UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

TO IOT OR NOT TO IOT: A CRITICAL ANALYSIS OF THE KEY LEGAL CONSIDERATIONS APPLICABLE TO INTERNET OF THINGS IMPLEMENTATIONS IN THE MINING INDUSTRY

By

CATHARINA HELENA (CARINA) WESSELS

96079976

submitted in partial fulfillment of the requirements for the degree

MAGISTER LEGUM (LLM) EXTRACTIVE INDUSTRY LAW IN AFRICA

prepared under the supervision of

Adv. Leonardus J. Gerber

Department of Public Law

Faculty of Law

University of Pretoria

December 2016

I declare that the dissertation, which I hereby submit for the degree Magister Legum (LLM) Extractive Industry Law in Africa at the University of Pretoria, is my own work and has not previously been submitted by me for a degree at this or any other tertiary institution.

The author, whose name appears on the title page of this dissertation, has obtained, for the research described in this work, the applicable research ethics approval.

The author declares that she has observed the ethical standards required in terms of the University of Pretoria's Code of Ethics for researchers and the Policy guidelines for responsible research.

_____

CH Wessels

30 December 2016

ABSTRACT

The research introduces the fourth industrial revolution philosophically, exploring the application of innovation and automation in broad terms and the Internet of Things (IoT) specifically within the mining industry. It explains the business and societal motivation for such interventions, highlighting some of the key benefits. It further explores the inadvertent risks, some of which have already manifested in mining applications and others which can be inferred from other industrial and social applications.

A critical analysis is conducted of the application of the South African Mine Health and Safety Act and Regulations on such applications in the mining environment, as well as considering key other pieces of South African legislation. A comparative analysis with Australian legislation confirms that Western Australia has recognised the need for regulation and have started regulating, primarily mining automation, at least. Through these analyses it is established that a legislative vacuum exists, despite the general application of many requirements in relation to safety considerations during the utilisation of IoT applications.

The paper concludes by recommending collaboration between the Department of Mineral Resources and the Chamber of Mines to seek ways to lead legislative and regulatory developments in this space in order to enable the sustainability of the South African mining industry. In particular, the research suggests the emphasis should be to legally encourage and permit the implementation of IoT solutions in the mining industry in as many instances as reasonably possible, whilst consecutively addressing the new and emerging risks created through such.

KEY TERMS

Fourth industrial revolution, Internet of Things, Industrial Internet of Things, IoT, IIoT

Mining automation, innovation in mining, modernisation

Mine Health and Safety Act 29 of 1996 and Regulations

Code of Practice for safe mobile autonomous mining in Western Australia

Bespoke IoT legislation

ACRONYMS

CEO: Chief Executive Officer.

Chamber: Chamber of Mines.

Chamber Annual Review: Chamber of Mines 2015 annual review.

Code of Practice: *Code of Practice for safe mobile autonomous mining in Western Australia* issued under the *Mines Safety and Inspection Act 1994.*

DMR: Department of Mineral Resources.

ECTA: Electronic Communications and Transactions Act 25 of 2002.

FTC: United States Federal Trade Commission.

FTC report: *Internet of things Privacy & Security in a Connected World FTC Staff Report FTC (2015).*

IIoT: Industrial Internet of Things.

IT: Information Technology.

IoT: Internet of Things.

MHSA: Mine Health and Safety Act 29 of 2009 and its Regulations.

Minerals Act Regulations: Regulations, published under the Mines and Works Act 27 of 1956, later in force under the Minerals Act 50 of 1991, now in force in terms of the MHSA.

Minister: Minister of Minerals and Energy.

OEM: Original Equipment Manufacturer.

Opinion 8/2014: *Opinion 8/2014 on the Recent Development of the IoT.*

PoPI: Protection of Personal Information Act 4 of 2013.

RFIDs: Radio frequency identification tags.

RPAS: Remotely piloted aircraft systems.

SABS: South African Bureau of Standards.

TMM: Trackless mobile machinery.

WA: Western Australia.

WHS: Workplace Health and Safety.

ACKNOWLEDGEMENTS

Adv. Leonardus J. Gerber for his guidance during the programme and the dissertation specifically.

My very patient and accommodating husband, Sas and daughter, Nicci.

The interviewees that provided extremely useful insights during my research.

Exxaro Resources Limited for allowing me to complete this programme.

Family and friends that willingly and unwillingly reviewed the dissertation.

TABLE OF CONTENTS

ABSTRACT **3**

KEY TERMS **3**

ACRONYMS **4**

ACKNOWLEDGEMENTS **5**

CHAPTER 1 – INTRODUCTION, RESEARCH METHODOLOGY AND RELEVANCE **7**

1.1. BACKGROUND 7
1.2. AIMS AND OBJECTIVES OF THE STUDY 8
1.3. RESEARCH QUESTIONS 9
1.4. RESEARCH METHODOLOGY 10
1.5. RELEVANCE OF THE STUDY 10
1.6. LIMITATIONS 12
1.7. CHAPTER OVERVIEW 12

CHAPTER 2 - UNDERSTANDING IOT AND INNOVATION IN MINING **13**

CHAPTER 3 - SOUTH AFRICAN LEGISLATIVE CONTEXT **18**

CHAPTER 4 - INTERNATIONAL LEGISLATIVE CONTEXT **31**

CHAPTER 5 - THE NEED FOR REGULATION **38**

CHAPTER 6 - RECOMMENDATIONS **46**

CHAPTER 7 – CONCLUSION **52**

BIBLIOGRAPHY **53**

CHAPTER 1 – INTRODUCTION, RESEARCH METHODOLOGY AND RELEVANCE

1.1. Background

Participants that attended the 2016 Cape Town Mining Indaba will undoubtedly confirm that innovation featured in many, if not most of the discussions. Mark Cutifani, Chief Executive Officer of Anglo American plc, in his address specifically highlighted, *inter alia*, the extent of challenges the industry was facing and the rate of global change that will require companies to, *inter alia*, be much more innovative technologically.[1]

Some mining companies however realised the need to innovate and the associated opportunities much sooner. Rio Tinto embarked on their Mine of the Future™ programme in 2008 (primarily to reduce environmental impacts and improve safety), with the aim to establish them as the global leader in fully integrated automated mining operations.[2]

As part of their programme, Rio Tinto mirrors Cutifani's sentiments, emphasising: "Innovation is the key to solving the increasing challenges posed by geology, legislation, economics and the need to keep our employees safe. We use it to identify, develop and implement smart step-change technologies that significantly improve how we work. Mine of the Future™ is also mastering the delicate relationship between human and machine."[3]

Technological advancement and innovation are however not unique responses by the mining industry to business challenges. At the World Economic Forum annual meeting in 2016, world leaders came together to, *inter alia*, discuss "mastering the fourth industrial revolution". "According to the World Economic Forum, the fourth industrial revolution is defined by disruptive technologies that blur the lines between the physical, digital, and biological."[4]

There are many definitions of what is meant by the fourth industrial revolution and many companies and scholars use it interchangeably with a definition of the Internet of Things (IoT) or the Industrial Internet of Things (IIoT) or innovation and disruptive innovation in the broadest sense. For purposes of this study, the concept or definition of IoT and IoT implementations will be used in the broadest sense,

---

1 Anglo American South African website: Partnerships and innovation are key themes on day one of mining Indaba.
2 Rio Tinto website: Mine of the Future™.
3 *Ibid*.
4 London Business School website.

with the purpose of incorporating digitisation, automation, modernisation, IoT and IIoT as subsets of innovation as a general concept. According to the United Nations International Telecommunications Union IoT is "…a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies…Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, …From a broader perspective, the IoT can be perceived as a vision with technological and societal implications."[5]

Recommendation ITU-T Y.2060 further comments that: "The IoT is expected to greatly integrate leading technologies, such as technologies related to advanced machine-to-machine communication, autonomic networking, data mining and decision-making, …, with technologies for advanced sensing and actuation."[6]

In an interview O'Reilly[7] also commented, when being questioned on the impact of IoT: "This wave of technology has more chance of reimagining whole swathes of the world than anything we've seen before. This is really going to disrupt everything."[8]

It is evident that we are indeed crossing the Rubicon, in respect of mining, other businesses, the world at large…

1.2. Aims and Objectives of the study

As established and discussed throughout the paper, IoT and related innovation initiatives will, in addition to other already more advanced industries, dramatically increase in the mining industry over the next decade. It is therefore critical to ensure that the legislative framework is well understood by mining companies when embarking on such implementations and that the Legislator and Regulators take note of

---

5 *Recommendation ITU-T Y.2060 June 2012* pp. 1.
The International Telecommunication Union (ITU) is the United Nations specialised agency in the field of telecommunications, information and communication technologies (ICTs).

6 *Ibid* pp. 2.

7 Founder of O'Reilly media, who, *inter alia*, coined the terms open source.

8 O'Brien, C. Tim O'Reilly: "Silicon Valley is massively underestimating the impact of IoT" (interview) *venturebeat* (2015).

potential legislative vacuums, as well as compensate for - or address - new risks being created by such initiatives.

The objectives of the research are to determine in what respect IoT and related solutions are governed through current South African legislation. Secondly, to compare South Africa's governance of IoT to Australian legislation and other jurisdictions where IoT related legislation are emerging. Thirdly, to establish the risks inherent in IoT applications and determine whether such consequential risks necessitate bespoke regulation and legislation. In conclusion, making recommendations for legislative and regulatory change.

Accordingly, the ultimate aims or outcomes of this research are:

- Utilisation of the research by South African mining companies in guiding them from a legislative, regulatory and general risk perspective during any proposed IoT type implementations.
- The Chamber of Mines, or the Legislator and/or Regulators considering the recommendations for changes in, or additional legislation during the development of future legislation, regulation and best practice codes.

1.3. Research questions

1. Does the Mine Health and Safety Act 29 of 2009 and its Regulations (MHSA) contemplate and regulate automated, connected or IoT enabled machinery and the use of unmanned aerial vehicles within a mining area and, with a cursory view only, determining whether there are any other key pieces of South African legislation applicable in this context?
2. How does the above legal framework and compliance requirements, if any, compare with, *inter alia*, Australian law (a well-established mining jurisdiction and where Rio Tinto operates its Mine of the Future™) and are there any other global examples of bespoke IoT related legislation?
3. What are the inherent risks in mining IoT type implementations or inferred risks for the industry, considering risks and incidents in other industries?
4. On critical analysis of the above, is there a legislative vacuum to be addressed in relation to IoT within the mining industry and how should it be addressed?

1.4. Research methodology

The research methodology employed was of a qualitative[9] nature, utilising:

- A literature review.
- Unstructured interviews with two large listed South African mining companies having either already implemented autonomous equipment in certain areas (and planning for future interventions) and/or having embarked on IoT enabled pilot projects in order to establish a clear general IoT implementation plan.
- An unstructured interview with the EY Global Mining & Metals Digital Leader, Australia.
- An unstructured interview with the Rio Tinto Director: Innovation Partnerships, Australia.
- An unstructured interview with the EY Global IoT and Operational Technology Leader, Poland.

