The Legal risks in IoTs processing of Personal Information: A South African Perspective

A research report presented

By

Anola Naidoo

Student Number: 331188

Word count: 14 679 words (excluding table of contents and bibliography but including footnotes)

DECLARATION

I **ANOLA NAIDOO** do hereby declare that this research report is my own unaided work. It is re-submitted in fulfilment of the requirements of the degree of Master of Commercial Law (LLM) in the Faculty of Commerce, Law and Management at the University of the Witwatersrand, Johannesburg.

Signed at Johannesburg on 16 September 2019

Johannesburg, September 2019

Contents

ACKNOWLEDGMENTS

First, I would like to thank my husband, Wesley, for his patience, encouragement and resilient support for over a decade. I draw strength from you in order to overcome life's obstacles and achieve my goals. To my precious daughter Omelia, who embodies the love and light shared between two soulmates, may you always know that you are loved beyond measure and that your happiness is the reason for every decision mum and dad make. To my parents, I dedicate this research report to you for all the sacrifices that you have made and continue to make, I would not be where I am today if it were not for having people like you to call mum and dad.

I would like to further take this opportunity to thank my supervisors, Ms. Verine Estebeth and Dr. Emile Zitzke, for their invaluable guidance and assistance herein.

ABSTRACT

The technological and competitive landscape has undergone a significant change over the past decade, leading to cheaper processes, improved networking capabilities, smart devices, appliances, vehicles, security systems, machine learning and artificial intelligence that have exponentially enhanced the manner in which humans interact globally. While the Internet of Things has facilitated the Fourth Industrial Revolution, the push for universal access to the internet and the intelligent collaborations between various objects anywhere and at any time, requires the Internet of Things more often than not, to demand an extensive amount of an individual's personal information be processed in order to perform its daily functions. This processing and increased complexity of these devices creates new safety, security, privacy, and usability challenges far beyond the difficult challenges' individuals face just securing a single device. Furthermore, without the ability of manufacturers, internet service providers and/or government being able to guarantee an acceptable security level to protect the personal information being processed, this report aims to ascertain the legal risks to data privacy and security when these Internet of Things process a person's personal information, the importance of one's Constitutional right to privacy together with attempting to highlight possible ways industry and individuals can mitigate these risks[1].

KEYWORDS

Internet of Things; personal information; data protection; data privacy and security.

[1] Nicola Fabiano 'Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation' (2017) 3 *Athens Journal of Law* 201-214*;* Weber, R.H 'Internet of Things – New Security and privacy challenges' (2010) 26 *Computer Law & Security Review* 23-30

I INTRODUCTION

The technological and competitive landscape has undergone a significant change over the past decade, with the digital era being one of the main reasons thereof.[2] The constant change has led companies to become so focused on bettering their own technology to keep up with competitors in order to meet ever-changing and increasingly demanding consumers' needs. In the process of doing so, some companies rush the process of change to the extent that they fail to prepare for the inherent risks and consequences of operating in the digital age.[3] One of these risks, as a result of the internet and in relation to the Internet of Things ('IoTs') is the risk to the right to privacy. Personal information, a sphere of privacy refers to more than a person's race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation or age.

In the digital age, the internet, volume, complexity, magnitude, capabilities of technological devices and geographic reach of information has resulted in personal information to go further to include *inter alia* a person's geolocation, financial information, buying habits, preferences, opinions and search history.[4]

The changing and expanding scale in which this personal information is processed is at an unprecedented speed and one's ability to understand and contend with the implications has resulted in consideration of the question, 'what are the legal risks in IoTs processing personal information?' In other words, if a company decides to use IoTs to process personal information of their customers, what are the potential liability issues that could arise? Accordingly, the aim of this research report is to identify the legal risks in processing personal information and the steps that can be taken to mitigate these risks, if any. I unpack this main research question in the following way: In Part II, I discuss 'what are the IoTs and other technological advancements in the digital age?' Then in Part III, I discuss privacy and the South African Constitution in relation to the IoTs together with certain foreign legislation relating to the right to privacy.

---

[2] Cavusgil, S.T., Knight, G and Riesenberger, T.R *International Business: The New Realities* (2012)
[3] Fu K., Kohno T., Lopresti D., Mynatt E., Nahrstedt K., Patel S., Richardson D., & Zorn B 'Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things' (2017), available at *http://cra.org/ccc/resources/ccc-led-whitepapers/*, accessed on 28 December 2018
[4] Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S 'Privacy and The Internet of Things, Lexis Nexis: Watching Me, Watching You: Surveillance, Privacy and The Media (2016) 21 *Media and Arts Law Review* 336-351; Waldo, James, Lin Herber and Millett Lynette *Engaging Privacy and Information Technology in a Digital Age* (2007)

Then in Part IV, I discuss the threats that the IoTs pose to data privacy. Then in Part V, I unpack the data protection laws in South Africa relevant to the IoTs. In Part VII, I provide recommendations to cater for the identified threats that the IoTs pose to data privacy and finally in Part VII, I provide a conclusion of the way forward for data privacy.

II THE INTERNET OF THINGS AND OTHER TECHNOLOGICAL ADVANCEMENTS INTEGRATED INTO THESE INTERNET OF THINGS

One must first ascertain what technological advancements exist and which of these pose the greatest risks to data privacy and security. The most significant technological trend in this era has to be the technological capabilities of IoTs[5] which encompasses aspects of artificial intelligence, Big Data and Cloud Computing in order to make life more manageable and effortless.[6] I now turn to explain these concepts for the sake of terminological clarity.

(a) The Internet of Things

Casagras[7] defines IoTs as a global infrastructure (hardware, software and services) linking physical and virtual objects through the exploitation of data capture and communication capabilities.[8] In layman's terms, this means that IoTs are everyday things, objects and devices connected to the internet and, in turn, to each other, by the sending and receiving of data.[9] These embedded computing devices are interconnected uniquely to the internet to form an IoT domain supporting the networking and communication of these objects that are active participants in processing personal information,[10] which means that real-time data is collected, transmitted, processed and stored between each device's unique identification.[11]

---

[5] Sophia Moganedi and Jabu Mtsweni 'Beyond the Convenience of the Internet of Things: Security and Privacy Concerns' 2017 *Council for Scientific and Industrial Research;* Weber, R.H op cit note 1 at 2
[6] Carsten Maple 'Security and privacy in the internet of things' (2017) 2 *Journal of Cyber Policy* 155-184; Cavoukian, A., & Jonas, J 'Privacy by Design in the Age of Big Data' 2012 *Information and Privacy Commissioner of Ontario, Canada*
[7] Coordination and Support Action for Global RFID-Related Activities and Standardization
[8] European Commission 'IoT Privacy, Data Protection, Information Security', available at *http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753, a*ccessed on 10 March 2018
[9] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3
[10] Sophia Moganedi and Jabu Mtsweni op cit note 5 at 4
[11] Leila Benaissa 'Legal challenges of the Internet of Things' (2015) Lexology, available at *http://www.lexology.com/library/detail.aspx?g=b5b1aba8-fefd-4fc5-8837-12647312377a,* accessed on

This real time transmission by IoTs includes communication between persons, person/s and machine and machine to machine communication.[12]

Currently, there are an estimated 25 billion things connected to the internet and many are of the view that by 2020, this number will increase to 50 billion, meaning that an average human will have an average of six IoTs at any given moment.[13] This increase in use, interconnectivity and ease in processing personal information thereof highlight the increasing risks to privacy as the number of IoTs grow.

(b) The Internet of Everything

ICT Insight conducted a survey amongst businesses and found that 63% believe IoTs are a business strategy, whilst 27% regarded it as a set of applications.[14] The rest were unsure as they admit that their knowledge of same is limited.[15] With the majority accepting the importance of IoTs, IoTs are left to continue to collect mass amounts of data without addressing the risks that this poses to the protection of data privacy and security.[16] The ability to convert this data to valuable data refers to the technology behind IoTs, being the 'Internet of Everything' ('IoE').[17] The four key features of IoEs are people, things, data and process. 'People' refers to the connection between persons as a result of IoTs. 'Things' refers to the network created by IoTs track and monitor the status or output of various devices. 'Data' refers to the raw data that is processed to make intelligent decisions. 'Process' refers to the information that is analysed and delivered to the right person at the right time in order to make sound decisions.[18]

---

21 July 2017; and Richard Kemp 'Legal Aspects of the Internet of Things' (2017) Kemp IT Law, available at *http://www.kempitlaw.com/wp-content/uploads/2017/06/Legal-Aspects-of-the-Internet-of-Things-KITL-20170610.pdf*, accessed on 21 July 2017

[12] Muhammad Iqbal, Oladiran Olaleye & Magdy Bayoumi 'Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches' (2016) 16 *Global Journal of Computer Science and Technology: E Network, Web & Security*

[13] Dave Evans, 'The Internet of Things How the Next Evolution of the Internet is Changing Everything' (2011) Cisco Internet Business Solutions Group (IBSG), available at *https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf*, accessed on 21 December 2018

[14] Suzanne Franco 'IoT Survey' (2018) *ICTInsight*, available at *http://books.itweb.co.za/ICTInsight/ICTInsight38_2018.pdf*, accessed on 1 February 2018

[15] Ibid.

[16] Ibid.

[17] Nebula 'The Internet of Things Vs the Internet of Everything – Why you need both' (2016), available at *https://www.nebula.co.za/2016/11/24/internet-things-vs-internet-everything-need/*, accessed on 10 March 2018

[18] Ahmed Banafa 'The Internet of Everything (IoE)' (2016) OpenMind, available at *https://www.bbvaopenmind.com/en/the-internet-of-everything-ioe/*, accessed on 10 March 2018

Unlike IoTs which has one feature (things) the IoE's four features allow for these interconnected devices to learn individual preferences and predict future actions through analysis of the data captured.[19] Accordingly, the term IoTs will be used throughout this research report and shall include IoEs unless specifically stated otherwise.

(c) Big Data and Cloud Computing

Cloud Computing is an online network of servers hosted on the internet to store, manage, and process data, rather than using a local server or a personal computer.[20] Cloud Computing has assisted with the rise in IoTs and IoTs has given rise to terms such as Big Data.[21] Big Data is not just the collection and storage of massive amounts of data, but rather, according to Ernst Janovsky head of Absa Agribusiness, 'Big data is about finding links between seemingly unrelated data, [thus,] [t]he key to big data is truly in the analysis – understanding how one aspect of the data affects another and unlocking new insights through identifying these links.'[22] The 'Big' in Big Data relates to (i) volume, being the vast amounts of data generated, (ii) velocity, referring to the exponential rate at which new data is generate and the speed it moves around, (iii) variety, being the different types of data that can be used and (iv) veracity which refers to the messiness or trustworthiness of the data itself.[23] Businesses take the data captured and processed by IoTs to translate the mass amounts of data into Big Data and make strategic business decisions about the market industry and consumers.[24]

[19] Nebula op cit note 17 at 5
[20] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3
[21] Carsten Maple op cit note 6 at 4; Richard Kemp op cit 11 at 5
[22] Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3
[23] Bernard Marr *Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results* (2016)
[24] Cukier. K & Mayer-Schonberger.V 'The rise of Big Data: How it's changing the way we think about the world' (2013) 92 *Foreign Affairs* 28-40

(d) Artificial Intelligence and Machine Learning

The rate of Big Data being processed has resulted in a need for better and efficient analytics tools that are able to adapt rapidly and evolve.[25] Artificial Intelligence ('AI') has been incorporated into IoTs and is 'concerned with the use of computers in tasks that are normally considered to require knowledge, perception, reasoning, learning, understanding and similar cognitive abilities.'[26]

Machine Learning ('ML') refers to the AI's capability to learn, improve and evolve its performance over a period of time.[27] ML tools are given unfettered access to the Big Data and it is predicted that network nodes, chips, sensors and software programs of the future will be operated by AIs.[28]

All of the above technological advancements have eased the way humans interact and do business. However, industry and individuals are not considering the potential infringement to privacy that the lack of data protection, security measures and sustainability of IoTs pose. Companies develop technology at a rapid rate that their own innovations have been the cause of their own demise (eg. Blackberry Messenger). Information, especially personal information of the company (and its employees), its consumers and its service providers are freely used, distributed, stored and modified in today's digital age. Confidentiality, accuracy and integrity of information together with aspects such as whether a person still has the right to privacy, have become questionable,[29] and consideration into whether any laws have been created to cater for any potential infringement of privacy rights will be discussed in the next two parts.

