and Transactions Act can be adapted to enable and facilitate electronic communications in the IoT by removing barriers through standardization of communications, involving SMMEs in the industry, combating cybercrime, protection of information through cryptography and monitoring information systems.

4.5. Electronic Communications Act

The objectives of the Electronic Communications (EC) Act (Electronic Communications Act, 2005) are:

- To promote convergence in the broadcasting, broadcasting signal distribution and telecommunications sectors and to provide a legal framework for convergence of these sectors
- To make new provision for the regulation of electronic communications services, electronic communications network services and broadcasting services
- To provide for the granting of new licences and new social obligations

ISBN: 978-1-920508-46-3

- To provide for the control of the radio frequency spectrum
- To provide for the continued existence of the Universal Service Agency and the Universal Service Fund

This Act can be adapted in IoT for the regulation of electronic communication services, control of the radio frequency spectrum and universal access.

4.6. SENTECH Act

The main objective and business of Sentech (SENTECH Act, 1996) is to provide as a common carrier, broadcasting signal distribution for broadcasting licensees in accordance with the provisions of the Independent Broadcasting Authority Act. The state is the only shareholder of the company. This Act can be adapted for a common OpenIoT platform, that is, standardization

• Conclusion

This document presents a framework within which IoT should operate in South Africa. This framework consists of S.A. legislations that relate to data privacy, legal and regulatory issues. Legal IoT issues from an international perspective are also reviewed at the end of the document.

This document reports on such legislation, by extracting aspects of these legislations that would apply to IoT. These aspects lead to the formulation of privacy, legal and regulatory issues of IoT for South Africa. Since IoT is an integration of big data, telecommunications, services and people, the identified aspects are those relate to the frequency spectrum, regulation of telecommunications, telecommunications policies, universal access, and interception of communications, rights of access to information, ethical issues and consumer protection. The information collected using IoT technologies should ensure that the privacy of the individual is observed. Government entities should be regulated within the sphere of IoT while undertaking their responsibilities. As has traditionally been the constitutional right of the individual to have access to data obtained and processed by the state, organisations and other individuals , so does the data that has been obtained or processed by the same via IoT be made available to protect the rights of the individuals. Even for data collected via IoT technologies the national Credit Act regulations stipulate how credit information is obtained, used and for how long it should remain on the consumer's profile. The IoT policies should also revolve around the regulation of the market and ethical issues of universal access, development of human resources in the sector and roping in SMMEs to provide services in the sector. The Electronic Communications and Transactions Act can be adapted to enable and facilitate electronic communications in the IoT by removing barriers through standardization of communications, involving SMMEs in the industry, combating cybercrime, protection of information through cryptography and monitoring information systems. The Sentech Act can be adapted for a common OpenIoT platform, that is, standardization.

• References

Anzelmo, E., Bassi, A., Caprio, D., Dodson, S., van Kranenburg, R., Ratto, M., (2011), Discussion paper on the Internet of Things, commissioned by the institute for Internet and Society, Berlin

Barbry, E., (2012), The internet of things, legal aspects: what will change everything, Digiworld Economic Journal, No. 87, pp. 83-100

Broadcasting Act 4 of 1999, http://www.info.gov.za/view/DownloadFileAction?id=70607

Constitution of the Republic of South Africa, http://www.gov.za/documents/constitution/1996/a108-96.pdf

Electronic Communications Act 2005, http://www.info.gov.za/view/DownloadFileAction?id=67890

Electronic Communications and Transaction Act 2002, http://www.info.gov.za/view/DownloadFileAction?id=68060

Horrow, S., Sardana, A., (2012), Identity management frameowrk for cloud-based internet of things, SecurIT 2012, August 17-19 2012, pp. 200-203, India

Independent Broadcasting Authority Act 153 of 1993, http://www.info.gov.za/acts/1993/a153-93.pdf

Independent Broadcasting Act of 1999, http://www.info.gov.za/view/DownloadFileAction?id=70607

ISBN: 978-1-920508-46-3

Independent Communications Authority of South Africa Act 2000, http://www.info.gov.za/view/DownloadFileAction?id=101146

Massit-Follea, F., (2009) L'internet des objets. Quels enjeux pour l'Europe?. Ed. Mauson des sciences de l'Homme. Paris.

National Credit Act, http://www.acts.co.za/national-credit-act-2005/

OECD guidelines on the protection of privacy and transborder flows of personal data: background, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OECD Policy Brief, (2008), The Future of the Internet Economy

Promotion of Access to Information Act 2000, http://www.info.gov.za/view/DownloadFileAction?id=68186

Protection of Personal Information Bill, http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionofPersonalInformation.pdf

Regulation of Interception of Communications and Provision of Communications-related information act, 2002, http://www.info.gov.za/gazette/acts/2002/a70-02.pdf

Sentech Act 1996, http://us-cdn.creamermedia.co.za/assets/articles/attachments/03007_sentechact63.pdf

Telecommunications Act 1996, http://www.info.gov.za/acts/1996/a103-96.pdf

Thornton, L., Telecommunications law – an overview, http://thornton.co.za/resources/Telecoms%20Law%20an%20Overview.pdf

Weber, R.H, (2010), Internet of Things – New Security and privacy challenges, Computer Law and security Review, No. 26, pp. 23-30

White paper on Telecommunications Policy, http://www.polity.org.za/polity/govdocs/white_papers/telewp.htmlJ. Clerk.

The protection of Stae Information Bill, http://www.parliament.gov.za/content/b%206b%20-%202010%20(protection%20of%20state%20information)~1.pdf

ISBN: 978-1-920508-46-3