Informed by both the literature review and interviews, the research entailed:

- A critical analysis of the legal framework applicable to IoT type implementations within the mining industry in South Africa, with specific reference to the MHSA.
- A comparative analysis with Australian mine health and safety legislation and regulations.
- A critical analysis of other legislation or case law that may be applicable to IoT implementations and which may have application in the mining industry.
- An analysis of the potential key risks flowing from IoT type implementations.

1.5. Relevance of the study

As discussed in greater detail in Chapter 2, the relevance of innovation, automation or modernisation in general and IoT specifically in addressing fundamental concerns within the mining industry, is undeniable

[9] Bryman and Bell "Business research methods" second edition *Oxford University Press* (2007) pp. 28 defines qualitative research as "… a research strategy that usually emphasises words rather than quantification in the collection and analysis of data and that: [*inter alia*] predominantly emphasises an inductive approach to the relationship between theory and research, in which the emphasis is placed on the generation of theories;…".

and is predicted to dramatically increase in the short to medium term. The Chamber of Mines in their 2015 annual review (Chamber Annual Review) specifically emphasised the need for modernisation: "Ultimately, without a shift in our approach to mining methodology, we will fail to mine South Africa's deep-level complex ore bodies profitably, which could see huge job losses. Recent research has suggested 200,000 job losses by 2030, which could affect two million people indirectly."[10] The significant positive impact on sustainability is further emphasised, *inter alia*, that at current assumptions it can extend mines' lives from 2024 (when conventional mining methods will no longer be economically viable) to 2035 and even 2040. They highlight that modernisation will be achieved through technological innovation and mechanisation, but also emphasise that a holistic approach to such should be employed.

In addition to the business imperative, as mentioned previously, the safety benefits of IoT solutions are undeniable, discussed in greater detail in Chapter 2, but to highlight some as reflected in the Chamber Annual Review: "The three top performing platinum mines in the 2015 MineSAFE Awards are mechanised mines. The first prize was won by a mechanised gold mine. All four of the top four safe collieries are mechanised. ... The diamond mines had similar safety performances."[11] The mechanisation discussed in this context can also be regarded to be at an infancy level when compared to the ultimate potential of IoT, but already indicative of the undeniable safety related benefits achieved through such interventions.

The Chamber resultantly spent significant effort in this area, *inter alia*, appointing a dedicated executive and in preparation for the mining Phakisa held in 2015 they developed a strategic framework for tackling the modernisation imperative, centred on the following key enablers: research and development, mining manufacturing and sustainability issues. The Chamber Annual Review section on the topic concludes by expressing its continued commitment towards this end: "It is the Chamber's view that the positive outcomes of modernisation will outweigh the challenges that will inevitably be encountered along the way. However, South Africa can ill-afford to delay these efforts if its mining sector is to remain globally competitive and achieve zero harm. The Chamber will continue to collaborate with all stakeholders to accelerate this journey."

The importance of innovation and modernisation (and by inference ultimately IoT enabled solutions) for the South African mining industry specifically is therefore irrefutable. Resulting from the safety and environmental risks inherent in mining operations, mining is one of the most regulated industries and

10 Integrated annual review 2015 Chamber of Mines of South Africa pp. 56.
11 *Ibid.*

hence, despite the clear safety and other benefits achievable through these measures, it should not occur in a legislative and regulatory vacuum. It is therefore argued that one of the potential "challenges" referred to by the Chamber above, is in fact the inadvertent risks created through these measures that, as discussed throughout this paper, are at present not sufficiently governed by legislation and regulation, but which - it is argued - should so be. It is further held that research like this can greatly assist the Chamber in proactively identifying the possible areas requiring further legislative attention and should be a key input into their future discourse on the subject.

1.6. Limitations

The concept of IoT and a comprehensive understanding thereof, especially from a legislative and regulatory risk perspective, is still in its infancy: *inter alia*, the full understanding of exactly where IoT starts and stops is still being defined and applicable examples of how legislation has adapted to this innovative environment, are therefore limited. In addition, very limited relevant academic papers or case law have as yet emerged.

A material limitation of this study is therefore the fact that it was potentially undertaken at too early a stage and hence the full scope of potential risk or areas that should likely be regulated not completely defined, as well as the ability to deliberate within an established academic legal realm equally limited. It is however held that, despite these limitations, the research establishes a solid practical basis, with sufficient definitive recommendations, so as not to affect its validity and the possibility to expand thereon in future research, which is also recommended in Chapter 6.

1.7. Chapter overview

Chapter 2 establishes what is meant by IoT specifically in a mining context, in order to enable the critical analysis of applicable South African legislation in Chapter 3 (research question one) and Australian legislation in Chapter 4 (research question two). Chapter 5 addresses research question three on the need for more bespoke IoT related regulation, whilst Chapter 6 answers research question four regarding proposed recommendations prior to the conclusion in Chapter 7.

CHAPTER 2 - UNDERSTANDING IOT AND INNOVATION IN MINING

In order to determine whether the current governance of IoT within the mining industry is indeed sufficient and underline exactly what such governance occasions, a solid understanding of IoT within the industry, as well as the potential resultant benefits (which may influence utilisation and the speed of adoption) are necessary.

Research conducted by McKinsey estimates that IoT implementations in worksites (which includes oil and gas, exploration and production and mining) can yield economic value of USD160 billion to USD930 billion per year by 2025.[12] During the MINExpo INTERNATIONAL® 2016, McKinsey further emphasised that in order to, *inter alia*, address the mining productivity challenge the "… Mine of the future takes advantage of data, digital and innovative technologies… [and that] Capturing the benefits of the "4th industrial revolution" requires a shift in operating models."[13] They highlight that, in the past, mining was not necessarily at the forefront of digital developments (also referenced in the Chamber Annual Review in explaining the rationale and need for immediate action by the industry at present), but in their view four major developments will accelerate change in the industry, namely:

- "Data, computational power and connectivity: 90 per cent of the world's data today was created in the last two years.
- Analytics and intelligence: There are ten to the power of 15 more computer operations per second than in the 1960s.
- Process digitisation: There are 250k times more RAM in an iPhone 5 than in the Apollo 11 computer which took it to the moon and back.
- Robotics and automation: There has been a 50 per cent reduction in the cost of robots since 1990, whilst labour costs in, *inter alia*, the United States have increased by 80 per cent."[14]

12 "The Internet of Things: Mapping the value beyond the hype" *McKinsey Global Institute* (2015).
13 "Where do we go from here? The market forces changing mining and the outlook for key commodities" MINExpo INTERNATIONAL® *McKinsey & Company* (2016) pp. 20.
14 *Ibid*, loosely quoted, pp. 23-24.

The above statistics clearly reinforce the contention that we are at a turning point and that those companies, and in fact industries wishing to survive and remain sustainable and relevant into the future, will have no choice but to cross the Rubicon.

McKinsey therefore is of the view that "…the future mine will be redesigned around a fully integrated digital platform."[15]

During their presentation, examples of real value created through mining companies having already embarked on IoT enabled initiatives included:

- "A 23 per cent increase in net present value through stochastic geological modelling at an African gold mine.
- USD250 million saved on mine planning through optimised scheduling and control.
- 10-15 per cent increase in production through automated drilling."[16]

These examples are further mirrored by BMI Research, also emphasising the importance of IoT platforms, processors and autonomous equipment to increase operational efficiency: using Rio Tinto's data to substantiate, *inter alia*, that their autonomous fleet utilisation had exceeded the manned fleet average by 12 per cent over the first half of 2015.[17]

In addition to the pure economic potential of IoT and innovation in general, the further (and often most important initial) rationale for such implementations, as was the case at the outset with the Rio Tinto programme and as also emphasised by the Chamber Annual Review in Chapter 1, is the potential positive impact on safety. Although fatalities in South African mines have reduced tremendously over the past decade, close to 100 employees are still fatality injured each year and hundreds suffer serious injuries. Any innovation or initiative that, even as part of its objectives, can assist in reducing the number of incidents will indeed be a worthwhile consideration. McKinsey's research supports this sentiment by suggesting a 25-75 per cent reduction in total injury frequency rate through utilisation of optimised scheduling and control, predictive maintenance strategies, digitally-enabled maintenance execution and automated equipment.[18]

---

15 *Ibid* pp. 26.
16 *Ibid*, loosely quoted, pp. 29.
17 "IoT: The future of mining" BMI Research (2016).
18 *Supra* 13 pp. 28.

According to a survey of, *inter alia*, 110 mine managers, maintenance and procurement managers across 94 African mines, a significant increase in the implementation of technologies are expected in the medium term.[19] 29 per cent of companies that have not yet invested in technologies are planning to apply capital towards drones, wearable technologies and real-time video training in the next two years.[20]

IoT and digitisation are new and continuously changing areas, not only within mining, but within general business. It provides an enormous opportunity for businesses, but at the same time, because legislation and regulation generally lags innovation and technological progress, tremendous uncertainty and potential risk if not carefully considered and managed.

In understanding the potential scope and application of IoT and digitation in the mining industry, Rio Tinto's Mine of the Future™, as briefly introduced in Chapter 1, is probably one of the most advanced examples of such implementations and, *inter alia*, involves:

- A centrally located operations or control centre controlling all their mines, ports and rail systems.
- Autonomous drilling and haulage of ore.
- Autonomous heavy-haul, long distance railway system (to be implemented).
- Improving the extraction of minerals by optimising conditions in the flotation tanks.
- Real-time data availability (big data sourced from, *inter alia,* equipment) and creation of user-friendly 3D displays from complex data sets.[21]

The two South African mining companies interviewed are employing similar strategies in their innovation roadmaps, in the form of three horizons. Generally the initial horizons are less aggressive, focusing on, *inter alia*, safety improvements (proximity detection, small scale automation) and clear immediate term efficiency improvements, with horizon two touching on increased automation and integration, but only horizon three achieving a true "smart mine" or almost fully autonomous integrated and IoT enabled mining operation as in Rio Tinto's programme. One of the key motivations for the three stage approach is the level of uncertainty regarding the art of the possible at present, as well as the

19 "Investment in drones, wearables to expand across African mines" Engineering News (2016).
20 *Ibid*.
21 *Supra* 2.

limited, and in many cases, no proven implementations of some of the concepts within the South African mining environment.

It is quite clear that complexity, integration and the utilisation of automation and IoT increase within and between the different horizons. It therefore follows that the level of uncertainty and potentially also the risk because of such uncertainty, similarly increase over the horizons, albeit that activities within previous horizons will, over time, assist in better understanding the present unknowns.