[25] Fluidity Software Solutions, 'IoT and Big Data' (2017). Available at http://www.fluidity.solutions/IoT-and-Big-Data.html. Accessed on 10 March 2018
[26] Tomáš Saloky and Jaroslav Šeminský 'Artificial Intelligence and Machine Learning'. Department of Automation and Control, faculty of Mechanical Engineering, Technical University of Košice, Slovak Republic, available at *http://conf.uni-obuda.hu/SAMI2005/SALOKY.pdf*, accessed on 10 March 2018
[27] Ibid.
[28] Steve Hanson 'How Big Data is Empowering AI and Machine Learning' (2017), available at *https://hackernoon.com/how-big-data-is-empowering-ai-and-machine-learning-4e93a1004c8f*, accessed on 10 March 2018
[29] Raul Rubio and Jaime Santisteban 'Cybersecurity, A new priority for Top Management' (2017), available at *http://www.lexology.com/library/detail.aspx?g=ffc8732c-d13d-410d-866a-6fbf540a75e9*, accessed on 21 July 2017

III PRIVACY AND THE CONSTITUTION

Now that the technological advancements that pose the greatest risks to data privacy and protection have been identified, one must determine the legal rights that could be infringed by IoTs and the recourse available should such right be infringed. The strongest right in data protection that could be infringed is the right to privacy.

(a) What is the right to privacy?

Section 14 of the South African Constitution states that everyone has the right to privacy, which shall include the right not to have their person, home or property searched, their possessions seized or the privacy of their communications infringed.[30]

As evident by the *O'Keeffe v Argus Printing and Publishing Co Ltd*,[31] the right to privacy – which has existed at common law for years – is divided into two parts, first, a general right of privacy and the second protects against specific infringements of privacy such as search and seizures together with infringements of privacy communications.[32] Within a technological context, this means that each user has the right not to have their IoT seized, communication using such IoTs intercepted, collected, monitored or shared without the user's knowledge and consent.[33]

It also extends to a person's legitimate expectation of privacy in this regard the court must deliberate who the user is and the role said user plays within the public and private spheres.[34] In *Bernstein v Bester*[35] the courts determined from the facts over which a person is entitled to have a subjective expectation of privacy and that society has recognised that expectation as objectively reasonable.[36]

---

[30] Johan De Waal, lain Currie and Gerhard Erasmus *The Bill of Rights Handbook* (4th Edition) (2001)
[31] O'Keeffe v Argus Printing and Publishing Co Ltd 1954 (3) 244 (C)
[32] Johan De Waal, lain Currie and Gerhard Erasmus op cit note 30 at 8
[33] Jonathan Burchell 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009) 3 *Electronic Journal of Comparative Law*; Lee Bygrave 'Privacy and Data Protection in an International Perspective' (2010) 56 *Scandinavian Studies in Law* 165
[34] Antoon De Baets 'A historian's view on the right to be forgotten (2016) 30 *International Review of Law, Computers & Technology* 57-66
[35] Bernstein v Bester No 1996 (2) SA 751 (CC)
[36] Neethling, J; M Potgieter, J M and Visser P J *Neethling's Law of Personality* (2005); Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; in re Hyundai Motor Distributors (Pty) Ltd v Smit NO 2001 (1) SA 545 (CC)

There are four forms of privacy to which IoTs are applicable to all. These forms include bodily privacy, including pictures; privacy communications such as emails, skype and WhatsApp calls; territorial privacy such as geolocation tags and cookies; and information/ data privacy including financial and medical information.[37]

With regards to IoTs and the constitutional right to privacy,[38] the GPEN Global Privacy Enforcement Network in 2016 found that two thirds of devices failed to explain in a plain and simple language to users how their/ its personal information will be collected, used, stored and transmitted. Furthermore, three quarters gave little to no evidence to show that the personal information could be deleted. Further, one third could not adequately provide contact details to users should they/ it intend to contact the IoT manufacturer or supplier.

(b) Limitation of Rights

As the right to privacy is not an absolute right,[39] the ability of the courts to limit the aforesaid right amounts to a consideration of section 36 of the Bill of Rights, being the law of general application.[40] The court will first consider whether, a right has been infringed by law or by way of conduct. Second, whether the infringement can be justified in terms of section 36. Only after the first investigation has been considered and answered in the positive, may the court look to justifying the infringement as a reasonable limitation.[41]

In *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers Association,*[42] it was held that 'a court will place the purpose, effects and importance of the infringing legislation on one side of the scales and the nature and effect of the infringement cause by the legislation on the other. The more substantial the invasion into fundamental rights, the more persuasive the grounds of justification must be.'

[37] Roos A, D. van der Merwe (eds) *Data privacy law, in Information Communications Technology Law* (2016); Van der Merwe, D *Information & Communication Technology Law* (2008)
[38] Section 14 of the Constitution of the Republic of South Africa
[39] Antoon De Baets op cit note 34 at 8
[40] Ibid.
[41] Section 36 of the Constitution of the Republic of South Africa
[42] Ketler Investments CC t/a Ketler Presentations v Internet Service Providers Association 2014 (2) SA 569 (GSJ)

All relevant factors including the nature of the right, the importance of the purpose of the limitation, the nature and extent of the limitation, the relation between the limitation and its purpose and any less restrictive means to achieve the purpose must be taken into account.[43]

Ultimately, it all boils down to a balance of rights and interests of different users on a case by case basis. On the one hand, IoTs can benefit and assist a person with everyday life tasks and on the other hand, personal information could be used for a secondary purpose unbeknown to the user.[44] Historically, the protection and limitation of privacy was effected through the common law *actio iniuriarum*. Since the Constitution has come into effect, the Constitutional Court has made it clear that the *actio iniuriarum* can be regarded as a common-law remedy that indirectly gives effect to the constitutional right to privacy.[45] However, in the last decade, various foreign jurisdictions have passed data privacy laws in an attempt to regulate this niche field of privacy. These foreign jurisdictions are discussed directly below on account of the facts that (a) foreign law may be considered in the process of interpreting the bill of rights[46] and (b) foreign law has influenced the pending introduction of the POPI Act in South Africa.

(c) Foreign Legislation

Unfortunately, the Constitution and common law principles do not cater completely for instances where a person is unaware that their personal information is being processed by a third party or that a person may correct the accuracy of their personal information.[47]

While the focus of this research report is South Africa, it must be noted that the legislatures considered, the privacy and data protection laws amongst other foreign legislation in multiple countries. Some of the top countries include the United Kingdom, United States of America, New Zealand, Canada and the European Union which regulates 28 member states across Europe.

[43] Antoon De Baets op cit note 34 at 8
[44] S v Makwanyane 1995 (3) SA 391 (CC)
[45] NM and Others V Smith and Others (Freedom of Expression Institute as Amicus Curiae) 2007 (5) SA 250 (CC); Neethling, J; M Potgieter, J M and Visser P J op cit note 36 at 8
[46] Section 39(1) Constitution of the Republic of South Africa
[47] Roos, A 'Data Protection: explaining the international backdrop and evaluating the current South African position' 2007 *SALJ* 402

Across the European Union, GDPR[48] on 25 May 2018 became directly applicable law in all 28 member states of the European Union without requiring member states to codify same into national law. The application of the GDPR depends on whether an organisation is established in the European Union. The interpretation of establishment is so wide that GDPR has extra-territorial effect in that an organisation that it is not registered within the European Union will still be subject to the GDPR if an IoT processes personal data of data subjects who are residing in the European Union where the processing activities are related to the offering of goods or services[49] to data subjects within the European Union or the monitoring of their behaviour[50] as far as their behaviour takes place within the European Union.

As the fines and penalties are quite extensive, many IoT manufacturers and processors must be able to answer certain questions prior to processing, including where the user is aware of the data being captured, the duration the data will be kept for, who can access the data, how the data will be destroyed and how to request the data to be removed.[51]

In Canada, the Personal Information Protection and Electronic Documents Act applies to consumer and employee personal information practices of organisations that are deemed to be a federal work, undertaking or business (eg banks, telecommunications companies, airlines, railways, and other interprovincial undertakings).[52]

The United Kingdom has prepared a new national data protection law, ahead of BREXIT, the Data Protection Act 2018 ('DPA'), which also, like GDPR comes into force on 25 May 2018. This allows for the continued application of the GDPR in UK national law once the UK leaves the European Union, it codifies the Law Enforcement Directive ((EU) 2016/680) into UK law, creating an updated data protection regime, setting out the scope of the Information Commissioner's mandate and enforcement powers and creates a number of criminal offences relating to processing personal data.[53]

---

[48] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union (2016), pp. 1-88 Key: citeulike:14071352

[49] Article 3(2)(a) of Ibid 48

[50] Article 3(2)(b) of Ibid 48

[51] Regulation (EU) 2016/679 op cit note 48 at 11; fines and penalties can amount to ten million Euros or up to 4% of an organisations global turnover, whichever is the greater

[52] Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)

[53] Data Protection Act 2018

In the United States of America, the US Federal Trade Commission ('FTC') is empowered to exercise jurisdiction over a wide range of commercial entities in order to prevent and protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices.[54]

Finally, in New Zealand the Privacy Act[55] governs how agencies collect, use, disclose, store, retain and give access to personal information. It gives the Privacy Commissioner the power to issue codes of practice that modify the operation of the legislation in relation to specific industries, agencies, activities or types of personal information.[56]

The above overview considers the application of right to privacy and the extent to which it can be applied in a person's life. However, as noted, there are varying literature on the extent the right of privacy in relation to personal information and due consideration must be given to the type of personal information processed by IoTs and thereafter, what processing could potential infringe on a person's right to privacy.

IV THE ROLE OF THE PROTECTION OF PERSONAL INFORMATION ACT

While the right to privacy is protected by the Constitution and common law, it is debateable whether information/ data privacy is covered in South Africa, in its entirety by this right. Accordingly, the South African Law Reform Commission, provided general guidelines for data protection and infringement when developing legislation. These guidelines, when applied to IoTs, include questioning whether: the information: was obtained in an intrusive manner; relates to intimate aspects of the subject's personal life; was collected for one purpose but further processed for another; was disseminated

[54] Federal Trade Commission Act 15 U.S.C. §§ 41-58, as amended. The FTC, among other things, issues regulations to enforce certain privacy laws and take enforcement actions and investigate companies for failing to implement reasonable data security measures, making materially inaccurate privacy and security representations in privacy policies, failing to abide by applicable industry self-regulatory principles, transferring or attempting to transfer personal information to an acquiring entity in a bankruptcy or merger and acquisition transaction, in a manner not expressly disclosed on the applicable consumer privacy policy, violating consumer privacy rights by collecting, using, sharing or failing to adequately protect consumer information, in violation of the FTC's consumer privacy framework or certain national privacy laws and regulations.