Although it is therefore difficult to, at the present stage of maturity, fully comprehend all aspects or areas that may be affected by IoT in the mining industry, a non-exhaustive list of the potential applications is:

- Mineral resource management: Utilisation of drones or unmanned aerial vehicles or remotely piloted aircraft systems (RPAS),[22] automated production planning and monitoring, wall monitoring, automated stockpile management, pit-to-port product tracking.
- Mining automation: Dispatch, autonomous drilling and hauling (either from the actual mining operation or a remote central location where more than one mining operation is controlled, also referred to by some as a thin operating platform), real-time payload monitoring, ground monitoring.
- Plant automation and beneficiation: Automated product blending, automated plant processes, mass flow balance.
- Logistics automation (like Rio Tinto's automated rail system).
- Engineering management: Predictive maintenance with smart ordering, failure analyses, automated water and energy management.
- Health and safety interventions through wearable technologies: Health and exposure tracking, security control through location tracking, automatic equipment response in relation to employees wearing devices.

[22] Defined as an unmanned aircraft which is piloted from a remote pilot station, excluding a model aircraft (non-human carrying aircraft capable of sustained flight in the atmosphere and used exclusively for air display, recreational use, sport or competitions) and a toy aircraft (product falling under the definition of aircraft which is designed or intended for use in play by children).

- Employee training: Augmented reality training based on real-time data from actual working operations.
- Supply chain and warehouse automation: Smart tagging and ordering.
- Sales and marketing: Automated invoicing and accounting based on processed mining product data.

It is clear that the options are almost endless and, although Rio Tinto is an excellent example of what may be expected in this space in the medium term, technological advancements are occurring at such a rapid pace that much more will be possible. As suggested through the Chamber's collaborative efforts, significant vigor will be employed in the short term to truly determine what may be possible so as to enable and sustain the South African mining industry through these types of interventions and applications.

CHAPTER 3 - SOUTH AFRICAN LEGISLATIVE CONTEXT

Resulting from some of the inherent industry challenges discussed earlier, many mining companies are desperately grasping at solutions being peddled to them. They are often enticed by consultants and service providers professing that they will remedy all their challenges through innovative technological means and these service providers often do not award the potential pitfalls and constraints equal attention. It is imperative for mining companies to not only be excited by the prospects of innovation and IoT solutions, but to also recognise that in an extremely regulated and inherently unsafe environment, a pragmatic approach is always apposite, no matter how necessary and inevitable the professed interventions may be. Mining companies therefore require a critical analysis of exactly how the MHSA applies to IoT interventions, but equally how their understanding and application of the MHSA might need to transform when implementing non-traditional mining methods, as well as which other key pieces of legislation will have to be observed.

Informed by the identified potential applications in Chapter 2, a critical analysis of the MHSA, including the Regulations incorporated from the Mines and Works Act 27 of 1956[23] follows in order to answer research question one.

On critical analysis of the MHSA it is evident that holistically many of the sections and regulations are germane to IoT type applications and can be interpreted widely enough so as to accommodate these type of implementations, as discussed below. However, the only sections that may be more directly correlated are:

- Requirements relating to “remote controlled” machinery in Regulation 8.10.19, as follows:

  “The employer must take reasonably practicable measures to ensure that remote control devices for trackless mobile machines using a wireless remote control device comply with: …” (Continues to list a number of South African Bureau of Standards (SABS) requirements to be adhered to in various applications). Remote controlled is however defined as the control and operation of a trackless mobile machine by an operator, by means of a wireless remote control device or a remote control device by means of a cable system, where the operator has direct physical sight

[23] Some regulations, published under the Mines and Works Act 27 of 1956, later in force under the Minerals Act 50 of 1991, are now in force in terms of the Mine Health and Safety Act 29 of 1996 (in order to distinguish between these regulations and the regulations incorporated *ab initio*, these are referred to as the Minerals Act Regulations for ease of referencing purposes.

of the trackless mobile machine.[24] The extent of automation envisioned by advanced IoT interventions (*inter alia* like Rio Tinto's central control room or a thin operating platform, many kilometres from actual mining sites) cannot be regarded to fall within the very narrow and simplistic definition of remote controlled, which still requires direct line of sight: hence it cannot be directly inferred that Regulation 8.10.19 will in fact be applicable to remote operations, other than line of sight remote operations (such example will, *inter alia*, be where a remote controlled hydraulic cannon is used in mineral sands mining).

- Minerals Act Regulations definition of "automatic winding plant" which refers to the driving machinery being operated automatically, without a driver in attendance. Minerals Act Regulations 16.9 dealing with the requirement for automatic overwind and automatic overspeed detection devices, as well as automatic halting of winding operations, 16.9.2.2 specifically: "The device or combination of devices contemplated in Regulation 16.9.2.1 (being the device or combination of devices that detect slack rope that must be installed on every winding plant in which the rope is attached to the drum operating in a vertical shaft, excluding a shaft in the course of being sunk) must on detecting a slack rope condition either automatically halt all winding operations in the vertical shaft safely or warn all winding engine drivers operating in such shaft of the slack rope condition."

  The above undoubtedly predates[25] any form of automation, as contemplated in the context of IoT, and usage of the term "automatic" possibly being misleading in the current context. However, theoretically it will apply because of the description of the device not unmistakably excluding application, as is the case with the remote controlled requirements discussed above.

The recent incorporation of the requirement for trackless mobile machinery to be fitted with collision detection or collision avoidance systems is quite possibly the first display of the Minister of Minerals and Energy (Minister) attempting to explicitly incorporate concepts akin to or which may be enabled by IoT solutions into the Regulations, albeit that the effective date for the automatic reaction without human intervention requirement, in some instances not yet having been determined. This is also a very good example of the Minister acknowledging the need for innovative or modernised means to be utilised to specifically address key safety concerns, but not doing so in an *ad hoc* manner or leaving it open for

24 Section 102 of the MHSA.
25 It was incorporated in 1981 and 1998 respectively.

interpretation, but rather being explicit through the inclusion of the following bespoke regulations in the MHSA:

"8.10.1 The employer must take reasonably practicable measures to ensure that pedestrian are prevented from being injured as a result of collisions between trackless mobile machines and pedestrian. At any mine where there is a significant risk of such collisions, such measures must include at least the following:

8.10.1.1 All electrically or battery powered trackless mobile machines, excluding shovels, bucket wheel excavators and overburden drills, must be provided with means to automatically detect the presence of any pedestrian within its vicinity. Upon detecting the presence of a pedestrian, the operator of the trackless mobile machine and the pedestrian must be warned of each other's presence by means of an effective warning. In the event where no action is taken to prevent potential collision, further means must be provided to retard the trackless mobile machine to a safe speed where after the brakes of the trackless mobile machine are automatically applied without human intervention.

8.10.1.2 All underground diesel powered trackless mobile machines must be provided with means:

(a) to automatically detect the presence of any pedestrian within its vicinity. Upon detecting the presence of a pedestrian, the operator of the diesel powered trackless mobile machine and the pedestrian shall be warned of each other's presence by means of an effective warning; and

(b) in the event where no action is taken to prevent potential collision, further means shall be provided to retard the diesel powered trackless mobile machine to a safe speed where after the brakes of the diesel powered trackless mobile machine are automatically applied. The prevent potential collision system on the diesel powered trackless mobile machine must fail to safe without human intervention.

(Commencement date of regulation 8.10.1.2(b) still to be determined)

8.10.2 The employer must take reasonably practicable measures to ensure that persons are prevented from being injured as a result of collisions between diesel powered trackless mobile machines. At any opencast or open pit mine where there is a significant risk of such collisions, such measures must include:

8.10.2.1 Every diesel powered trackless mobile machine must be provided with means to automatically detect the presence of any other diesel powered trackless mobile machine within its vicinity; and

(a) upon detecting the presence of another diesel powered trackless mobile machine, the operators of both diesel powered trackless mobile machines shall be warned of each other's presence by means of an effective warning; and

(b) in the event where no action is taken to prevent potential collision, further means shall be provided to retard the diesel powered trackless mobile machine to a safe speed where after the brakes of the diesel powered trackless mobile machine are automatically applied. The prevent potential collision system on the diesel powered trackless mobile machine must "fail to safe" without human intervention.

(Commencement date of regulation 8.10.2.1(b) still to be determined)

8.10.2.2 The employer must take reasonably practicable measures to ensure that persons are prevented from being injured as a result of collisions between trackless mobile machines and rail bound equipment. At underground operations where there are a significant risk of such collisions, such measures must include warning the operators of the trackless mobile machine and the locomotive of each other's presence by means of an effective warning."

In respect of the general application sections as mentioned above, the most critical of these are analysed below, whilst others are given cursory consideration.

Section 2(1) of the MHSA sets the cornerstone for safe practices and requires the owner of every mine to, as reasonably practicable, ensure it is designed, constructed and equipped to, *inter alia*, provide safe conditions, supported by the necessary equipment to achieve such, as well as that it is operated in such manner that employees can perform their work without endangering their health and safety or that of any other person, throughout the life of the mine and including during decommissioning. Section 5(1) of the MHSA equally requires from every manager to provide a safe working environment. It is clear that where a mine owner or manager considers IoT enabled equipment and processes, these sections will require measures to be taken to evaluate its inherent safety and whether incorporating such equipment and interventions will indeed improve or in fact adversely affect the ability not to endanger oneself.

Section 5(2) of the MHSA essentially extends the above obligation on a manager to non-employees. It also includes the first introduction to the concept of hazards, in that it requires the manager to identify the hazards and risks to which non-employees may be exposed and to ensure any such individuals that may be directly affected by mine activities are not exposed to any health and safety hazards. Along similar lines, Section 7(1)(e) of the MHSA requires the manager to also ensure work is being performed under the supervision of a person trained to understand the associated hazards.

A hazard is defined as a source of or exposure to danger and hence can be in relation to any type of equipment or process,[26] although it is argued that the manner in which the hazard is assessed and managed will likely differ significantly depending on traditional versus IoT enabled mining and processing methods. In fact, in respect of safety specifically, the interviews of both the South African mining companies confirmed their traditionalist safety approach to implementing automation and IoT enabled solutions, utilising the standard mining understanding and perspective of hazards and not necessarily focusing on unique IoT or automation type hazards, *inter alia,* placing too little emphasis on cyber attacks on equipment. They have clearly not necessarily challenged their own views of potential emerging hazards, also correlating with the suggestion that in some instances the focus has been too much on the positive consequences only. It is contended that the traditional training provided to managers and employees does not sufficiently sensitise them to be able to identify and address the inherent, but possibly unapparent IoT related hazards, therefore emphasising the importance of research question four in order to identify and analyse risks that may require more bespoke governance.

Section 7(1)(d) of the MHSA requires a manager to further, as reasonably practicable, reflect on an employee's training and capabilities *apropos* health and safety before assigning any task, once again clearly applicable to any training and capabilities, but again likely not cognisant of the different training and capabilities that may be of relevance, as referenced above, and which needs to be considered in this regard where an employee is assigned a task significantly impacted by IoT (which will be more closely evaluated in considering research questions four and five).

Section 10 of the MHSA, *inter alia*, specifically addresses the need for employee training (in addition to the training on first starting work) in case of significant changes to procedures, mining and ventilation layouts, mining methods, plant or equipment and material, any or all of which are likely to be affected through IoT interventions at some point, as detailed in Chapter 2 and hence requiring compliance in order

[26] *Supra* 24.

to prepare employees for the resultant changed procedures and risks. The training must enable the employee to deal with every risk to his health or safety as identified during the Section 11 of the MHSA hazard identification process, as well as the associated measures to eliminate, control and minimise those, the work and relevant emergency procedures. Once again, it is contended that the interviews highlighted the potential risk wherein companies have, to date, possibly underestimated the change effected through an IoT enabled solution and have not awarded this sufficient attention due to it likely not being interpreted to impact operations materially (as discussed earlier, although some impacts are already suggested to be sufficiently material, materiality will definitely increase over implementation horizons).

Section 21 of the MHSA is critical in the context of especially new and different equipment and systems being introduced in an IoT enabled mining environment. More especially where such service providers may not have been traditional mining industry service providers and again, although not explicit in nature, will naturally apply to IoT enabled equipment and solutions. It requires any person that designs, manufactures, repairs, imports or supplies any article for use at a mine to ensure, as far as reasonably practicable, that such complies with all requirements in the MHSA, that ergonomic principles are considered and implemented throughout the design to installation process, that the article is safe and without risk to health and safety when properly used, as well as that any assemblies or installations by the manner in which its installed, does not result in it becoming unsafe. In terms of Section 21(2) of the MHSA, the duty can be transferred where such individual is merely an intermediary passing it onto or supplying it to a second party, where such second party provides an undertaking to ensure compliance with the requirements as articulated above.

In any piece of legislation, once the duties have been established, the risk of liability on non-observance of such duties is a critical concept to be considered, especially so in the inherently dangerous mining environment and in the context of the broad and encompassing duties discussed earlier. Informed by the likely extent of service providers and the extent of integration between systems and physical equipment, an IoT enabled mining environment converges into an ecosystem, rather than traditional segregated silos: the cross over or clear accountability between traditional legal appointees or departments and service providers or agents become increasingly unclear, resulting in potential higher uncertainty regarding the seat of liability when something goes awry. The MHSA liability sections have

very broad application, determining a negligent act or omission by any person who endangers the health or safety of a person at a mine as an offence.[27]

In accordance with Section 86(2) of the MHSA an owner or manager must be convicted of an offence where the State proves:

- A person's health or safety was endangered or that a person was seriously injured at the mine;
- The working environment was not safe and was not without risk to the health of employees; and
- The danger or injury was due, wholly or partly, to the condition of the working environment.

Masilo and Rautenbach, on the topic of the employer's duty and the likelihood of liability arising in general, specifically comment that: "As far as the question of unlawfulness is concerned, the duties that have been imposed by ss2, 5 and 11, among others, establish onerous duties that require *proactive* measures from the employer. The legal test to determine the existence of negligence on the part of any person is whether a reasonable person would have foreseen the possibility that the conduct would cause harm and would have taken steps to avoid the harm, and whether the person failed to take these steps to avoid the harm."[28] They further continue to discuss the requirement for a reasonable person to have foreseen the harm and reference the example where an employee argues that an incident occurred because of the employer's failure to ensure the environment's safety: "…the employee has to show that an employer was aware of or must have foreseen that an accident might happen in the ordinary common use of the machinery."[29] Firstly, an interesting question may be if IoT enabled use of the machinery will equate to "common use" – the contention being that as soon as such becomes the norm in which the equipment operates, it will be common use, albeit that a pilot or test implementation may not achieve the standard of common use. Secondly, the newly emerging hazards flowing from IoT enabled solutions and some of the manifestations thereof discussed in Chapter 5, leads to the contention that an employer will probably find it difficult to argue that an accident was completely unforeseen and therefore equally difficult to escape potential liability.

In addition to the above sections, the Mine Health and Safety Amendment Act 74 of 2008 introduced Section 86A (although it is yet to be put into operation by proclamation), in terms of which an employer, Chief Executive Officer (CEO), manager, agent or employee will be committing an offence in case of

---

27 Section 86(1) of the MHSA.

28 Masilo, P. and Rautenbach, G. "Commentary on the Mine Health and Safety Act and Regulations" Revision Service 3 Juta (2011) pp. 8.

29 *Ibid*.

contravening or failing to comply with the MHSA's provisions causing death, serious injury or illness. Section 86A(2) of the MHSA establishes joint vicarious liability in respect of the employer where the act or omission is executed within the authority or employment of the wide group named in Section 86A(1) of the MHSA and the employer:

- Colluded with or permitted the performance or permission; or
- Did not take all the reasonable steps to prevent the performance or omission.

In evaluating these sections in relation to an IoT enabled process, a good practical example is: An autonomous truck not responding as intended, driving over a high wall, falling into the open pit on top of an employee standing below wearing a wearable device intended to also warn him of approaching machinery, instantly killing the employee.

The enquiry into the death will have to determine whether any person or potentially multiple people can be held liable in accordance with any of the above sections. Whilst the same determination will be required in respect of such incident in a traditional mining environment, the complexity introduced through IoT in such instances through the insertion of multiple potentially guilty or liable parties (in addition to the employer, owner, manager and CEO) is evident below:

Traditional mining	**IoT enabled mining**
Truck operator	Control room operator managing autonomous fleet or may even be an autonomous control room operation
Maintenance staff or Engineer	Maintenance staff or Engineer
Original equipment manufacturer (OEM)	OEM
	Network service provider (including GPS enabler)
	Pit beacon service provider
	Autonomous system provider (if different from OEM and may be multiple providers)
	Cyber criminal hacking into the machine

In discussing Section 86A of the MHSA Farisani specifically commented that: "By including managers, agents and employees, the umbrella of possible wrongdoers is opened, and thus making it difficult for the mine to escape liability on account of the inability to pinpoint the culprit. Furthermore, the situation where liability is escaped as a result of the inability to identify a particular senior person who is responsible for the death, injury or illness, is also avoided."[30]

The intention of this research is not to extensively debate the aspect of civil or criminal liability in such instances, but the important conclusion to be drawn from the above is that where an incident occurs within an IoT enabled mining environment, the MHSA's general liability provisions will apply (subject to the normal requirement of causation and then, until Section 86A of the MHSA becomes effective, the requirement of negligence), but the potential net of individuals with joint and several liability will clearly be much broader – hence escaping liability merely because an incident was caused by a "non-human", is not an automatic assumption. It is further held that the proposed Section 86A of the MHSA, albeit generally negatively received by the Chamber and mining companies and despite the complexity it brings, as discussed above, will be an improvement in the context of IoT enabled mining operations in especially emphasising the accountability by "agents" considering the increased impact that, *inter alia*, Information Technology (IT) related system agents may have in causing incidents in an IoT enabled environment. These agents may be unaccustomed to operating within the risky mining industry, more akin to an entrepreneurial and risk prone research and development type environment and therefore, reinforcing the criticality of their duties through onerous liability measures, potentially appropriate.

Some of the more critical Regulations (not an exhaustive list) that can be read to holistically apply in an IoT context are:

- Chapter 8 of the MHSA General Regulations: machinery and equipment and most especially, for example:
  - Regulation 8.2 regarding the braking system requirements for underground rail bound transport and the brake tests to be performed, which naturally will have to be observed when such equipment is controlled through IoT enabled solutions.
  - Regulation 8.8(2) requiring the employer to take reasonably practicable measures to prevent injuries due to machine failure because of incorrect design, incorrect installation,

[30] Farisani, D.M. "Corporate criminal liability for deaths, injuries and illnesses: Is South Africa's mining sector ready for change" Speculum Juris (2012) pp. 51.

poor maintenance or incorrect use or non-compliance with proper operating or safety procedures.

- Regulation 8.8(3) requiring very specific measures to prevent injury, *inter alia*, in instances where moving machinery may pose significant risk to any person, such being moved only under constant supervision of a competent person, fully aware of the risks. In an IoT context a key aspect to be considered in this case and all others where reference is made to the performance of a function by a competent person, is in fact who this competent person may be in future. Also whether such individual can indeed be regarded as fully aware of the risks if, *inter alia*, they do not have a solid understanding of potential IT influenced risks as well. It also poses the question of whether oversight by a competent person, *inter alia*, remotely, will equate to compliance where the actual physical task required of such competent person may in fact be performed by a piece of equipment or system. It is contended that in the current context, the Regulations are too restrictive to indeed allow for such, although some more aggressive (or progressive) mining companies may indeed use the non-explicit exclusion as a legislative ambiguity to in fact introduce such solutions. It also requires appropriate pre-start warning devices where equipment might unexpectedly move, a specific risk also discussed in Chapter 5 as a possibility in respect of IoT enabled equipment, which it is argued will be applicable in all respects, irrespective of how such may be conducted in an IoT enabled environment.
- Regulation 8.10(3)-(17), in this case it is useful to note that many of the risks these Regulations aim to mitigate, will likely be automatically mitigated or prevented in the case of automation and IoT enabled solutions, *inter alia*, measures to deal with driver fatigue (although a control room operator controlling a fleet of autonomous trucks may also be fatigued and therefore reinforcing the continued need for regulation, albeit in a different form, as discussed in Chapter 6).

- Regulation 23.4(l) of the MHSA requires reporting to the DMR of any self-propelled mobile machine which may pose a risk to persons running out of control, which as discussed in Chapter 5, is indeed also a possibility in respect of IoT enabled equipment.

From the above it is evident that no bespoke sections or regulations have been included in the MHSA to explicitly deal with the concept of automation or IoT, whilst only limited regulations are considered wide enough to encompass more specific reference to such (albeit that they were undoubtedly not

drafted with IoT precisely in mind). Many sections and regulations are however holistic enough to require compliance, despite the activities being performed through non-traditional mining methods, however quite a number of areas do exist where it can be argued that the wording may, by inference, exclude more innovative mining methods and hence pose the risk of mining companies proceeding on the basis that such requirements are not to be adhered to in employing more modernised mining methods. Further, as detailed in Chapter 5, certain of the inherent IoT type hazards do potentially require customised inclusion and it is therefore already held that a MHSA legislative vacuum indeed exists, however research question five is only fully answered in Chapter 5.

Although not modified for the mining industry per se, the general utilisation of RPAS is governed by Part 101 of the South African Civil Aviation Regulations which came into force on 1 July 2015 and established South Africa as one of the first countries to promulgate legislation on the subject. It, *inter alia*, governs commercial and corporate operations and therefore applies whether mining companies insource or outsource this service. Some of the key requirements include:

- A certificate of registration and letter of approval is required for each RPA.[31]
- Documentation to substantiate that the RPAS is capable of being operated safely for the work deployed.
- Continual maintenance by an acceptable person.[32]
- Pilots must be in possession of a valid remote pilot's licence[33] (airplane, helicopter or multi-rotor), as well as, in respect of commercial operations, a valid RPAS operating certificate and an air services licence issued in accordance with the Air Services Licensing Act 115 of 1990.
- Employing specific security measures, including background and criminal record checks on employees, protecting the RPAS from external interference.