[55] The Privacy Act 28 of 1993

[56] Also note that a Privacy Amendment Act 12 of 2017 was introduced to New Zealand's parliament in 2018. If enacted it will give the Privacy Commissioner a higher level of authority and power, create mandatory reporting of breaches in privacy, new offenses and increased fines

to the public and the subject could reasonably expect such information to remain confidential.[57]

The Protection of Personal Information Act 4 of 2013 ('POPIA') has attempted to clarify the extent of this Constitutional right by making provision for the manner in which personal information of a data subject is to be protected and processed, and the consequences for non-compliance with those requirements.[58]

So, what is personal information? POPIA[59] provides a very broad definition of personal information and further defines the term processing to include *inter alia* the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use, dissemination, merging, erasure or destruction of information.[60] The legislatures observed European and North American law when drafting POPIA. However, POPIA defines personal information more broadly than that of a prominent piece of legislation, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[61] ('GDPR') which refers to personal data as any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier[62]. This means that in South Africa, unlike GDPR, protection would fall to both natural and juristic persons.[63]

As IoTs process a huge amount of personal information, both passively[64] and actively,[65] the aim of this section is to examine the type of personal information IoTs process. IoTs at the core of its functioning requires the processing of personal information in order to render the services/ provide the goods.[66] First, IoTs require the identity of its users as the

[57] South African Law Reform Commission (2005) Discussion Paper 109 (Project 124) Privacy and Data Protection.
[58] Preamble to the Protection of Personal Information Act 4 of 2013
[59] Section 1 Protection of Personal Information Act 4 of 2013
[60]Roos A, D. van der Merwe (eds) op cit note 37 at 9; Van der Merwe, D op cite note 37 at 9
[61] Regulation (EU) 2016/679 op cit note 48 at 11
[62] Ibid.
[63] Roos A, D. van der Merwe (eds) op cit note 37 at 9; Roos, A Data Protection in Van der Merwe, D; Roos, A; Pistorius, T; and Eiselen, S *Information & Communication Technology Law* (2008)
[64] A 'passive digital footprint' is a data trail you unintentionally leave online as defined by TechTerms, available at *https://techterms.com/definition/digital_footprint*, accessed on 10 March 2018
[65] An 'active digital footprint' includes data that you intentionally submit online as defined by TechTerms, available at *https://techterms.com/definition/digital_footprint*, accessed on 10 March 2018
[66] Leloglu E 'A Review of Security Concerns in Internet of Things' (2017) 5 *Journal of Computer and Communications* 121-136

personal information can only be transmitted only when the IoT is linked to a user thus it is imperative that the user explicitly consents and that the user is not automatically linked to the object. Once the user is identified, profiling of the user through tracking buyer habits, likes, dislikes and most visited locations occurs in order to determine what the data subject requires when and where.

Finally, with globalisation, IoTs have the capability to transmit personal information across borders within seconds and store the personal information on a multitude of servers that may not have the required high-security measures.[67] While many see this as a way to ease their busy life schedules, the risk of relying too much on IoTs could strongly infringe a user's right to privacy by failing to adequately cater for data protection.[68]

Now that we have determined what personal information relates to a person's right to privacy and, in basic terms, what types of personal information are processed by IoTs, consideration must be given to the risks IoTs could pose to the right to privacy by processing personal information.

V HOW IOTS PROCESS YOUR PERSONAL INFORMATION RISKS YOUR RIGHT TO PRIVACY

(a) IoTs, IoEs, Big Data, AI and ML

IoTs process personal information through numerous applications including *inter alia* cookies, spiders and geotagging. Cookies are programs that permit the company to retain your personal information, spiders crawl the worldwide web in order to find the specific results a data subject has entered. Companies having access to this information can track a data subject's buying behaviour, credit card details, preferred time of shopping, geolocation and target market a data subject in order to increase the chances of a purchase.[69]

[67] Cassim F 'Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study' (2009) 12 Potchefstroom Electronic Journal 36-79
[68] Nicola Fabiano op cit note 1 at 2
[69] Tech Law Blog 'The Internet of Things: Legal challenges in an ultra-connected World' (2016) Mason, Hayes & Curran, available at *https://www.mhc.ie/latest/blog/the-internet-of-things-legal-challenges-in-an-ultra-connected-world*, accessed on 21 July 2017; and Sophia Moganedi and Jabu Mtsweni op cit note 5 at 4

This has led to numerous risks to a person's right to privacy, especially in cases where a company does not have the adequate security. Unauthorised access to information could result in a data subject suffering financial or physical harm as criminals are able to determine the data subject's location at a specific time in the day or transact using a data subject's financial information. Besides criminal activities, inadequate protection of databases could result in spiders 'crawling' into the company's financial information, trade secrets, databases of suppliers and consumers, which could result in a breach of confidentiality and cause reputational and financial harm to the company.[70]

One of the greatest risks to privacy is that safety and security measures to the hardware and software are sometimes seen as an add on with many IoTs, especially to the simple, everyday IoT like mobile apps, resulting in manufacturers not adequately catering for safety and security measures at the development or coding phase of the IoT.[71] With many person's connecting personal IoTs to work IoTs, security attacks could affect intellectual property, financial security, competitive advantage, operational stability, compliance and reputation to both a natural and juristic persons detriment.[72]

Employers must authorise the use of private IoTs and ensure that the device has the same or better security features imposed on the business's IoTs. An agreement between the parties would be required to ensure that the employee understands the intended restrictions imposed on the employee's privacy.[73]

A weak or no security in one device could compromise the best security system in another IoT due to the interconnectivity of these devices.[74] Should cyber criminals be able to access an IoT using a person's personal information or hack the device, as a result of a weak network security and gain access to a person's personal information, the cybercriminal could sell the personal information to third parties,[75] access the person's funding and/or withhold access to a person's personal information via ransomware.[76]

---

[70] Ibid.; Reinhardt Buys & Francis Cronjé *Cyberlaw@SA II: The Internet and the Law in South Africa* (2004); Reinhardt Buys *Cyberlaw@SA: The Internet and the Law in South Africa* (2000

[71] Cassim F op cit note 67 at 14; Federal Trade Commission, v. D-Link Corporation and D-Link Systems, Inc., corporations, 3:17-CV-00039-JD

[72] Marié Mcgregor 'The Right To Privacy In The Workplace: General Case Law And Guidelines For Using The Internet And E-Mail' 2004 *SAMLJ* 16

[73] Pistorius, T 'Monitoring, Interception and Big Boss In The Workplace: Is The Devil In The Details?' (2009) 12 *Potchefstroom Electronic Law Journal*

[74] Muhammad Iqbal, Oladiran Olaleye & Magdy Bayoumi op cit note 12 at 5

[75] Papadopoulos, S 'Are we about to cure the scourge of spam? A commentary on current and proposed South African legislative intervention' 2012 *THRHR* 75

[76] Cassim F op cit note 67 at 14

Another risk to privacy in a person's intimate space is where IoTs with camera functionality are unlawfully accessed and images/ videos are shared or sold, without the person's consent.[77]

Adequate safety and security require consideration into aspects such as confidentiality, integrity, authenticity and availability.[78] The personal information being transmitted must be transmitted by legitimate entities and remain confidential until it is received by the correct IoT and should only open once the intended person accesses the transmission through secure authentication.[79] Furthermore, any personal information that was erroneously sent or contains inaccuracies should be able to be revoked, deleted or sealed prior to being open by the incorrect person. IoTs transmitting person information amongst one another should only transmit personal information amongst trusted devices that the person has authenticated and authorised and this authorisation should not be for an indefinite period.[80] This will assist in reducing the risk of criminals impersonating an individual and limits the risk to breaches in security.[81]

IoTs that are too complex or have a software problem without the ability of being rectified or detected could lead to incorrect communication from one device to another which could result in a system failure or error in performance by the IoT[82] i.e. incorrect medication dispensed after an incorrect reading of a patient's vitals. It is important that there is no general authorisation in the transferability of personal information and that privileges are limited to processing only that personal information which is required to fulfil a specific function.[83]

Different regulations in different countries may cause security risks and an abuse of personal information, especially in instances where data protection laws are inadequate when compared to South Africa.[84]

---

[77] Anthony Woolley And Deborah Woolley Against Nahid Akbar Or Akram [2017] Scotsc 7 (03 February 2017)
[78] Cassim F op cit note 67 at 14
[79] Muhammad Iqbal, Oladiran Olaleye & Magdy Bayoumi op cit note 12 at 5
[80] Cassim F 'Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players' (2011) 15 *Comparative and International Law Journal of Southern Africa* 123–138
[81] Reinhardt Buys & Francis Cronjé op cit note 70 at 15; Reinhardt Buys op cit note 70 at 15
[82] Al-Ko Kober Ltd & Anor v Sambhi [2018] EWHC 165 (QB) (02 February 2018)
[83] Leloglu E op cit note 66 at 13
[84] Cassim F op cit note 80 at 16

Therefore, an IoT created in a country with less data protection laws could permit the process of personal information without requiring a person's consent or allowing a system to update and rectify errors.[85] Accordingly, stopping or deleting the circulation of incorrect personal information may be too difficult especially if unauthorised IoTs accessed a person's network and further process the personal information without consent.[86]

Real time data collection such as geolocation or geotagging and tracking of a person's behavioural habits could infringe on a person's privacy by third parties using the personal information to conduct criminal activities such as home burglaries or human trafficking.[87]

(b) Cloud Computing

A further risk to a person's personal information can be found in companies' application of Cloud Computing or the cloud.[88] It operates outside the confines of the traditional territorial boundaries, thereby increasing its complexity.[89] Cloud Computing refers to a network of computer servers located locally or across the globe.[90]

The increase in connectivity means that personal information moves around the world relatively quickly and freely. Unsecure connections such as employees home networks, hotels, airports and coffee shops result in personal information, unbeknown to the user, being transmitted to the cloud unsecured, unlike a corporate network which would encrypt and secure the personal information prior to transmission.[91] Unsecure access to the network via a IoT could lead to processing of personal information captured on the network without the user consenting or having knowledge thereof.

---

[85] Cassim F op cit note 67 at 14
[86] Carsten Maple op cit note 6 at 4
[87] Campbell F 'An analysis of the emerging role of social media in human trafficking: Examples from labour and human organ trading' (2016) 15 *International Journal of Development Issues* 98-112; George Beall 'How Hackers are using social media to hack' (2017), available at *https://thenextweb.com/contributors/2017/08/23/hackers-using-social-media-hack/*, accessed on 25 March 2018
[88] Rajkumar Buyya, James Broberg and Andrzej Goscinki *Cloud Computing Principles and Paradigms* (2010)
[89] Hauman M 'A South African Perspective on User-Created Content in Cloud Computing: A Copyright Conundrum'. (2014). University of Free State Dissertation; Reinhardt Buys & Francis Cronjé op cit note 70 at 15
[90] Rajkumar Buyya, James Broberg and Andrzej Goscinki op cit note 88 at 17
[91] Kim Re 'Randsomed, Hacked and Attacked? – You'll 'Wannacry' (2017) Without Prejudice; Reinhardt Buys & Francis Cronjé 'op cit note 70 at 15

(d) Malware and Ransomware

Cloud Computing increased the use of malware attacks to gain unauthorised access to personal information over multiple networks.[92] It has also facilitated attacks via ransomware.[93] Malware refers to programs such as computer viruses, trojan horses and worms that are embedded in the electronic device and that could wreak havoc on the IoT by corrupting same or worse, gaining unauthorised access to a person's personal information, including credit card information and passwords and stealing same.[94]

Malware has been found more and more in 'fake' mobile applications whereby unsuspecting consumers due to the ease if installing new programs, download various mobile applications, only to find that the mobile application contains malware and has infiltrated the data subject's single device, which is connected to various other devices.[95]