Therefore, where utilisation of drones form part of the modernisation or IoT strategy, compliance with the above requirements are necessary. The interviews however confirmed that the companies utilising outsourced service providers may be placing too much emphasis on blindly trusting the compliance by service providers and not taking accountability of ensuring such themselves, whereas some

31 CAR Part 101, sub-part 2 and *Ibid*, sub-part 4.
32 *Ibid*, sub-part 6.
33 *Ibid*, sub-part 3.

mining companies have in fact established their own drone departments and in such instances will likely be more conscious of the requirements.

In relation to data and information systems in general, aspects of the Electronic Communications and Transactions Act 25 of 2002 (ECTA) will be applicable in the context of IoT implementations: information systems are defined as "a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet", whilst data is defined as "electronic representations of information in any form" and hence includes systems utilised in autonomous and IoT enabled applications. In the context of the risks discussed in Chapter 5, the most important sections of the ECTA in this context are probably those dealing with cyber crime or the unauthorised access of data. It establishes that a person who intentionally accesses or intercepts data without permission or authority, is guilty of an offence, including anybody aiding or abetting such individual.[34] It, however, does not place specific obligations on a company to *inter alia* take reasonable steps to protect their operations against cyber crime and also does not deal with IoT in any bespoke manner.

Legislation that will however place obligations on a company, in respect of specifically wearables, is the Protection of Personal Information Act 4 of 2013 (PoPI). The commencement date of PoPI has not yet been determined, but once it becomes effective, companies that utilise wearables will have to ensure compliance with the data collection and processing requirements, as the data collected by wearables will undoubtedly fall into the category of personal information, which, *inter alia*, includes information on age, physical or mental health, well-being and disability.

In brief, PoPI requires compliance with eight conditions in order for data processing to be regarded as legitimate, namely:

- The processing party must ensure adherence with PoPI.
- The processing limitations must be observed, *inter alia*, processing must be lawful and not infringe privacy: adequate, relevant and not excessive, given the purpose.
- Data must be collected for a specific purpose and individuals must be made aware of such. Data must also not be kept for longer than required for the intended purpose.
- Any further processing must be compatible with the purpose of collection.

[34] Sections 86-88 of the ECTA.

- The processing party must take reasonable steps to ensure the personal information is complete, accurate, not misleading and updated when necessary.
- Steps must be taken to ensure the data subject is aware of the collection.
- Information must be secured and the data subject advised in case of a breach.
- The data subject can request whether a company holds their private information and what is held and may also request the correction or deletion of information.

Once again, neither the ECTA, nor PoPI deals with IoT in a bespoke manner and, resulting from many of the inadvertent risks created through IoT applications, *inter alia*, hacking of systems as discussed in Chapter 5 relating to these pieces of legislation, more explicit inclusion of IoT rules or regulations is appropriate.

CHAPTER 4 - INTERNATIONAL LEGISLATIVE CONTEXT

In order to confirm whether a legislative vacuum indeed exists and to gauge legislative developments in more developed countries, a comparative legal analysis was performed. Informed by the inference that Australia is one of the most mature mining environments in respect of mining automation, the international analysis of this research focused on this jurisdiction. In Australia the exploration and extraction of minerals are governed in accordance with the respective State or Territory's legislation. Similarly, the States and Territories have workplace health and safety (WHS) legislation that generally applies in the jurisdiction, with some exceptions, and hence the Australian Government does not regulate WHS in the mining industry.[35] Harmonised WHS legislation was introduced on 1 January 2012 and although it was intended for the model Mines Regulations to be included in the model WHS Regulations at the time, such was not achieved due to a lack of Ministerial support. The draft model Mines Regulations were however sent to the various jurisdictions in September 2014 to consider such for implementation.

Due to the Federal system of government, the legislative framework is clearly more complex than that of South Africa, a summary (only of those jurisdictions with bespoke extractive industry safety legislation) is included below:

Jurisdiction	**Bespoke safety legislative framework[36]**
New South Wales	*Work Health and Safety (Mines and Petroleum Sites) Act 2013* *Health and Safety (Mines and Petroleum Sites) Regulation 2014*
Northern Territory	*Chapter 10 of the Mines Work Health and Safety (National Uniform Legislation) Regulations*
Queensland	*Mining and Quarrying Safety and Health Act 1999* *Mining and Quarrying Safety and Health Regulation 2001* *Coal Mining Safety and Health Act 1999* *Coal Mining Safety and Health Regulation 2001*

[35] "The international Comparative Legal Guide to: Mining Law" *Global Legal Group* (2014) pp. 42-47.
[36] Safe Work Australia website.

Tasmania	*Mines Work Health and Safety (Supplementary Requirements) Act 2012* *Mines Work Health and Safety (Supplementary Requirements) Regulations 2012*
Western Australia (WA)	*Mines Safety and Inspection Act 1994* *Mines Safety and Inspection Regulations 1995*

The above legislation also generally, *inter alia*, requires owners and managers to take steps to protect health and safety, imposes obligations on those who design, manufacture, import and supply plant substances or structures and to implement a safe system of work, which includes proper risk management processes. Similar to South Africa, no bespoke legislative rules exist to govern automated processes or IoT applications. Contrary to South Africa (which was a leader in this regard as discussed in Chapter 3), Australia does not regulate RPAS at present.

However, in recognition of the developments in automation specifically and likely because of their more mature state, a *Code of Practice*[37] *for safe mobile autonomous mining in Western Australia* was issued in 2015 by Resources Safety under the *Mines Safety and Inspection Act 1994 (Code of Practice)*, with the endorsement of the Mining Industry Advisory Committee and approval from the Government of WA Minister for Mines and Petroleum.

The *Code of Practice* specifically provides guidance on mobile autonomous and semi-autonomous systems and developing and evaluating safe work procedures for such. It focuses on the control of such equipment and the identification of the unique risk profiles in relation to new or existing mobile autonomous mining systems. It does not apply to underground coal mines, nor remote operations centres, unmanned aerial vehicles, remote controlled systems, although parts may be relevant to mobile tele-remote systems if they incorporate additional functionality that takes autonomous control of machines, autonomous functionality of a process or machine that moves on fixed infrastructure such as rail and a fixed base like laboratory robots.

[37] A practical guide to achieving the standards required under legislation. Codes of practice are admissible in court proceedings in Australia: Courts may regard such as evidence of what is known about a hazard, risk or control and may rely on such.

The *Code of Practice* establishes the following requirements and controls:

- Adapting mine planning and design protocols and processes to specifically provide for hazard control.
- System builders and users must identify, assess and control the hazards associated with autonomous operations (thereby recognising the unique hazards applicable in such instances, as discussed in Chapter 3). Safety functions and the required performance levels against such should be informed by the hazard identification and risk assessment process, including:
  - Clearly defining the roles and responsibilities of system operators and builders (again, emphasising the role played by "agents" as also discussed in Chapter 3).
  - Designing and configuring systems with appropriate access control restrictions and layers of protection.
  - Designing a fail-to-safe state.
  - Implementing periodic reviews and audit processes.
  - Ensuring proper records management and system change logs.
  - Implementing appropriate system security.
- Commissioning activities for autonomous equipment should adequately address:
  - The roles and responsibilities of system operators and builders, *inter alia*, agreeing, defining and documenting boundaries (touching on the overlaps and potentially unclear boundaries within the ecosystem discussed in Chapter 3).
  - Proper risk management processes, commissioning planning and testing, as well as functional and user acceptance testing and formal approval processes and systems acceptance.
- The design and function of operational practices should adequately address:
  - Management, supervision and roles and responsibilities.
  - Technical and systems knowledge within operating teams, including competency validation (emphasising the need to have IT knowledge in positions previously likely not requiring such, as highlighted in Chapter 3).
  - Change management, including changes to standard operating procedures and training materials and processes prior to implementing such changes (an aspect highlighted in Chapter 3).

  - Interaction rules: how changes between traditional and autonomous operations, including traffic management are controlled, documented and communicated.
  - Planning for and managing human factors.
  - Area security and control, tools and processes (like, *inter alia*, emergency response) and technical support.
- Maintenance activities should, *inter alia*, adequately address recovery procedures in autonomous areas, effective condition monitoring, diagnostics and error reporting analysis to indicate system behavior, calibration and testing.

Although the *Code of Practice* undoubtedly provides good guidance as to aspects to be considered and implemented in respect of autonomous operations, it will need further development to holistically address IoT application in the wider sense, but as referenced above already addresses a number of the concerns raised in respect of MHSA lacunas in Chapter 3.

The interviews confirmed the outcomes of the above literature review, in that:

- IoT type implementations, including autonomous operations (other than through the above *Code of Practice*), as well as the utilisation of drones are principally unregulated in Australia.

- Regulation and legislation globally have not kept pace with the rate of innovation and technological development and to date there are not many, if any, legislation enacted or regulations developed to address IoT type implementations specifically.

The conclusion therefore that no bespoke mining IoT related legislation has been enacted and, in fact, none was found. However, limited other pieces of legislation can be read to have bearing on some of the intended usages in mining, for example, the *Italian Jobs Act*[38] in respect of wearables. Coraggio of DLA Piper discusses the *Italian Jobs Act*, which specifically governs the usage of IoT devices in respect of employees. It, *inter alia*, prohibits devices with the sole purpose to monitor employees, whilst some used for security purposes or the protection of company assets may be used with the prior approval of trade unions and devices used for working activity or for the recording of accesses/presence at the workplace do not require union consent, only the provision of a privacy information notice to employees.[39]

[38] An English version of this piece of legislation was unavailable in order to accurately reference such.
[39] Coraggio, G. "The Internet of Things after the Jobs Act" *DLA Piper* (2016).

To be expected, resulting from the industries that early adopted IoT solutions, the first regulatory focus areas have been the technological aspects of IoT, *inter alia*, roaming, spectrum allocation policy, net neutrality of the internet: many of these also not yet formally regulated, as well as data protection and data security regulation (also not bespoke IoT). A brief overview of key international developments in this regard are detailed below.

As per the United States Federal Trade Commission (FTC)[40] report recommendations discussed in greater detail in Chapter 5, the United States and the European Union have mainly focused on IoT providers to incorporate standard data protection requirements and best practices into their development, rather than developing bespoke data protection legislation for IoT. Although Clubb, Lirch and Patwa[41] highlight a number of pieces of general United States legislation that are applicable in respect of the collection of data, none of these specifically contemplate data collection through IoT devices and therefore do not include any bespoke requirements.

The working party on the protection of individuals with regard to the processing of personal data issued *Opinion 8/2014 on the Recent Development of the IoT*, adopted in September 2014 (*Opinion 8/2004*).[42] It focuses on the main data protection risks in relation to IoT and how the European legal framework should be applied to such. *Opinion 8/2014* emphasises that "The complex mesh of stakeholders involved asks for or implies the necessity of a precise allocation of legal responsibilities among them with regard to the processing of the individual's personal data, based on the specificities of their respective interventions."[43] This aspect has been discussed from a perspective of mine health and safety above, but clearly requires clarification and attention in other areas as well.

They regard device manufacturers as data controllers in accordance with EU legislation, as well as assign responsibilities to any social media platforms that may aggregate such data. In addition to the guidelines suggesting that service providers within the IoT ecosystem should ensure compliance with standard data protection legislation and guidelines, a number of specific recommendations applicable to

---

40 Federal Trade Commission website: "The Federal Trade Commission works for consumers to prevent fraudulent, deceptive and unfair business practices and to provide information to help spot, stop and avoid them.".

41 Clubb, K., Kirch, L. and Patwa, N.I. "The Ethics, Privacy and Legal Issues around the Internet of Things" *Berkely School of Information* (2015).

42 "This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC."

43 *Opinion 8/2014 on the Recent Development on the Internet of Things* pp. 11.

all stakeholders were included in, *inter alia*, *Opinion 8/2014*, as well as Deloitte's recommendations[44] on safeguarding the IoT, which include:

- A material focus on data privacy and associated actions, which generally align with what most countries regard as good data protection measures:
  - Performing privacy impact assessments on launching new IoT applications (not an action that is part of PoPI and hence an aspect that should potentially be considered for inclusion in PoPI).
  - Deleting data at the nearest collection stage and observing the principle of self-determination through users being able to control their own data, as well as regular system reminders that data is being collected (similar to that contained in PoPI, although PoPI is not explicit in respect of "the nearest collection stage").
  - As also suggested by the *FTC report*, the principles of privacy by design and privacy by default should be incorporated (PoPI does require this at present).
- Emphasising the importance of different systems from different suppliers being able to integrate, as often the point of integration becomes the area causing interoperability problems and security concerns (which can lead to equipment not operating as intended). This aspect was also specifically highlighted in Chapter 3 due to the likely high number of parties and different systems in the ecosystem and also emphasised as an area requiring focus in the *Code of Practice*.

Opinion 8/2014 continues to provide similar specific detailed recommendations for device manufacturers, application developers, social platforms, IoT device owners, additional recipients and standardisation bodies and data platforms.

The *FTC report* (discussed further in Chapter 5) recommends a number of additional best practices to be implemented by companies providing IoT devices, *inter alia*:

- Ensuring the company's personal practices promote good security through the level of accountability and staff training.

---

[44] Saif, I. Peasley, S. and Perinkolam, A. "Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age" *Deloitte Review Issue 17* (2015).

- Ensure service providers also maintain safety protocols and perform reviews over such to obtain assurance of its reasonableness.
- Systems with heightened risk should include security measures at various levels and increased levels of encryption.
- Implement reasonable access control measures to restrict unlawful access to devices, data or the network.
- Monitor products through its lifecycle to especially address increased vulnerabilities at the end of the lifecycle or on out-of-date devices.
- Observe certain of the fair information practice principles that can be applicable in the IoT context like data minimization.
- The report also suggested "The establishment of legislative or widely-accepted multi-stakeholder use-based frameworks could potentially address some of these concerns and should be considered."[45]

The *Code of Practice* and other recommendations provide good insights to what should be considered for South African application.

[45] "Internet of things Privacy & Security in a Connected World FTC Staff Report" *FTC* (2015) pp. 46.

CHAPTER 5 - THE NEED FOR REGULATION

Previous Chapters have already in a number of respects highlighted possible legislative or regulatory *lacunae*. In this Chapter many of the IoT related inherent risks are discussed in greater detail, as well as a number of authors' views regarding the need for explicit IoT legislation or regulation. It is held that the extent of the risks highlighted and the views that regulation is becoming necessary, affirm the contention that bespoke governance of IoT interventions is appropriate in order to address the perceived risks consequential to IoT type interventions in the mining industry specifically.

The *Code of Practice* emphasises that the addition of autonomous equipment can introduce hazardous situations unlike those anticipated in conventional operations. Even more so in instances where conventional and autonomous operations operate simultaneously, emphasising the need for comprehensive risk assessments, well-articulated business cases that include the hazards and limitations, integrating the thinking around autonomous systems at a planning and design stage already and well-documented change management processes.[46] The following potential risks are, *inter alia*, highlighted: interference with autonomous equipment communication systems, loss of control over autonomous equipment and deviating from the programmed area, interactions with pedestrians and other infrastructure, human errors, inadvertent access or hacking, access into the autonomous area by unauthorised personnel or equipment and natural phenomena.[47] The inability to, in absolute terms, comprehend what IoT is, how far it may extend and to predict exactly what it may look like in the future due to its rapid expansion, underscores the need to evaluate how to address the key risks and uncertainties through legislation and regulation, but without inhibiting innovation and technological development.

Chui, Löffler and Roberts in 2010 already suggested that, *inter alia,* policy should be addressed before IoT is widely embraced: "Industry groups and government regulators should study rules on data privacy and data security, particularly for uses that touch on sensitive consumer information. Legal liability frameworks for the bad decisions of automated systems will have to be established by governments, companies and risk analysts, in consort with insurers."[48]

---

46 *Code of Practice for safe mobile autonomous mining in Western Australia* was issued in 2015 pp. 25.
47 *Ibid* pp. 29.
48 Chui, M., Löffler, M. and Roberts, R. "The Internet of Things" *McKinsey & Company* (2010).

Roberts[49] references attorney and technology expert Kraig Baker who emphasised some of the key concerns and risks consequential to IoT, namely data security, product liability and intellectual property. Roberts further also broadly discusses the increased risk as a result of IoT devices being hacked and specifically the seat of liability in such instances. He references two examples which are very appropriate in the discussion of mining IoT applications. Firstly, that of a New Jersey man shooting down a drone over his property and the fact that some scholars argued it justifiable based on the concept of privacy based self-defence. Secondly, driver-less cars, not unlike autonomous trucks utilised in mining, and the legislative uncertainty as to where liability will rest in case of an accident: for example, with the driver or the vehicle manufacturer, and one he had not even included, possibly even the network service provider in case of network instability or network security lapses (as discussed in the example in Chapter 3).

The article further emphasises the fact that case law has largely been based on a linear view of objects and liability, but "Those principles may not apply very well when everyday objects act on their own, and as part of a globally-connected network." Roberts concludes that "…we're just beginning to recognise the new legal issues related to the internet of things, and are a long way from writing rules for them."[50] As mentioned in Chapter 3, the intention of the paper is not to evaluate where liability will rest, but merely to elucidate the additional complexity created in relation to liability in an IoT enabled environment.

Research has indicated that IoT devices may be more prone to cyber attacks than traditional IT infrastructure: according to Hewlett Packard, 70 per cent of the most commonly used IoT devices contain vulnerabilities.[51] One of the consequences of the integrated nature of IoT solutions is the inability of one company to completely secure against cyber attacks, due to the number of devices, vendors and partners involved.

In this regard, in January 2014 the FTC handed down an order to TRENDnet Incorporated[52] after they were accused of violating the *Federal Trade Commission Act 15* in that they falsely marketed the security of their products and had not implemented sufficient measures to safeguard their products from being illegally accessed, resulting in internet users gaining access to hundreds of consumers' private camera feeds. In summary, the FTC sanction was that TRENDnet:

---

49 Roberts, J. "The internet of things is here, but the rules to run it are not" *Gigaom* (2014).

50 *Ibid.*

51 Hewlett Packard website: HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack.

52 *United States of America before the Federal Trade Commission in the matter of TRENDnet Incorporated, a corporation, Docket No. C-4426*.

- May not misrepresent the security of the cameras, the data transmitted or the level of control a consumer is able to exercise over the camera data.

- Was required to establish a comprehensive information security programme to mitigate the risk of unauthorised access or unauthorised use of information and requiring third-party validation of the security programme every two years for the next 20 years.

- Was required to advise all customers of the security risks and provide them with free technical support for two years to, *inter alia*, install software updates to correct the security deficiencies.

Influenced by this case and other developments, in January 2015 the FTC issued a report on IoT[53], urging companies to adopt best practices to address consumer privacy and security risks specifically. The report focused on consumer devices, rather than business-to-business solutions, but still provides some useful insights into the risks and potential mitigating steps to address such.

Some of the risks identified include:

- Enabling unauthorised access and misuse of personal information. As mentioned earlier in the Chapter, an increase in connected devices may increase the number of vulnerabilities.

- Facilitating attacks on other systems or the network.

- Creating risks to personal safety, *inter alia*, through hacking into and illegally controlling vehicles.

- Privacy risks from the collection of personal information: the shear quantum of data that can be collected and its granularity can enable significantly more advanced data analytics to be performed, possibly also for purposes not disclosed or initially intended.

In specifically addressing legislation in relation to data collected through IoT, the report suggested that IoT specific legislation was not necessary as such may stifle innovation. It rather suggested specific self-regulatory practices per industry.[54] This paper fundamentally differs from this view and suggests that it is a balancing act between legislation, regulation and innovation. It is contended that legislation can in fact enable increased ultilisation of IoT solutions though explicit inclusion and allowance, as suggested in

53 *Supra* 45.
54 *Ibid* pp. 47-52.

Chapter 6 and further that any governance implemented must not stifle the ability to innovate and modernise.

A 2015 article supports the above contention and questions the United States' response to IoT and argues that Washington has also not kept up with the changing times: "Congress has written no laws or any kind of overarching national strategy specifically for the Internet of Things."[55] The article touches on the seemingly fragmented approach employed to address certain IoT related risks and areas, as well as the more reactive approach favoured by many senators, in certain instances because of their deemed uncertainty as to how to legislate these aspects. The focus of discussions on Capitol Hill also seemingly focused on the benefits of IoT only, ignoring or skimming over the potential problems simultaneously created.[56] The second comment indeed having been emphasised in Chapter 2 as a key risk in current mining implementations.

Williams[57] consolidates many of the risks identified in previous articles and also emphasises the lack of legal frameworks to accommodate IoT and its challenges. He specifically expands beyond the data privacy and security risks to elucidate the following concerns:

- Labour legislation considerations in respect of wearable devices and how information collected from these may be used.
- Liability overlap and uncertainty in case of incidents (as discussed in the example in Chapter 3 and elsewhere).
- Uncertainty regarding data ownership.

An example of the *FTC report* risk to personal safety and the liability overlap mentioned in Williams[58], is the 2015 incident where two automotive cybersecurity researchers remotely hacked a Jeep Cherokee and paralysed it on the highway. The impact could have been much worse had they been malicious and not reported the deficiencies to Chrysler in order for it to be addressed.[59]

---

55 Samuelsohn, D. "What Washington really knows about the Internet of Things" *POLITICO* (2015) pp. 4.
56 *Ibid* pp. 10-11.
57 Williams, L. "The Wild West of IoT Legislation" *CMS WiRE* (2016).
58 *Ibid.*
59 Greenberg, A. "The Jeep hackers are back to prove car hacking can get much worse" *Wired Magazine* (2016).

In relation to general vehicle automation, the two recent Tesla deaths can also not be ignored: the first fatal incident occurred in the United States in May 2015, with the second in China in January 2016. The first a confirmed auto pilot death, whilst the cause of the second incident has not been definitively established, although the auto pilot was also suggested.