Unlike malware, ransomware does not steal the personal information, instead, an unauthorised user encrypts the personal information by denying the authorised user access to their personal information.[96] A message is then sent to the owner of the personal information in which the unauthorised user demands payment for the release of the personal information, failing such payment, the personal information will be deleted or released to the public.[97] The massive worldwide cyberattack involving WannaCry ransomware that affected over 200 000 systems in more than 150 countries, the cyber-attacks on companies like Ashley Madison, the tracking of consumers buying behaviour and the geotagging abilities of most mobile applications have all whilst increased profits for companies and open the doors to a whole new market, have also increased the potential for abuse to a person's privacy.[98]

[92] Cassim F op cit note 80 at 16; Suryateja, P 'Threats and Vulnerabilities of Cloud Computing: A Review' (2008) 6 *International Journal of Computer Sciences and Engineering*
[93] Suryateja, P op cit note 92 at 18
[94] Cybercrime.org.za, 'Malware Definition', available at *http://cybercrime.org.za/malware/*, accessed on 10 March 2018
[95]Norton Security Centre 'Malware', available at *https://za.norton.com/internetsecurity-malware.html?inid=nortoncom_nav_internetsecurity-malware_homepage:homepage*, accessed on 10 March 2018; Suryateja, P op cit note 92 at 18
[96] Suryateja, P op cit note 92 at 18
[97] Kim Re op cit note 91 at 18; Cassim F op cit note 91 at 17
[98] Raul Rubio and Jaime Santisteban op cit note 29 at 7

A company's failure to examine its safety protocols and take the necessary precautions in protecting its consumer's personal information held electronically or reduce its risks can be devastating to the consumer and detrimental to the company's reputation.[99] With the number of cyber-attacks and ransomware increasing drastically, the value of personal data is growing exponentially with many hackers and scammers being able to access a person's account by knowing simple personal information insight including mother's maiden name, primary school or name of first pet, which are easily identifiable on social media networks,[100] having this knowledge makes access to financial accounts and conducting legal transactions easier.

Cloning of personal information such as identification documents and passwords are also becoming easier and more dangerous since most insurances do not cover transactions that have been authorised.[101]

(e) Phishing, Smishing and Vishing

Phishing is concerned with the creation of what seems to be a legitimate-looking email, appearing to come from a well-known institution such as a bank or other financial institution, requesting the user to click on a link in order to update or verify their personal or account information. If a user clicks on the link, it directs the user to a legitimate-looking website. After entering the user's personal details, account details, PIN and password on the fake website, the information is forwarded to the attackers, who are then able to access the user's bank account and transfer funds from the account into the attackers specially opened bank accounts. These accounts are then cleared of the transferred funds within minutes.[102]

Smishing is much like phishing, except that a text message is sent to cell phones instead of emails.[103]

---

[99] Mark Schroder 'To Catch a Cyber Thief' (2017). Without Prejudice
[100] Campbell F op cit note 87 at 17; George Beall op cit note 87 at 17
[101] Papadopoulos, Sylvia & Snail, Sizwe (eds) *Cyberlaw@SA III: The law of the internet in South Africa* (2012); Cassim F 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' (2015) 18 *Potchefstroom Electronic Journal* 93
[102] Nedbank 'Phishing, Smishing and Vishing', available at https://www.nedbank.co.za/content/nedbank/desktop/gt/en/aboutus/legal/fraud-awareness/phishing.html, accessed on 25 March 2018; Papadopoulos, Sylvia & Snail, Sizwe op cit note 101 at 19
[103] Ibid.

Vishing entails social engineering over the telephone where the user is called and lured into divulging personal information to an automated system. Fraudsters also use a technique called 'caller identity spoofing', where calls appear to be made from a legitimate or known number, allowing the fraudster to obtain your personal details.[104]

(f) Social Media and Social Engineering

The rise in IoTs and social media has produced another risk, social engineering, which refers to the process of retrieving valuable and often sensitive and personal information through illegal means and/or the realisation of some other illegal objective that targets individuals through deception and manipulation.[105] Social engineering could result in serious reputational damage to the person or, if the person uses the IoT for work purposes, major security breaches in a company.[106]

Lack of regulation on the processing of personal information on social media has opened the gates to the misuse of personal information together with many copyright and trademark infringement cases.[107]

Shandre Jansen van Rensburg and Johan Prinsloo illustrate the social engineering attack framework (that the attackers use to obtain personal information) as follows:

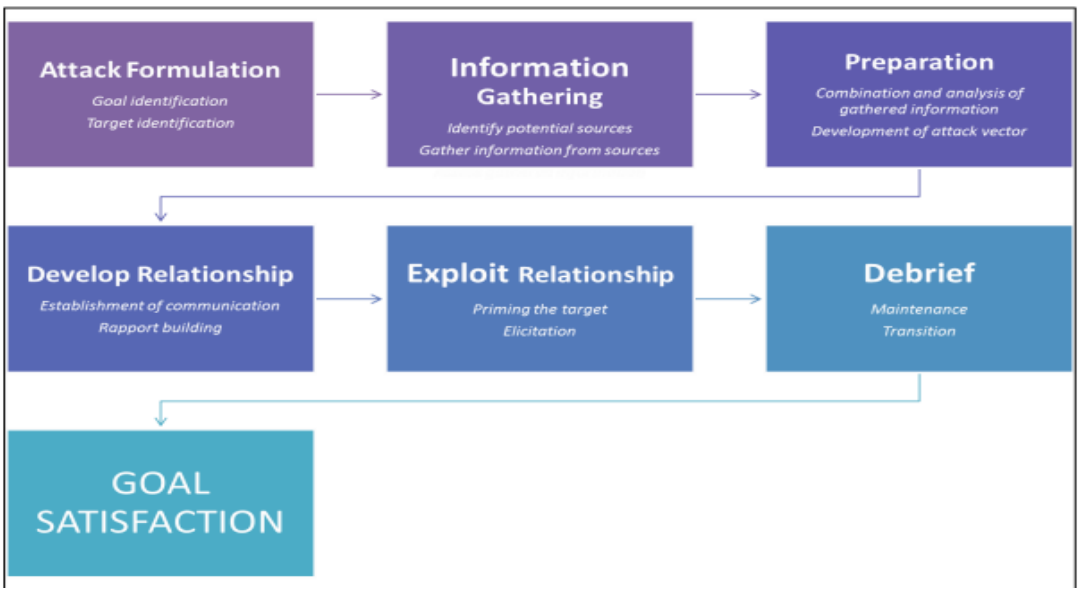

Figure 1: Social Engineering Attack Framework

[104] Ibid.
[105] Shandre Jansen van Rensburg and Johan Prinsloo 'The Criminogenic Significance of Social Engineering and the Need for Information Security' 2015 *Southern African Journal of Criminology* at 47
[106] Ibid.
[107] Campbell F op cit note 87 at 17; George Beall op cit note 87 at 17

Due to personal information forming part of a species of the right to privacy, not trite in law, South African case law and legislation has attempted to address some of the above risks identified through various court decisions and legislation as will be discussed in the next part.[108]

VI DATA PROTECTION LAWS IN SOUTH AFRICA RELEVANT TO IoTS

(a) Consumer Protection Act

As IoTs become more automated and decision making taken with limited or no human intervention after the coding stage, the question then as to who is liable when an IoT malfunctions or privacy is infringed becomes difficult to answer. Section 61 of the Consumer Protection Act[109] ('CPA') provides that irrespective of negligence each producer, importer, distributor or retailer of a particular product is strictly liable for any harm caused wholly or partly as a consequence of supplying any unsafe goods or a product failure, defect or hazard in any goods or instants where the consumer was provided with inadequate instructions or warnings in relation to any hazard arising from or associated with the use of the product.[110]

Each producer, importer, distributor and retailer of the product is jointly and severally liable, meaning that a person who suffers harm from a defective product can bring a claim against any person in the supply chain.[111]

For example, the vehicle manufacturers that aim to have a self-driven vehicle, able to learn and adapt could potentially learn the bad driving habits of the driver and accelerate too quickly or cause a traffic accident or in instances where a manufacturer who knowing the information security risks in its product, elects not to apply the necessary security measures to its device.[112] In terms of the CPA, every person in the supply chain from IoTs manufacturer, the suppliers, software programmer, business analysts, the company

[108] Waldo, James, Lin Herber and Millett Lynette op cit note 4 at 3
[109] Consumer Protection Act 68 of 2008
[110] Section 61(1) of the Consumer Protection Act 68 of 2008
[111] Consumer Protection Act 68 of 2008
[112] Brian A Browne, 'Self-driving Cars: On the Road To A New Regulatory Era' (2017) 8 *Journal of Law, Technology and the Internet*; Richard Kam, 'Connected cars: security and privacy risks on wheels' IAPP, available at *https://iapp.org/news/a/connected-cars-security-and-privacy-risks-on-wheels/*, accessed on 23 March 2018

that hosts a consumer/ businesses data to the system designers of various components that interlink and communicate with each other could be held liable.[113]

The CPA provides that a consumer may claim for the (a) death of, or injury to, any natural person; (b) an illness of any natural person; (c) any loss of, or physical damage to, any property, irrespective of whether it is movable or immovable. However, any economic loss that results from harm contemplated in paragraph (a), (b) or (c) due to the infringement to a consumer's privacy and/or failure to secure the personal information of a consumer has not been catered for by the CPA.[114]

Noteworthy is that juristic persons with a turnover in excess of R2 million are exempt from application of certain provisions, including the above provision in the CPA in terms of section 5 of the CPA. Accordingly, these juristic persons require other data protection laws in order to seek protection and enforcement of its right to privacy.

Section 11(3) of the Consumer Protection Act ('CPA'), read together with reg 4(3)(g) of the regulations provides for the establishment of an opt-out registry.[115] This registry enhances a consumer's right to privacy by allowing the consumer to unsubscribe or opt out from any subscription. With the interconnectedness of IoTs, the question remains, does opting out of one IoT mean that all IoTs on the network are precluded from receiving the communication?

(b) Electronic Communications and Transactions Act

With regard to IoTs operating in the world of electronic communications, the Electronic Communications and Transactions Act ('ECTA') together with the CPA regulates this environment.[116] ECTA deals with electronic contracts concluded by persons using a machine or electronic device as a medium.

[113] Jamie Cartwright 'Product liability and the internet of things' (2017) Charles Russel Speechlys, available at *https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/commercial/2017/product-liability-and-the-internet-of-things/*, accessed on 21 July 2017

[114] Section 61(5) of the Consumer Protection Act 68 of 2008

[115] Consumer Protection Act 68 of 2008.

[116] Electronic Communications and Transactions Act 25 of 2002; Consumer Protection Act 68 of 2008

ECTA has attempted to enhance or amend the common law to include protection of a person's personal information and to combat cybercrime. Regulation into the protection of personal information by ECTA is governed by chapter 8, however, the adherence to the principles therein are voluntary and regulated by agreement between the parties.[117]

Once agreed, the parties are obliged to subscribe to all 9 data protection principles including processing personal information with the knowledge of the data subject[118] for a lawful[119] purpose[120] and which process is only necessary to fulfil the purpose.[121] Disclosure to third parties may take place under circumstance where it is required, permitted by or with the express written consent of the data subject.[122]

If personal information is processed outside of the purpose its was collected, the data subject must have expressly consented thereto.[123] Records of the personal information, its specific purpose, details of a third party should personal information be disclosed must be retained for as long the personal information is being used and at least 12 months thereafter.[124]Any personal information must either be destroyed or converted to statistics whereby the identification of the data subject is unknown and cannot be ascertained.[125]

The issue with ECTA is that compliance by IoT manufactures and suppliers is voluntary and there is no provision for the establishment of a regulatory authority to enforce compliance.[126]

Although ECTA makes provision for cyber inspectors, the provisions are largely ineffective as to date, no cyber inspectors have been appointed in South Africa. With regard to IoTs, ECTA regulates automated contracts entered into without human intervention or authorisation by acknowledging that no agreement is formed where a natural person directly interacts with an electronic agent of another person and has made a material error during the transaction provided the electronic agent did not provide the

[117] Section 50(4) of the Electronic Communications and Transactions Act 25 of 2002
[118] Section 52(3) of the Electronic Communications and Transactions Act 25 of 2002
[119] Section 52(2) of the Electronic Communications and Transactions Act 25 of 2002
[120] Section 52(2) of the Electronic Communications and Transactions Act 25 of 2002
[121] Section 52(4) of the Electronic Communications and Transactions Act 25 of 2002
[122] Section 52(4) of the Electronic Communications and Transactions Act 25 of 2002
[123] Section 52(5)-(8) of the Electronic Communications and Transactions Act 25 of 2002
[124] Section 52() of the Electronic Communications and Transactions Act 25 of 2002
[125] Section 52(9) of the Electronic Communications and Transactions Act 25 of 2002
[126] S v Miller and Others 2016(1) SACR 251 (WCC)

person with an opportunity to address the error.[127] The question however remains that in instances where a natural person has provided once-off consent to transactions as deemed necessary by an IoT with AI or ML capabilities, will such person's consent create a legally binding agreement if the AI or ML determines that a deviation from authorised instruction is required and that such deviation does not warrant new authorisation.

(c) Promotion to Access to Information Act

The Promotion to Access to Information Act[128] ('PAIA') permits the overriding of an individual's privacy rights with regards to the processing of their personal information in favour of the public interest argument or an individual's Constitutional right of access to information.[129]In terms of PAIA, every entity is required to have a PAIA manual which stipulates what information a person has the right to request and grounds for refusing access.[130]

Data protection principles are addressed in PAIA by granting individuals access to records containing personal information relating to themselves, requiring persons to take reasonable steps to establish suitable internal mechanisms that enable the correction of personal information and prohibits the disclosure of records that identify personal information relating to third parties.[131] These data protection principles empower individuals to take active steps to manage what and how their personal information is processed and thereby reduce the risks to the mismanagement of an individuals' personal information

(d) The National Credit Act

The National Credit Act[132] ('NCA') gives individuals the right to access and challenge credit records and whilst limiting in data protection, it does provide for the right to confidentiality by stating that 'any person who receives, complies, retains or reports

[127]Section 20 of the Electronic Communications and Transactions Act 25 of 2002; see also S v Miller and Others 2016(1) SACR 251 (WCC)
[128] Promotion to Access to Information Act 2 of 2000
[129] Section 32 of the Constitution of the Republic of South Africa; Brümmer v Minister for Social Development and Others 2009 (11) BCLR 1075 (CC)
[130] Preamble to the Promotion to Access to Information Act 2 of 2000; see also BHP Billiton PLC Inc v De Lange (189/2012) [2013] ZASCA 11
[131] Section 11, 34, 50 and 63 of the Promotion to Access to Information Act 2 of 2000; Mahaeeane v Anglogold (85/2016) [2017] ZASCA 090
[132] The National Credit Act 34 of 2005

confidential information relating to a consumer or prospective consumer must protect the confidentiality of that information'.[133] IoTs, such as mobile applications with credit facilities and payment mechanisms processing financial information must ensure compliance with the NCA.

Confidential Information is defined in the NCA as personal information that belongs to a person and is not generally available to or known by others.[134]Personal information has not been defined but a definition for consumer credit information held by credit bureaus has been provided for.[135] Among other responsibilities, the NCA requires credit bureaus to take reasonable steps to verify the accuracy of the consumer credit information, retain records for the prescribed period, erase any records not permitted to be recorded or is required to be removed and from knowingly or negligently providing any credit report containing inaccurate information pertaining to the consumer's credit.[136]

The benefit of the NCA to data protection is that there is a regulatory body which can issue enforcement notices and provides for non-compliance as an offence.[137] As consumer credit information would form part of the definition of personal information due to it being related to a data subject's financial information, the National Consumer Tribunal would need to also develop regulations to ensure that credit bureaus process personal information in line with POPIA, once enacted.[138]

(e) RICA and ICASA

A powerful South African piece of legislation that both protects the right to privacy and limits this right can be found in the Regulation of Interception of Communications and Provision of Communication Related Information Act'(RICA').[139] RICA provides that no person, who is not a party to the communication or who has not obtained prior written consent or is not acting in the course of business, may at any place in South Africa intentionally intercept, attempt to intercept, authorise or procure any other person to

[133] Section 68 of the National Credit Act 34 of 2005
[134] Section 1 of the National Credit Act 34 of 2005
[135] Section 70 of the NCA defines consumer credit information to include *inter alia* a person's credit history (application for credit, credit agreements concluded etc), financial history (past and present income, assets and liabilities etc), education, employment, business history or identity)
[136] Section 70(2) of the National Credit Act 34 of 2005
[137] Section 12 of the National Credit Act 34 of 2005
[138] Section 1 of the Protection of Personal Information Act 4 of 2013
[139] Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002

intercept or attempt to intercept any communication in the course of its occurrence or transmission.[140] Accordingly, internet service providers may only intercept and monitor any communication between IoTs with the authority of a judge and subject to this authority must ensure that they protect the communication thereof.[141]

Furthermore, the Independent Communications Authority of South Africa ('ICASA') is a regulatory body that requires the registration of devices that transmit digital signals/ frequencies.[142] Therefore, ICASA has the potential to regulate IoTs which produce an electronic signature when processing personal information between devices and these regulations should be adapted in line with the principles of POPIA.[143]

(f) Protection of Personal Information Act

One of the biggest threats and risks from the use of IoTs is data privacy and security of personal information.[144] Currently, the most important legislation relevant to addressing these risks are POPIA.[145] However, it must be noted that whilst the Information Regulator has published the highly anticipated regulations pertaining to POPIA,[146] at the time of preparing this research report, POPIA is was not effective.

The regulations highlight the responsibilities of the information officers including inter alia, the development of a PAIA manual, setting out a compliance framework which implements, monitors and assesses compliance with POPIA when processing personal information together with an obligation to conduct internal training awareness programs.[147]

[140] Section 12 and 15 of Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002
[141] S v Miller and Others 2016(1) SACR 251 (WCC)
[142] Independent Communications Authority of South Africa Act 13 of 2014; Type Approval Regulations 2013; ICASA Code of Ethical Conduct (2016)
[143] Independent Communications Authority of South Africa Act 13 of 2014; Type Approval Regulations 2013; ICASA Code of Ethical Conduct (2016)
[144] Cassim F op cit note 101 at 19*;* Dhillon, G., and Backhouse, J 'Information system security management in the new millennium' (2000) 43 *Communications of the ACM* 125- 128
[145] Preamble to the Protection of Personal Information Act 4 of 2013
[146] Regulations relating to the Protection of Personal Information, published in the Government Gazette, volume 642, 14 December 2018, number 42110
[147] Ibid.

The amount of personal information a data subject inputs on a company's online platform such as its websites or mobile applications, the permissions that are to be granted in order for the IoT to operate has led many companies with an abundance of Big Data.[148]

Any person who processes the data subject's personal information will be considered a responsible party and will need to comply with POPIA.[149] The definition of processing in terms of POPIA is so broad that one must then consider the individual's right to privacy and the extent to which an individual can claim privacy in the digital age. As previously discussed, this involves determining the role the individual plays and the type/ nature of the personal information processed.[150]

The lack in territorial limitation in the use of IoTs has resulted in governments establishing co-operation mechanisms to ensure that domestic legislation is in line with international standards.[151] Many businesses in South Africa are as a result of franchises and licenses from franchisors and licensors outside the Republic which requires information, especially personal information to be transferred outside South Africa.[152] Accordingly, section 72 of POPIA is applicable as it details when a company may process the personal information outside the Republic.[153] Section 72 facilitates maintenance of foreign law and regulations as countries in the European Union[154], Canada,[155] United Kingdom,[156] United States of America[157] and New Zealand[158] have developed legislation that is compliant if not stricter than POPIA in order to create a harmony between cross border transactions.

---

[148] Bernard Marr op cit note 23 at 6

[149] Section 8 of the Protection of Personal Information Act 4 of 2013

[150] Roos, A op cit note 47 at 10; Verine Estebeth, 'Individuality and Privacy slides' University of Witwatersrand (2017)

[151] Section 72 of the Protection of Personal Information Act 4 of 2013; Naude and Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (2)' (2016) 79 *THRHR*, 213–230

[152] Research IQ survey commissioned by Franchise Association of South Africa in collaboration with Sanlam. The estimated turnover for the franchise market in 2016 was R587 billion Rand, which amounted to 13,3% of the South African GDP. Furthermore, one in eight franchises claimed to be an international brand

[153] Section 72 of the Protection of Personal Information Act 4 of 2013

[154] Regulation (EU) 2016/679 op cit note 48 at 11

[155] Personal Information Protection and Electronic Documents Act op cit note 52 at 11

[156] Data Protection Act 2018 op cit 53 at 11

[157] Federal Trade Commission Act op cit note 54 at 12

[158] The Privacy Act 28 of 1993 op cit note 55 at 12

In line with POPIA, the following challenges have been identified and related to each of the 8 conditions thereof.

Condition 1 refers to accountability whereby the responsible party is to ensure conditions for lawful processing are upheld.[159] The responsible party is the person who determines the purpose and means for processing the personal information.[160] The question who is the responsible party is important, is it the device manufacturers, social media platform, third party application developer, data hosts/ internet service providers or insurers.[161]
As a machine cannot be held liable, investigation into the source of the error, i.e at the time personal information was collected, transmitted between IoTs, internet service providers or social media platform, whether the personal information was stored on servers situated locally or internationally must be considered to assess who the responsible party or at least operators are. The question arises whether the data subject could employ section 61 of the CPA and hold any person within the distribution network liable thereof.[162] Failing the applicability hereof, the common law principles pertaining to proving a delictual claim would need to be undertaken.[163]

Condition 2 refers to lawfulness, minimality, consent and collection of personal information.[164] Only personal information required for its specific purpose may be processed and the responsible party cannot process personal information that they believe will be used in the future. In order to process the personal information, the responsible party must either have the data subject's consent, process the personal information that is necessary for the performance of the contract which the data subject is a party to, or if the process is necessary for a legitimate interest of the responsible party except where it conflicts with the rights of the data subject.[165]

[159] Section 8 of the Protection of Personal Information Act 4 of 2013
[160] Section 8 of the Protection of Personal Information Act 4 of 2013
[161] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3; and Promotion to Access to Information Act 2 of 2000
[162] Jamie Cartwright op cit 113 at 22
[163] Roos A, D. van der Merwe (eds) op cit note 37 at 9; Neethling, J; M Potgieter, J M and Visser P J op cit note 36 at 8
[164] Section 9 of the Protection of Personal Information Act
[165] Section 9, 10, 11, 12 and 18 of the Protection of Personal Information Act

To ensure informed consent is obtained, IoTs must have the technological capabilities of giving a data subject sufficient information about the personal information that will be processed.[166] More importantly, should a data subject refuse to give consent to the processing of certain personal information, the data subject should not be precluded from using the IoT (provided the personal information required is not fundamental to the IoT being able to function).[167] Informed consent may result in tick boxes being insufficient for purposes of providing proof that the data subject has been informed about the manner in which personal information will be processed.