Whilst an incident in Germany contextualises some of the risk to physical property when cyber attacks cause equipment to respond differently than anticipated or not at all: in this instance it was reported that control systems at an unnamed steel mill was so adversely affected that a blast furnace was unable to be shut down, resulting in material damage.[60]

However, one should also not underestimate things merely running awry (without malicious interference) when so many objects and, especially objects from different suppliers and operating on different platforms, interact. Also in Germany, one of the earlier smart houses stopped responding to the owner's commands. After much investigation, he realised that a burnt out light bulb was continuously attempting to inform the system nucleus that it required attention and through this action overloaded the system, causing a total system freeze. The owner admitted that the light bulb was not supposed to act in this manner, but indeed had, suggesting that systems are not always as predictable as often presumed and hence elucidating the risk in this regard.[61]

According to Baker & McKenzie, the United States Senate passed a resolution in March 2015 calling for a "…national strategy for the IoT to promote economic growth and consumer empowerment". The resolution referred to the US prioritising the development and deployment of the IoT in a way that "…responsibly protects against misuse…"[62], reinforcing the above contention that, some form of governance is becoming necessary and appropriate governance can enable innovation and growth, whilst ensuring protection against risks.

From some of the interviews, it was, *inter alia*, confirmed that although the benefits have been undeniable, a number of risks were emerging as mining companies progressed down the IoT path and started to better comprehend the associated complexities.

---

60 Zetter, K. "A cyberattack has caused confirmed physical damage for the second time ever" *Wired* (2015).
61 Hill, K. "This guy's light bulb performed a DoS attack on his entire smart house" *Fusion* (2015).
62 "Internet of Things some legal and regulatory implications" *Baker & McKenzie* (2016) pp. 8.

In one interviewee's view the main risks requiring attention were:

- Even though the inherently unsafe mining environment has become safer because of automation and a general reduction of human intervention, in his view, safety related risks have in certain respects actually increased when humans interface with autonomous and IoT driven operations.

  The risk avoidance culture, through an increased focus on mechanisation and lesser utilisation of people, has in fact resulted in the remaining humans being less experienced in day-to-day operations and interactions with equipment: thus, although the magnitude of the risk has possibly reduced due to fewer people, the intensity of the risk per individual has potentially increased.

- Date privacy risks and issues were continuously emerging and the highest risks included, *inter alia*, where data resides, where it is legally created and how it is shared.

  Utilisation of remote operation centres (like the Rio Tinto one) further increases the risk of data sovereignty, especially in countries like Australia with varying legislation in different States, as discussed in Chapter 4 (*inter alia* Western Australia does not have data privacy legislation).

- The risk of infringement of intellectual property rights have increased with the borderless nature of IoT solutions, both from a geographical and systems perspective.

- An emerging area of concern was infringement of employee relations or labour conditions and legislation. The prevalence varied from area to area, but primarily related to issues of:

  – Local employment.

  – Retention of staff.

  – Potential infringement of contractual employment terms.

  He specifically emphasised that companies may be too focused on the benefits of automation and IoT (highlighted as a risk throughout the paper), thereby possibly losing sight of labour relations infringements that may be consequentially caused.

  James Goodnow, a partner at the law firm of Lamber Goodnow was quoted by Morgan articulating the risk that, due to the unregulated nature of the collection of specifically health related information by companies, such should be treated with caution, especially where such

data is used to terminate employment: "…The information you've collected may show a disability by tracking heart rate or activity or that someone isn't as healthy as they should be."[63]

- As also highlighted by the literature review, significantly increased cyber security risk: increased risk of malicious attacks, but also materially increased potential negative impacts of such attacks because of the higher number and the importance of equipment that will be exposed to potential hacking.

  The risks associated with cyber attacks and data security was underscored by Wassom as some of the top IoT related risks and he specifically emphasised the general lack of standards in relation to IoT, as well as the speed of innovation and development in this field as material contributing factors to the risk. He also refers to research having articulated the extent of potential exposure, *inter alia*, 70 per cent of IoT devices sending data over unencrypted networks and he questions how many instances of hacking will be necessary before law makers and the public took real notice of the risks.[64] Morgan also refers to research where 73 per cent of participants (IT professionals) expressed a concern regarding the lack of security standards to address IoT risks.[65]

In summary, it is therefore held that the key risks that at present justify some form of bespoke regulation, in relation to the current understanding of what mining IoT implementations may entail are:

- Equipment operating other than as planned or outside of planned parameters, either through equipment malfunction or malicious attacks: especially the risk to human life caused by such incidents.

- Privacy and labour related considerations and risks in relation to specifically wearables.

- General data security and sovereignty.

Having already established that none of these risks are at present addressed in any bespoke manner within the South African landscape, except in the case of RPAS, it is held that consideration should be given to particular recommendations to mitigate these risks. In the context of this research, the focus is

63 Morgan, L. "IoT raises new legal challenges for business" Information Week (2016).
64 Wassom, B.D. "Top 5 legal issues in the internet of things, part 1: data security and privacy" *Wassom.com* (2015).
65 *Supra* 63.

however on specifically considering recommendations that can be achieved through the scope and application of the MHSA and therefore the first risk, whereas further research is recommended in Chapter 6 regarding the other risks.

CHAPTER 6 - RECOMMENDATIONS

Having clearly established the regulatory vacuum, as well as the stated need to fill such vacuum, some key recommendations are made in this Chapter. Some of these are broader in nature, as such will require additional detailed technical evaluation to determine the exact extent of the risk to be mitigated, whilst others are more explicit.

The recommendations are also not an exhaustive list and in the first instance, it is recommended that a DMR and Chamber task team (especially considering the ability to eliminate and mitigate many of the traditional dangers that have affected human life within the industry in the past and the strategic industry drive towards zero harm), consisting of technical, legal, IT, innovation and safety specialists, be constituted to perform a detailed evaluation of the potential opportunities and risks of IoT implementations. This task team to, after such analysis, collaboratively draft holistic amendments to the MHSA, informed by the below recommendations.

1. Draft bespoke regulations to deal with autonomous and IoT enabled equipment in its broadest sense. In this regard the *Code of Practice* should be utilised as a good basis, albeit that it will require development to specifically accommodate IoT in a wider sense. Amend all current regulations to include special requirements to mitigate the risks associated with IoT enabled equipment, *inter alia,* specifically address:
    a. The processes to declare equipment or apparatus safe for use (in light of recommendation three below, but also in general), *inter alia*, the tests to be conducted or the SABS adherence requirements (clearly in this regard collaborative efforts with the SABS will also be necessary to determine and establish such) for autonomous equipment, wearable devices, systems and any other IoT enabled equipment. For example, the requirement for a flammable gas measuring instrument (as defined in the Minerals Act Regulations) to comply with SABS 1515: it should be carefully considered whether this standard can be applied to IoT enabled or automated measuring instruments, merely by incorporating a reference thereto in the definition akin to that in recommendation three below, or whether a bespoke standard and requirements may be necessary. As discussed in recommendation 2(a) below, purposefully explore opportunities to reduce human exposure to higher danger areas, like those where flammable gas measuring instruments are required and others. Amendments should

therefore aspire to enable the utilisation of IoT enabled solutions in such instances, whilst mitigating any new risk introduced by such devices.

b. The need for special codes of practice and training on identifying the different types of hazards associated with IoT enabled equipment. These codes and training interventions should include the potential hazard of unlawful access to equipment – interaction between operators and IT staff or even operators with a different skillset (which includes a comprehension of IT aspects) need to be specifically considered in this regard.

c. Amend Regulation 8.10 of the MHSA on trackless mobile machinery (TMM) in detail to incorporate autonomous and IoT applications, *inter alia*, the definition of "remote controlled" as discussed in Chapter 3. As also discussed in Chapter 3, a number of requirements in Regulation 8.10 may in fact be entirely negated resulting from the utilisation of autonomous and IoT enabled equipment, for example, the need to take measures to address the risk of objects falling onto operators and TMM or counter acting restricted operator visibility. Further establish whether amendments to the collision detection and collision avoidance measures, as contained in Regulations 8.10.1 and 8.10.2 of the MHSA, may be required, specially addressing:

- Interaction between equipment with detection and avoidance measures and employees wearing wearable devices.
- Circumstances where no human intervention may be possible at any stage due to the equipment being fully automated or IoT controlled.

d. Specific contractual relationships or special risk mitigating measures that may be required due to the introduction of IT service providers in areas or processes where they were not previously involved, *inter alia*, the kind of testing their systems and processes will need to undergo before being regarded as sufficiently proven for safe installation, as also highlighted in the *Code of Practice*.

2. Critically evaluate and address the potential impact on the numerous requirements in the MHSA regarding work to be performed by a competent person. Ensuring that, *inter alia*, the risk mitigating measures are adequately covered contractually where there is an interrelationship between the traditional competent person and either an IT service provider or quite possibly an IoT enabled machine operating autonomously or making the decisions on behalf of the competent person. Some of the risk mitigating measures (which also includes enabling provisions to potentially mitigate other general safety risks) may include:

a. To incorporate a list of actions, in the bespoke regulations referred to above, for which IoT enabled systems may not be used to replace the definite action by a human being and list those where such will be acceptable or include such allowances by amendment in the MHSA. In assessing what is allowable and not, as previously indicated, an aggressive view is recommended to, as far as rationally and reasonably possible, remove the need for physical human inspection, as removing such will naturally reduce the risk of impact to human life. For example, in relation to the Minerals Act Regulations 2.15.5 and 2.15.6 regarding the functions of the shift boss, possible amendments may include:

> "2.15.5 Each shift boss shall inspect all workings in his section as frequently as he may deem necessary in the interest of safety and health: Provided that, unless such inspections can be virtually conducted through approved cameras and systems in which case a physical inspection is not required –
>
> (a) he shall inspect every working face in his section which has been blasted and in which persons are working within two working days of each blast therein;
>
> (b) he shall inspect all other workings at least once every week at intervals not exceeding 10 days; and
>
> (c) he shall daily during his shift -
>
> (i) …
>
> (ii) …
>
> (iii) … The shift boss shall record a report on each such test at the end of his shift in the acceptable format ~~logbook~~ referred to in regulation 2.15.6.
>
> 2.15.6 Each shift boss shall ensure the capturing, during or at the conclusion of his shift, of a record in ~~ink in his logbook~~ any acceptable format [the definition of accepted format should include capturing such by electronic means or even automatic capturing of results without intervention by the shift boss per se] – …"

Naturally, if the above approach is followed, a resulting regulatory requirement will be when and by whom it may be necessary to inspect the equipment and systems used to replace the above human inspections, so as to maintain the necessary trust in the monitoring

processes. Important to note that, in such case, the inspection may have to include someone from IT or someone with IT skills, as also emphasised elsewhere.

b. To adjust the Government Certificate of Competency curriculum to include a focus on IT and how it interacts with and affects traditional general engineering, mining and surveying principles when equipment is IoT enabled and there is a high utilisation of automation, drones etc.