Furthermore, because of IoTs capabilities of linking and transferring personal information between devices, informed consent must be granted prior to an IoT sharing personal information and the data subject should be able to evaluate and determine its own trusted network of devices.[168] IoT security must be able to preclude the transfer of personal information from devices not on the trusted network or a new device entering a network if informed consent has not been granted.[169] Due to the landscape evolving, new IoTs are being developed on a daily basis. Once-off consent could increase the risk of a data subject's privacy being invaded.[170]

Condition 3 makes specific reference to collection for the specific purpose and discusses the retention and restriction of records.[171] Because IoTs communicate between devices, IoTs are able to aggregate data and form Big Data which has the potential to reveal specific aspects of a data subject's habits, behaviour and preferences ,resulting in the data subject being susceptible to IoTs invading the data subject's privacy and exploiting the personal information gathered.[172] For example, take the incident at Target whereby the organisation was able to track the purchasing behaviour of an individual and when the Big Data was processed, Target was able to analyse that the individual was pregnant and start target marketing the individual with maternity advertisements.

[166] Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3
[167] Jessica W. Berg *Informed Consent: Legal Theory and Clinical Practice* (2nd edition) (1986)
[168] Ibid.
[169] Ibid.
[170] Ibid.
[171] Section 13 and 14 of the Protection of Personal Information Act 4 of 2013
[172] ZXC v Bloomberg LP 92017) EWHC 328 (QB); Cukier. K & Mayer-Schonberger.V op cit note 24 at 6; Bernard Marr op cit note 23 at 6

The problem was that the individual was age 16 and furthermore she had not informed her father who had started receiving the marketing material as the daughter would use her father's credit details.[173] Thus, IoT stakeholders need to have an already perceived overview of the business, what personal information and why same is being processed. It must therefore be asked: was the aggregation of data by Target correct?

Furthermore, personal information is not permitted in terms of POPIA to be retained longer then the its purpose.[174] Each responsible party's or operators' requirements and use for the personal information must be clear in order to be communicated with the data subject before the information is processed as to the period of retention and the ability to operate same.[175] For example, any personal information that is processed when a data subject subscribes to an IoT must be deleted should that data subject unsubscribe unless it is required to be kept for a prescribed period or converted into de-identifiable statistics.[176]

Condition 4 refers to further processing which uses the personal information that was obtained for a specific purpose for a secondary purpose.[177] It entails using Big Data for a different purpose for which consent was provided for.[178] IoTs capabilities in processing Big Data should, unless informed consent is granted, be limited to processing personal information required for its functionality. Should a capability arise to better enhance user experience, a pop-up message requesting consent to the further processing should appear prior to any processing.[179] Only once permission is granted can the IoT process the personal information and such information that is processed cannot be historical information but rather only the personal information gathered from the date of consent.[180]

---

[173] Hill K 'How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did' (2012), available at *https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#66b387ef6668*, accessed on 17 July 2017
[174] Section 14 of the Protection of Personal Information Act 4 of 2013
[175] Cukier. K & Mayer-Schonberger.V op cit note 24 at 6; Bernard Marr op cit note 23 at 6
[176] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3; and Promotion to Access to Information Act 2 of 2000.
[177] Section 15 of the Protection of Personal Information Act 4 of 2013
[178] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3
[179] Jessica W. Berg op cit note 167 at 29
[180] Hussain v Sandwell MBC (2017) EWHC 1641

Condition 5 states that information must be of a good quality.[181] With so many IoTs connected and managed by one user, the responsible party or operator processing the personal information must ensure that it obtains complete, accurate and information that is not misleading. Further, it must take the necessary steps to provide the data subject with an opportunity to update and delete the personal information.[182] Cloud Computing and social media however have complicated this requirement because personal information processed by IoTs through search engines such as Google and various social media platforms are never truly deleted in its entirety.

European case law[183] has attempted to place an obligation on companies such as Google to provide the data subject with the right to be forgotten[184] from online searches and metadata keyword searches in the event that personal information is outdated or inaccurate, however, the application this ruling is still in its infancy phase.

Condition 6 refers to openness or transparency[185] which is the key to ensuring information quality is maintained. The data subject must clearly be notified about the identity of the responsible party or operator, the reasons for the processing and how to contact the responsible party in order to amend, delete or update any of the data subject's personal information.[186] This right is also facilitate by the rights governed in PAIA, as discussed previously and the CPA which requires that such notification must be in plain and simple language in order for the consumer to make a fair and informed decision.[187]

Condition 7 refers to security of personal information.[188] The responsible party must take the necessary precautions and implement appropriate technical and organisational measures and protocols to protect the integrity, access of the personal information, prevent a breach and notify the relevant parties if a breach does occur.[189]

---

[181] Section 16 of the Protection of Personal Information Act 4 of 2013
[182] Al-Ko Kober Ltd & Anor v Sambhi [2018] EWHC 165 (QB) (02 February 2018); Richard Kemp op cit 11 at 5; and Promotion to Access to Information Act 2 of 2000
[183] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014) Court of Justice European Union, Luxembourg
[184] Article 17 (2) of Regulation (EU) 2016/679 op cit note 48 at 11
[185] Section 16 and 17 of the Protection of Personal Information Act 4 of 2013
[186]Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3
[187] Section 22 of the Consumer Protection Act 68 of 2008
[188] Section 19 – 22 of the Protection of Personal Information Act 4 of 2013
[189] Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3; Cybercrimes and Security Bill, 2017 and Hauman M op cit note 89 at 17

The question remains who is the responsible party and if multiple responsible parties or operators, who must ensure compliance with condition 7? As discussed in chapter 5 of this report, the security risks IoTs face on a daily basis results in security breaches being one of the greatest risks to data privacy. It is therefore imperative that condition 7 is addressed from the conception of the IoT to the distribution and usage of the IoT. Furthermore, security to the IoT together with security to the network itself is required in order to ensure a complete security compliance check. These safety measures must always remain updated in order to stay abreast with the latest cybercrime activities.

Condition 8 refers to the data subject's participation.[190] The user must have control over the processing of its personal information and because all IoTs are interconnected, it remains possible to re-identify the user even after being anonymised on one device, thus the user has certain rights to participate with the personal information being processed. The IoTs responsible party and the user must have the ability at all times to obtain the details of its personal information that was or is being processed and to also be able to withdraw the consent previously granted to the responsible party or to object to the processing of certain personal information.[191]

A solution for compliance with POPIA could potentially rest in the use of blockchain technology. Blockchain technology may assist in mitigating some of the risks due to its transparency and accountability of transactional recordings. A blockchain is a relatively new technology whereby a general ledger is created, certified and distributed amongst multiple nodes either publicly as in the case of Bitcoin or more recently within a specific network of organisations such as banks through the use of private blockchains.[192]
Whichever user has been granted access to the network effectively has access to the information contained on that blockchain.[193] The ledger forms an immutable record in that once the transaction has been entered into the blockchain, it is distributed and cannot be modified by the users on the network.[194]

[190] Section 23 – 25 of the Protection of Personal Information Act 4 of 2013
Richard Kemp op cit 11 at 5; and Promotion to Access to Information Act 2 of 2000
[192] Collin Thompson, 'The difference between a Private, Public & consortium Blockchain' available at *http://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html,* accessed on 1 June 2017
[193] Greg McMullen and Florian Glatz 'Blockchain & Law in 2017: Finally friends or still foes?', available at *https://medium.com/ipdb-blog/blockchain-and-law-in-2017-f535cb0e06c4*, accessed on 28 July 2017
[194] Tech Law Blog op cit note 69 at 14

Therefore, public blockchains are peer-to-peer reviewed transactions with each transaction being time stamped which time stamp is inalterable and once combined to form a block, the block is linked to the previous block by way of a complex computer algorithm.[195] Effectively these blocks cannot be altered, deleted or amended. To the extent that a modification does take place, the modification is recorded as a separate transaction which is reflected in the blockchain, thus, one will always be able to view the original transaction and the amended transaction somewhere in the blockchain.[196] Blockchains do however have the potential to conflict with condition 5 in that personal information not being processed or found to be obsolete must be deleted. This would require an old block to be deleted, which is difficult on a blockchain as the blocks interrelate. While parties would still require an agreement or contract, blockchains would facilitate the payment or performance and the recordal thereof.[197]

In the context of POPIA, should there be non-compliance in terms of protecting a data subject's personal information, the aggrieved party may lodge a complaint with the Information Regulator.[198] The Information Regulator does not require a court order to institute a fine for negligence or non-compliance in favour of the aggrieved party in terms of POPIA. Accordingly, a maximum period of imprisonment of ten years, or an undisclosed maximum fine, which is determined by the relevant court on a case-by-case basis.[199] Furthermore, the Information Regulator may assert an administrative fine up to a maximum amount of ten million Rand.[200]

(g) Cybercrimes Bill

Cybercrime or computer crime has no exact definition due to the reason that the context of the criminal activity dictates the definition. For example, an IoT could be seen as an object when the hardware or software is stolen in which case the crime relates to theft of property, however, where the device is used as an instrument to commit a crime, the

[195] Tech Law Blog op cit note 69 at 14; Bhaskara Sannapureddy 'Pros & Cons of Internet of Things (IoT)' (2015) LinkedIn, available at *https://www.linkedin.com/pulse/pros-cons-internet-things-iot-bhaskara-reddy-sannapureddy*, accessed on 2 July 2017 and Sophia Moganedi and Jabu Mtsweni op cit note 5 at 4
[196] Tech Law Blog op cit note 69 at 14; and Sophia Moganedi and Jabu Mtsweni op cit note 5 at 4
[197] Bhaskara Sannapureddy op cit note 195 at 33; and Greg McMullen and Florian Glatz op cit note 193 at 32
[198] Section 74 pf the Protection of Personal Information Act 4 of 2013
[199] Section 107 of the Protection of Personal Information Act 4 of 2013
[200] Section 109 of the Protection of Personal Information Act 4 of 2013

criminal offence is that of computer crime or cybercrime in terms of the Criminal Procedure Act.[201] The latter examples is relevant to this research report, as will be discussed below.

Organised cyber groups, new smart viruses and the fact that cybercrime is borderless has complicated our current legal structure and requires new law that is adaptable.[202] As cyber hacking and cyber ransomware can use personal information processed by IoTs the South African legislature has proposed new legislation in the form of the Cybercrimes Bill[203].

For purposes of this report, only application of section 2 to sections 9 will be discussed. These sections in the Bill provide offences that criminalise the unlawful securing of access without the necessary authority,[204] the use of software or hardware tools in the commission of a cybercrime,[205] the unlawful inferences with data or a computer program and a computer data storage medium or a computer system,[206] the unlawful use of passwords, access codes and similar data or devices to commit an offence.[207]

Section 2 caters for the unauthorised access of data by a person or causing a computer program to access the data without authorisation. Persons using IoTs to access and process personal information without a data subject's consent could be found guilty of an offence.[208] The Bill does not require that the data must be used for illegal purposes, merely that accessing same without authority is an offence.

Section 3 makes it an offence to possess personal information of a third party for purposes of committing an offence and provided such person cannot provide satisfactory reasons as to the possession thereof.[209]

---

[201] Criminal Procedure Act 51 of 1977; Magobodi v Minister of Safety and Security 2009 (1) SACR 355 (Tk); Cassim F op cit note 80 at 16

[202] Ewan Sutherland 'Governance of cybersecurity- the case of South Africa' (2017) 20 *The African Journal of Information and Communication* 83-112

[203] Final Bill as Presented by Portfolio Committee on Justice and Correctional Services dated 23 October 2018, as introduced to the National Assembly as the Cybercrimes and Cybersecurity and Related Matters Bill, published in the Government Gazette, volume 603, 2 September 2015, number 39161, hereinafter referred to as the 'Bill'

[204] Section 2 and 3 of the Bill

[205] Section 4 of the Bill

[206] Section 5 and 6 of the Bill

[207] Section 7 of the Bill; Tech Law Blog op cit note 69 at 14; and Cassim F op cit note 80 at 16

[208] Ewan Sutherland op cit note 202 at 34

[209] Ewan Sutherland op cit note 202 at 34

This provision provides for the use of interception tools such as social engineering, dumpster diving and attempts to criminalise phishing attacks, identity theft, ransomware attacks and behavioural tracking on another person.[210]

Section 4 caters for scenarios whereby criminals access an IoT in order to access the general network that the device is connected to with the intention to interfere or intercept data in order to commit further crimes.[211]

Section 5 and 6 attempts to protect the integrity, confidentiality and availability of data, computer programs, data storage mediums and computer systems by criminalising the interception thereof. This section reiterates the provisions of RICA, as previously discussed in this report.

Section 7 aims to protect the unauthorised access and distribution of passwords, codes and similar data where the intention is to do for the purposes of committing an offence.[212]

Section 8 and section 9 provides that the use of any of the above sections for purposes of defrauding or misrepresenting a situation or makes/passes off false data or a false computer program that causes actual or potential prejudice amounts to an offence in terms of cyber fraud or cyber forgery and uttering.[213] In terms of section 10 a person or unlawfully and intentionally threatens to commit any offence; or commits the offence, for the purpose of obtaining any advantage from another person or compelling another person to perform or to abstain from performing any act shall be guilty of cyber extortion.[214]

One of the aims of the Bill is to address the security and legal risks IoTs pose when processing personal information.[215] Bearing in mind one of the disadvantages being different jurisdictional laws of the different countries, the Bill declares that offences occurs within the boundaries of the Republic of South Africa if the offence occurred in the Republic of South Africa or if offence occurred outside the Republic of South Africa but the effect is in the Republic of South Africa.[216]Accordingly, any court in the Republic

[210] Arnaud De Borchgrave *Cyber Threats and Information Security: Meeting the 2 1'1 Century Challenge* (2001)
[211] Ewan Sutherland op cit note 202 at 34
[212] Section 7 of the Bill
[213] Section 8 and 9 of the Bill; Ewan Sutherland op cit note 202 at 34
[214] Section 10 of the Bill; Jonathan Burchell op cit note 33 at 8
[215] Preamble to the Bill
[216] Section 24 of the Bill

of South Africa has jurisdiction and thus there is no restrictions in terms of radius of courts and with regards to IoTs, ships and aircrafts, the registered address must be in the Republic of South Africa.[217]

The above legislation when viewed holistically aims to address the gap in the right of a person's privacy in relation to personal information processed by third parties. Once legislation such as POPIA and the Bill are enacted, it is hopeful that the recommendations which are discussed directly below will become enforceable to ensure that the risks are mitigated as far as possible and if not, that recourse is available to persons whose rights have been infringed.

VII RECOMMENDATIONS

After consideration of all applicable data protection laws in South Africa and internationally and on review of the ICO,[218] GDPR,[219],FTC[220] and POPIA[221] commentary, certain steps need to be taken by the various stakeholders in the development of IoTs. These would include conducting a privacy impact assessment prior to launching any new IoT, deleting the raw data immediately once the data that is required and consent to the processing has been extracted and applying the principles of privacy by design and privacy by default which means that the that the data protection protocol and compliance framework must be integrated into the design of IoTs and that the compliance framework should be the default with reference to the privacy rules.[222]

The data subjects should always remain in control and be able to participate in the processing of its personal information and this personal information should be disseminated to the data subject in a user-friendly manner that is in plain and simple language.[223]

---

[217] Section 24 of the Bill; Papadopoulos, Sylvia & Snail, Sizwe op cit note 101 at 19; and Sophia Moganedi and Jabu Mtsweni op cit note 5 at 4; and Cassim F op cit note 80 at 16

[218] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3

[219] Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3; and James Halliday and Rebekah Lam, 'Internet of Things some legal and regulatory implications' (2016) Baker and Mckenzie, available at *http://www.bakermckenzie.com/en/insight/publications/2016/02/internet-of-things-some-legal-and-regulatory-imp__/*, accessed on 21 July 2017

[220] Richard Kemp op cit 11 at 5; and Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3

[221]Richard Kemp op cit 11 at 5; and Carsten Maple op cit note 6 at 4

[222] Ettiene Retief, 'Look within' (2017) Without Prejudice; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3

[223] Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3

Explicit, informed and freely given consent of the data subject must be obtained and the data subject must be permitted to withdraw consent at anytime and show evidence that such personal information has indeed been deleted.[224]

Only trusted and authenticated coding or software programs are to be executed on the IoT for which international standards or regulations should be developed to confirm the trustworthiness and authenticity of the program.[225]

Personal networks should not be permitted access to work networks and the number of users who have access to a single device should be limited to those who essentially require same.[226]

Records that tracks user's logins and logouts together with an analysis of what actions were taken by the IoT should be created.[227] Blockchain technology is useful in this regard as the ledge provides an immutable record.

Constant risk training and awareness programs must be provided on a regular basis to all staff who have access to any IoT or the network itself.[228]

From a manufacturing point of view, manufacturers of IoTs should first, amongst others, ensure that it gives the data subject due notice of the information it collected, stored, used, disseminated, shared, received and how the information will be combined, if applicable.[229] Secondly, manufacturers must maintain a list of all applicable stakeholders to a given device and notify same when a data subject withdraws consent. Thirdly, afford an IoT the ability to disable the wireless interface when the device is not being used together with providing tools and a system that permits the data subject to edit or update the data before it is transferred to the responsible party.

---

[224] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3

[225] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3

[226] Arnaud De Borchgrave op cit note 210 at 35; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3

[227] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3

[228] Arnaud De Borchgrave op cit note 210 at 35; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3

[229] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3; and James Halliday and Rebekah Lam op cit 219 at 36; and Alison Job 'IoT and Cyber security' (2017) IT Web, available at *http://v2.itweb.co.za/event/itweb/security-summit-ct2018/?page=news&itwid=166589*, accessed on 10 March 2018

Fourthly, manufactures should aim to work together with organizations to standardize IoTs, develop common protocols amongst all stakeholders and perform regular training and awareness programs to employees and data subjects on the processing of information and ensuring adequate security features are undertaken by the data subject's device and ensure there are adequate multiple layers of security in IoTs in order to prevent or mitigate the cyber security risks.[230]

VIII CONCLUSION

South Africa needs to ensure that multiple steps are undertaken in order to effectively combat the legal risks in the processing of personal information.[231]

First, organisations must conduct a POPIA compliance assessment to help mitigate data privacy risks. It requires the appropriate and reasonable measures as discussed above in the eight conditions.[232] Together with this exercise, organisation must conduct risk assessments in which it identifies the risks in order to establish safe guards and most importantly constantly update its system. This assessment entails assessing your organisations data, identifying where it is located, and security around it. Around the world, organisations are using what is known as 'white hacker', who are individuals who perform penetration tests with the organisations consent in order to assess an organisations security safeguards and determines its risks.[233]

Secondly, organisations must take technical and organisational measures such as having computer passwords at an acceptable standard and which are constantly changed. Organisational policy should stipulate that employees are to lock their computer when leaving their desk and close the doors if in an access control area.[234] However, the most important aspects that organisations must cater for are (1) human error and (2) that employees will only become cyber vigilant if they are constantly trained and informed of the potential threats. Thus, a compliance culture must be adopted to protect your own

[230] Arnaud De Borchgrave op cit note 210 at 35
[231] Melody Musoni 'Is cyber search and seizure under the cybercrimes and cybersecurity bill consistent with the protection of personal information act' 2016 *Obiter* 683–694
Richard Kemp op cit 11 at 5; and James Halliday and Rebekah Lam op cit 219 at 36
[233] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3
[234] Richard Kemp op cit 11 at 5; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3

and the organizations personal information in order to reduce employee and organisation risks.[235]

Thirdly, as with many of the technological nuisances, new business ventures are created. Cyber insurance is one of these nuisances, with many global firms offering various packages. The issue with cyber insurance is that it mitigates an organisation's liability but does not prevent the cyber-attack itself.[236]

The aim of this report has been to provide the reader with a basic overview about IoTs, data privacy and security risks inherent in current IoTs against existing legislation as well as highlight some recommendations to both manufacturers and legislatures to mitigate these risks to privacy. South Africa needs to urgently look to foreign practices in order to enact a legal framework that caters for the current digital issues reflected above as well as for futuristic problems. The law needs to be flexible, hopefully with the constant publication of regulations and protocols in order that one can enjoy the benefits of the fourth industrial revolutions while simultaneously limiting the risks to privacy.

[235] Carsten Maple op cit note 6 at 4; Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S op cit note 4 at 3

[236] Partly Report SA 'Cybercrime and cybersecurity bill invokes suspicion', available at *http://parlyreportsa.co.za/communications/cybercrime-cybersecurity-bill-invokes-suspicion/*, accessed on 24 July 2017

BIBLIOGRAPHY

SOUTH AFRICAN LEGISLATION AND BILLS

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Criminal Procedure Act 51 of 1977

Cybercrimes and Cybersecurity Bill, (2017)

Electronic Communications and Transactions Act 25 of 2002

Final Bill as Presented by Portfolio Committee on Justice and Correctional Services dated 23 October 2018, as introduced to the National Assembly as the Cybercrimes and Cybersecurity and Related Matters Bill, published in the Government Gazette, volume 603, 2 September 2015, number 39161

Financial Intelligence Centre Act 38 of 2001.

Independent Communications Authority of South Africa Act 13 of 2014

National Credit Act 34 of 2005

Prevention of Organised Crime Act 121 of 1998.

Promotion to Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002

FOREIGN STATUTES

Data Protection Act 2018

Federal Trade Commission Act 15 U.S.C. §§ 41-58, as amended

Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)

Privacy Act 28 of 1993

Privacy Amendment Act 12 of 2017

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (2016), pp. 1-88 Key: citeulike:14071352

CASE LIST

SOUTH AFRICAN

Bernstein v Bester No 1996 (2) SA 751 (CC)

Brümmer v Minister for Social Development and Others 2009 (11) BCLR 1075 (CC)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; in re Hyundai Motor Distributors (Pty) Ltd v Smit NO 2001 (1) SA 545 (CC)

Jafta v Esemvelo KZN Wildlife (D204/07) (2008) ZALC 84

Ketler Investments CC t/a Ketler Presentations v Internet Service Providers Association 2014 (2) SA 569 (GSJ)

Magobodi v Minister of Safety and Security 2009 (1) SACR 355 (Tk)

Mahaeeane v Anglogold (85/2016) [2017] ZASCA 090

Nm and Others V Smith and Others (Freedom of Expression Institute as Amicus Curiae) 2007 (5) SA 250 (CC)

O'Keeffe v Argus Printing and Publishing Co Ltd 1954 (3) 244 (C)

S v Makwanyane 1995 (3) SA 391 (CC)

S v Miller and Others 2016(1) SACR 251 (WCC)

FOREIGN

Al-Ko Kober Ltd & Anor v Sambhi [2018] EWHC 165 (QB) (02 February 2018)

Anthony Woolley And Deborah Woolley Against Nahid Akbar Or Akram (2017) Scotsc 7 (03 February 2017)

Federal Trade Commission, v. D-Link Corporation and D-Link Systems, Inc., corporations, 3:17-CV-00039-JD

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014) Court of Justice European Union, Luxembourg

Hussain v Sandwell MBC (2017) EWHC 1641

ZXC v Bloomberg LP 92017) EWHC 328 (QB)

BOOKS

Jessica W. Berg *Informed Consent: Legal Theory and Clinical Practice* (2nd edition) (1986) Oxford University Press

Arnaud De Borchgrave *Cyber Threats and Information Security: Meeting the 2 1'1 Century Challenge* (2001) Washington D.C, CSIS Press

Reinhardt Buys & Francis Cronjé *Cyberlaw@SA II: The Internet and the Law in South Africa* (2004) Van Schaik Publishers