3. Consider an amendment to the definition in Section (46C) of the Minerals Act Regulations: "intrinsically safe apparatus means electric apparatus constructed in such a manner that, when connected through standard, wireless network or any other possible means as in the case of IoT applications and used, any sparking that may occur under any service or fault condition (either in the apparatus or in the circuit or network associated with the apparatus) is not capable of igniting flammable gas."
4. In respect of the Explosives Regulations, this paper did not specifically consider utilisation of robotics, which will be a natural progression. Although the area of explosives, because of the extreme risk and level of detailed regulation, may not be first on the schedule for such implementations, the very detailed regulations should be materially reviewed to consider the application and implications of robotics in this area.
5. In respect of legal appointments, it is recommended that the implications of IoT be considered in relation to:
    a. Remote operation centres: establish whether a legal appointee far removed from the physical site, for which the appointment applies, will be acceptable compliance with the MHSA, as well as where such appointee may be responsible for numerous sites at the same time (the so called thin operating platform).
    b. The MHSA is presently very explicit that legal appointments may not overlap: clarify the position and implication of system overlaps or more unclear system and process boundaries, as discussed elsewhere, and address this in amendments to the MHSA. Even consider whether IT accountable individuals need to be legally appointed where systems perform functions traditionally performed by engineering technical individuals.
6. Although recommendations are focused on MHSA amendments, it is also recommended that amendments to the ECTA and PoPI be considered to incorporate some of the suggested best practices highlighted in *Opinion 8/2014* and the *FTC report* recommendations.

It is, however, recognised that the above processes and proposed amendments or drafting of new requirements will likely be protracted, especially due to the steep learning curve of drafters in order to fully comprehend IoT, its applications and implications. Resultantly, the below recommendations are made for immediate implementation in respect of all mining companies intending to introduce IoT enabled solutions.

The Chief Inspector of Mines to instruct, in accordance with Section 9(2) of the MHSA, the managers of all such mines to prepare and implement a code of practice dealing with the impact and handling of IoT interventions, with specific consideration of the *Code of Practice*, as well as the recommendations regarding, especially, security and encryption, unlawful access and monitoring of system vulnerabilities, as suggested in *Opinion 8/2014* and the *FTC report*. The code of practice should also suggest *ISO/IEC 27001:2013*[66] certification as a minimum standard in order to assist mining companies to establish their security framework, as well as include principles to guide them in determining the appropriate security level based on the risk of the application or equipment. In addition, recommending a specific level of security encryption may be appropriate: at present the highest level is 1024bit encryption and although an aspirational level for all applications, the code should suggest a minimum level of encryption (at least the current deemed norm of 128bit).

The code should also reinforce the need for such mining companies to:

- In accordance with Section 8(1) of the MHSA, update mine policies to incorporate IoT and the impact thereof on operations, as required.
- Ensure training programmes and material have been updated to incorporate changed processes, but also that training in fact positions employees to better understand IoT related hazards.

The instruction must further, in accordance with Section 9(7) of the MHSA, require the review of specific other codes of practice regarded as inadequately protecting health and safety, post the analysis of the impacts of IoT interventions as part of the specific IoT code suggested above.

[66] ISO/IEC 27001:2013 specifies a management system proposed to bring information security under explicit management control.

It is recommended that the following research questions be considered in future research on this topic:

1. In an inter-related mining technological ecosystem, with a variety of different outsourced service providers generating data in addition to internal and employee data generation, explicitly clarify automatic data ownership and intellectual property rights?
2. Critically analyse the South African legislative requirements applicable where employees are required to wear radio frequency identification tags (RFIDs)?
    i. Can employees be legally compelled to do so?
    ii. Can data from RFIDs be used to discipline employees or hold them legally liable for offences?

CHAPTER 7 – CONCLUSION

The fourth industrial revolution is indeed upon us, albeit in some industries more so than in others. The need for innovation, automation, IoT and IIoT in the broadest sense possible and the definite benefits thereof for the mining industry have been clearly presented and also recognised, not only by many progressive and innovative global diversified miners, but also by the South African Chamber of Mines. The motivation not only a business imperative, but also a desire to achieve the objective of zero harm – vital in order for the mining industry to remain socially and morally sustainable in an environment with ever changing societal demands.

The research indicates that, although the MHSA can in many respects be holistically applied to automation and IoT applications, the MHSA really did precede these concepts. It is shown that Australia, as arguably the most mature mining environment with respect to specifically mining automation, has recognised the need for addressing the risks associated with such in a bespoke manner, albeit that their C*ode of Practice* also do not yet fully address IoT.

Although the full scope and potential of IoT is still poorly understood and developing at a rapid pace, despite the very positive results in many areas, some explicit new risks have already emerged and this paper contends that those should be addressed in a proactive, rather than a reactive manner. However, this should not be confused with a conservative or restrictive approach - it is in fact suggested that steps be taken to legally enable the application and implementation of IoT solutions in the mining industry in as many instances as reasonably possible, whilst consecutively and proactively addressing the new and emerging risks created though such.

Instead of legislation lagging innovation, as in most other instances globally, this paper challenges the DMR and Chamber to collaborate in seeking ways to lead legislative and regulatory developments in this space in order to support and enable the sustainability of the South African mining industry.

BIBLIOGRAPHY

Books

Bryman and Bell "Business research methods" second edition *Oxford University Press* (2007).

Masilo, P. and Rautenbach, G. "Commentary on the Mine Health and Safety Act and Regulations" Revision Service 3 Juta (2011).

"The international Comparative Legal Guide to: Mining Law" *Global Legal Group* (2014).

Case law

United States of America before the Federal Trade Commission in the matter of TRENDnet Incorporated, a corporation, Docket No. C-4426.

Domestic Legislation

Electronic Communications and Transactions Act 25 of 2002.

Mine Health and Safety Act 29 of 2009 and its Regulations.

Part 101 of the South African Civil Aviation Regulations.

Protection of Personal Information Act 4 of 2013.

International Legislation and standards

Chapter 10 of the Mines Work Health and Safety (National Uniform Legislation) Regulations.

Coal Mining Safety and Health Act 1999.

Coal Mining Safety and Health Regulation 2001.

Health and Safety (Mines and Petroleum Sites) Regulation 2014.

ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.

Mines Safety and Inspection Act 1994.

Mines Safety and Inspection Regulations 1995.

Mines Work Health and Safety (Supplementary Requirements) Act 2012.

Mines Work Health and Safety (Supplementary Requirements) Regulations 2012.

Mining and Quarrying Safety and Health Act 1999.

Mining and Quarrying Safety and Health Regulation 2001.

Recommendation ITU-T Y.2060 June *2012.*

Work Health and Safety (Mines and Petroleum Sites) Act 2013.

Journals and articles

Catlin, T., Scanlan, J. and Willmott, P. "Raising your Digital Quotient" *Strategy & Corporate Finance McKinsey Quarterly* (2015).

Clubb, K., Kirch, L. and Patwa, N.I. "The Ethics, Privacy and Legal Issues around the Internet of Things" *Berkely School of Information* (2015).

Chui, M., Löffler, M. and Roberts, R. "The Internet of Things" *McKinsey & Company* (2010).

Damisch, A. "Challenges and Opportunities in the Internet of things" *M2M Magazine* (2014).

De Menses, G. "Four industrial revolutions, Internet of things" *ITWeb Tech Forum* (2016).

Farisani, D.M. "Corporate criminal liability for deaths, injuries and illnesses: Is South Africa's mining sector ready for change" Speculum Juris (2012).

Gandhi, P., Khanna, S. and Ramaswamy, S. "How Digitally Advanced Is Your Sector? Which Industries Are the Most Digital (and Why)?" *Harvard Business Review* (2016).

Gross, G. "Senators to push privacy, security legislation for IoT, connected cars" *IDG News Service* (2016).

Hill, K. "This guy's light bulb performed a DoS attack on his entire smart house" *Fusion* (2015).

Hopwood, P. "Global Mining IT/OT convergence: Naturally resourceful" *Deloitte Touche Tohmatsu Limited* (2015).

"Investment in drones, wearables to expand across African mines" Engineering News (2016).

"IoT: The future of mining" *BMI Research* (2016).

Manyika, J., Pinkus, G. and Ramaswamy, S. "The Most Digital Companies are leaving all the rest behind" *Harvard Business Review* (2016).

Mielli, F. "The internet of thins (IoT) and … Mining operations?" *Schneider Electric Blog* (2013).

Morgan, L. "IoT raises new legal challenges for business" *Information Week* (2016).

O'Brien, C. Tim O'Reilly: "Silicon Valley is massively underestimating the impact of IoT" (interview) *venturebeat* (2015).

"OEM Autonomous Driving Strategies: A Review" *BMI Research* (2016).

Pereira, A.G., Benessia, A. and Curvelo, P. "Agency in the Internet of Things" *JRC Scientific and Policy Reports* (2013).

Raynor, M.E. and Cotteleer, M.J. "The more things change: Value creation, value capture, and the Internet of Things" *Deloitte Review Issue 17* (2015).

Roberts, J. "The internet of things is here, but the rules to run it are not" *Gigaom* (2014)

Saif, I. Peasley, S. and Perinkolam, A. "Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age" *Deloitte Review Issue 17* (2015).

Samuelsohn, D. "What Washington really knows about the Internet of Things" *POLITICO* (2015).

"The Internet of Things: Mapping the value beyond the hype" *McKinsey Global Institute* (2015).

"Towards 2050: Megatrends in Industry, Politics and the Global Economy" *BMI Research Special Report* (2016).

Wassom, B.D. "Top 5 legal issues in the internet of things, part 1: data security and privacy" *Wassom.com* (2015).

Williams, L. "The Wild West of IoT Legislation" *CMS WiRE* (2016).

Zetter, K. "A cyberattack has caused confirmed physical damage for the second time ever" *Wired* (2015).

Presentations and company documents

"Integrated annual review 2015 Chamber of Mines of South Africa".

"Rio Tinto Mine of the Future™ Next generation mining: people and technology working together".

"Where do we go from here? The market forces changing mining and the outlook for key commodities" MINExpo INTERNATIONAL® *McKinsey & Company* (2016).

Websites

Anglo American South African website: Partnerships and innovation are key themes on day one of mining Indaba, http://www.angloamerican.co.za/our-stories/partnership-and-innovation-mining-indaba.aspx

Chamber of mines website: http://www.chamberofmines.org.za/

Hewlett Packard: http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.VrLfonJf2Gk

Federal Trade Commission website: https://www.ftc.gov/

International Telecommunication Union website: http://www.itu.int/en/about/Pages/default.aspx

London Business School website: https://www.london.edu/faculty-and-research/lbsr/davos-2016-fourth-industrial-revolution#.V3uCL3lf3IU

Safe Work Australia website: http://www.safeworkaustralia.gov.au/sites/swa/whs-information/mining/pages/mining

Rio Tinto website: Mine of the Future™ http://www.riotinto.com/australia/pilbara/mine-of-the-future-9603.aspx