Reinhardt Buys *Cyberlaw@SA: The Internet and the Law in South Africa* (2nd ed) (2000) Van Schaik Publishers

Rajkumar Buyya, James Broberg and Andrzej Goscinki *Cloud Computing Principles and Paradigms* (2010) Wiley Publishers

Cavusgil, S.T., Knight, G and Riesenberger, T.R *International Business: The New Realities* (2012) New Jersey: Pearson Education

Johan De Waal, lain Currie and Gerhard Erasmus *The Bill of Rights Handbook* (4th Edition) (2001) Cape Town, Juta & Co Ltd

Bernard Marr *Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results* (2016) Wiley Publishers

Neethling, J; M Potgieter, J M and Visser P J *Neethling's Law of Personality* (2005) Durban, Butterworths

Papadopoulos, Sylvia & Snail, Sizwe (eds) *Cyberlaw@SA III: The law of the internet in South Africa* (2012) Van Schaik Publishers, Pretoria

Roos A, D. van der Merwe (eds) *Data privacy law, in Information Communications Technology Law* (2016) LexisNexis, Johannesburg. p. 363-487

Roos, A Data Protection in Van der Merwe, D; Roos, A; Pistorius, T; and Eiselen, S *Information & Communication Technology Law* (2008) Durban, LexisNexis Chapter 9

Van der Merwe, D *Information & Communication Technology Law* (2008) Durban, LexisNexis

Waldo, James, Lin Herber and Millett Lynette *Engaging Privacy and Information Technology in a Digital Age* (2007) Washington, DC: The National Academies Press

JOURNAL ARTICLES

Brian A Browne, ‘Self-driving Cars: On the Road To A New Regulatory Era’ (2017) 8 *Journal of Law, Technology and the Internet*

Jonathan Burchell 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid’ (2009) 3 *Electronic Journal of Comparative Law*

Lee Bygrave 'Privacy and Data Protection in an International Perspective' (2010) 56 *Scandinavian Studies in Law* 165

Campbell F ‘An analysis of the emerging role of social media in human trafficking: Examples from labour and human organ trading’ (2016) 15 *International Journal of Development Issues* 98-112

Cassim F ‘Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players’ (2011) 15 *Comparative and International Law Journal of Southern Africa* 123-138

Cassim F ‘Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study’ (2009) 12 *Potchefstroom Electronic Journal* 36-79

Cassim F ‘Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?’ (2015) 18 *Potchefstroom Electronic Journal* 93

Cavoukian, A., & Jonas, J ‘Privacy by Design in the Age of Big Data’ 2012 *Information and Privacy Commissioner of Ontario, Canada*

Cukier. K & Mayer-Schonberger.V ‘The rise of Big Data: How it’s changing the way we think about the world’ (2013) 92 *Foreign Affairs* 28-40

Antoon De Baets ‘A historian’s view on the right to be forgotten (2016) 30 *International Review of Law, Computers & Technology* 57-66

Dhillon, G., and Backhouse, J ‘Information system security management in the new millennium’ (2000) 43 *Communications of the ACM* 125-128

Nicola Fabiano ‘Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation’ (2017) 3 *Athens Journal of Law* 201-214

Muhammad Iqbal, Oladiran Olaleye & Magdy Bayoumi ‘Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches’ (2016) 16 *Global Journal of Computer Science and Technology: E Network, Web & Security*

Shandre Jansen van Rensburg and Johan Prinsloo ‘The Criminogenic Significance of Social Engineering and the Need for Information Security’ 2015 *Southern African Journal of Criminology* at 47

Leloglu E ‘A Review of Security Concerns in Internet of Things’ (2017) 5 *Journal of Computer and Communications* 121-136

Carsten Maple ‘Security and privacy in the internet of things’ (2017) 2 *Journal of Cyber Policy* 155-184

Marié Mcgregor ‘The Right To Privacy In The Workplace: General Case Law And Guidelines For Using The Internet And E-Mail’ 2004 *SAMLJ* 16

Sophia Moganedi and Jabu Mtsweni ‘Beyond the Convenience of the Internet of Things: Security and Privacy Concerns’ 2017 *Council for Scientific and Industrial Research*

Melody Musoni ‘Is cyber search and seizure under the cybercrimes and cybersecurity bill consistent with the protection of personal information act’ 2016 *Obiter* 683–694

Naude and Papadopoulos ‘Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (2)’ (2016) 79 *THRHR* 213–230

Papadopoulos, S ‘Are we about to cure the scourge of spam? A commentary on current and proposed South African legislative intervention’ 2012 *THRHR* 75

Pistorius, T ‘Monitoring, Interception and Big Boss in The Workplace: Is The Devil In The Details?’ (2009) 12 *Potchefstroom Electronic Law Journal*

Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S 'Privacy and The Internet of Things, Lexis Nexis: Watching Me, Watching You: Surveillance, Privacy and The Media (2016) 21 *Media and Arts Law Review* 336-351

Roos, A 'Data Protection: explaining the international backdrop and evaluating the current South African position' 2007 *SALJ* 402

Suryateja, P 'Threats and Vulnerabilities of Cloud Computing: A Review' (2008) 6 *International Journal of Computer Sciences and Engineering*

Ewan Sutherland 'Governance of cybersecurity- the case of South Africa' (2017) 20 *The African Journal of Information and Communication* 83-112

Weber, R.H 'Internet of Things – New Security and privacy challenges' (2010) 26 *Computer Law & Security Review* 23-30

INTERNET SOURCES

Ahmed Banafa 'The Internet of Everything (IoE)' (2016) OpenMind, available at *https://www.bbvaopenmind.com/en/the-internet-of-everything-ioe/,* accessed on 10 March 2018

Alison Job 'IoT and Cyber security' (2017) IT Web, available at *http://v2.itweb.co.za/event/itweb/security-summit-ct2018/?page=news&itwid=166589,* accessed on 10 March 2018

Bhaskara Sannapureddy 'Pros & Cons of Internet of Things (IoT)' (2015) LinkedIn, available at *https://www.linkedin.com/pulse/pros-cons-internet-things-iot-bhaskara-reddy-sannapureddy,* accessed on 2 July 2017

Collin Thompson, 'The difference between a Private, Public & consortium Blockchain' available at *http://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html,* accessed on 1 June 2017

Cybercrime.org.za, 'Malware Definition', available at *http://cybercrime.org.za/malware/,* accessed on 10 March 2018

Coordination and Support Action for Global RFID-Related Activities and Standardization

Dave Evans, 'The Internet of Things How the Next Evolution of the Internet is Changing Everything' (2011) Cisco Internet Business Solutions Group (IBSG), available at *https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf* , accessed on 21 December 2018

Ettiene Retief, 'Look within' (2017) Without Prejudice

European Commission 'IoT Privacy, Data Protection, Information Security', available at *http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753*, accessed on 10 March 2018

Fluidity Software Solutions, 'IoT and Big Data' (2017), available at *http://www.fluidity.solutions/IoT-and-Big-Data.html*, accessed on 10 March 2018

Fu K., Kohno T., Lopresti D., Mynatt E., Nahrstedt K., Patel S., Richardson D., & Zorn B 'Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things' (2017), available at *http://cra.org/ccc/resources/ccc-led-whitepapers/,* accessed on 28 December 2018

George Beall 'How Hackers are using social media to hack' (2017), available at *https://thenextweb.com/contributors/2017/08/23/hackers-using-social-media-hack/,* accessed on 25 March 2018

GPEN Global Privacy Enforcement Network in 2016

Greg McMullen and Florian Glatz 'Blockchain & Law in 2017: Finally friends or still foes?', available at *https://medium.com/ipdb-blog/blockchain-and-law-in-2017-f535cb0e06c4*, accessed on 28 July 2017

Hauman M 'A South African Perspective on User-Created Content in Cloud Computing: A Copyright Conundrum'. (2014). University of Free State Dissertation

Hill K 'How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did' (2012), available at *https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#66b387ef6668*, accessed on 17 July 2017

James Halliday and Rebekah Lam, 'Internet of Things some legal and regulatory implications' (2016) Baker and Mckenzie, available at *http://www.bakermckenzie.com/en/insight/publications/2016/02/internet-of-things-some-legal-and-regulatory-imp__/*, accessed on 21 July 2017

Jamie Cartwright 'Product liability and the internet of things' (2017) Charles Russel Speechlys, available at *https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/commercial/2017/product-liability-and-the-internet-of-things/*, accessed on 21 July 2017

Kim Re 'Randsomed, Hacked and Attacked? – You'll 'Wannacry' (2017) Without Prejudice

Leila Benaissa 'Legal challenges of the Internet of Things' (2015) Lexology, available at *http://www.lexology.com/library/detail.aspx?g=b5b1aba8-fefd-4fc5-8837-12647312377a*, accessed on 21 July 2017

Mark Schroder 'To Catch a Cyber Thief' (2017). Without Prejudice

Nebula 'The Internet of Things Vs the Internet of Everything – Why you need both' (2016), available at *https://www.nebula.co.za/2016/11/24/internet-things-vs-internet-everything-need/*, accessed on 10 March 2018

Nedbank, Phishing, Smishing and Vishing, available at *https://www.nedbank.co.za/content/nedbank/desktop/gt/en/aboutus/legal/fraud-awareness/phishing.html*, accessed on 25 March 2018

Norton Security Centre 'Malware', available at *https://za.norton.com/internetsecurity-malware.html?inid=nortoncom_nav_internetsecurity-malware_homepage:homepage*, accessed on 10 March 2018

Partly Report SA 'Cybercrime and cybersecurity bill invokes suspicion', available at *http://parlyreportsa.co.za/communications/cybercrime-cybersecurity-bill-invokes-suspicion/*, accessed on 24 July 2017

Raul Rubio and Jaime Santisteban 'Cybersecurity, A new priority for Top Management' (2017), available at *http://www.lexology.com/library/detail.aspx?g=ffc8732c-d13d-410d-866a-6fbf540a75e9*, accessed on 21 July 2017

Richard Kam ‘Connected cars: security and privacy risks on wheels’ IAPP, available at *https://iapp.org/news/a/connected-cars-security-and-privacy-risks-on-wheels/*, accessed on 23 March 2018

Richard Kemp ‘Legal Aspects of the Internet of Things’ (2017) Kemp IT Law, available at *http://www.kempitlaw.com/wp-content/uploads/2017/06/Legal-Aspects-of-the-Internet-of-Things-KITL-20170610.pdf*, accessed on 21 July 2017

South African Law Reform Commission (2005) Discussion Paper 109 (Project 124) Privacy and Data Protection

Steve Hanson ‘How Big Data is Empowering AI and Machine Learning’ (2017), available at *https://hackernoon.com/how-big-data-is-empowering-ai-and-machine-learning-4e93a1004c8f*, accessed on 10 March 2018

Suzanne Franco ‘IoT Survey’ (2018) *ICTInsight,* available at *http://books.itweb.co.za/ICTInsight/ICTInsight38_2018.pdf, a*ccessed on 1 February 2018

Tech Law Blog ‘The Internet of Things: Legal challenges in an ultra-connected World’ (2016) Mason, Hayes & Curran, available at *https://www.mhc.ie/latest/blog/the-internet-of-things-legal-challenges-in-an-ultra-connected-world*, accessed on 21 July 2017

‘TechTerms’ available at *https://techterms.com/definition/digital_footprint*, accessed on 10 March 2018

Tomáš Saloky and Jaroslav Šeminský ‘Artificial Intelligence and Machine Learning’. Department of Automation and Control, faculty of Mechanical Engineering, Technical University of Košice, Slovak Republic, available at *http://conf.uni-obuda.hu/SAMI2005/SALOKY.pdf,* accessed on 10 March 2018