An Analysis of Social Media Misconduct in the Workplace

By

Ramesh Thilak Arjun

Submitted in partial fulfilment of the requirements of an LLM
(Labour Studies)

University Of KwaZulu-Natal
College of Law and Management Studies
School of Law
Howard College Campus

Supervisor:
Ms Rowena Bernard
2018

DECLARATION

I, Ramesh Thilak Arjun, hereby declare that:

1. I fully understand what plagiarism is and the policy of the University of KwaZulu-Natal regarding plagiarism;
2. I declare that I have not copied and pasted any material from any source directly and presented it as my own;
3. I have cited all the sources accordingly by referencing and footnoting;
4. I have not copied anyone's work and submitted it as my own;
5. I have not passed this work to anyone to copy and submit as their own; and
6. I am the sole author of this work.

…… ……..

Signature Date

ACKNOWLEDGEMENTS

My eternal gratitude to my wife Nishee Arjun (1962-2010) for having taught me the values and the joys of family life, and for sharing with me her uninhibited love for the mountains, rivers, oceans, rainy days, wild flowers and Bollywood movies.

I thank my son Teyash Arjun for granting me the greatest accolade possible, that of being his father, and for allowing me to be a part of his life's journey for the past two decades. I hope to share in his journey for many, many more decades.

My thanks go also to Ms Rowena Bernard for her patience, her superb supervisory skills and her willingness to help.

ABBREVIATIONS

CCMA	Commission for Conciliation, Mediation and Arbitration
ECPA	Electronic Communications Privacy Act of 1986
ECTA	Electronic Communications and Transactions Act 25 of 2002
ERA	Employment Relations Act 24 of 2000
LRA	Labour Relations Act 66 of 1995
NLRA	National Labor Relations Act 29 U.S.C 151-169 (2012)
NZBOR	New Zealand Bill of Rights Act 109 of 1990
POPI	Protection of Personal Information Act 4 of 2013
RICA	Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002

TABLE OF CONTENTS

DECLARATION 2
Chapter 1 8
Introduction 8
1.1 Introduction 8
1.2 Background 8
1.3 Research questions 10
1.4 Objectives: 10
1.5 Research methodology: 10
1.6 Structure of the dissertation: 11
Social and psychological factors that influence human behaviour 12
2.1 Introduction 12
2.2 Understanding the 'social' in social media 12
2.3 Understanding social network services and social media 14
2.4 Types of social networks 15
2.5 Summary: 17
Chapter 3 18
Dignity, privacy, freedom of expression 18
3.1 Introduction 18
3.2 Dignity 18
3.3 Privacy 22
3.4 Freedom of expression 26
Chapter 4: 29
Risks to the employer arising from social media misconduct 29
4.1 Introduction 29
4.2 Vicarious liability 30
4.3 Defamation 33
4.4 Harassment and discrimination 34
4.5 Breach of copyright 35
4.6 Inadvertent formation of contracts 35
4.7 Productivity and efficiency 36
4.8 Summary 37
Chapter 5: 39
Foreign Law 39

5.1 Introduction 39
5.2 The USA 39
5.2.1 Introduction – Public Sector Employee 39
5.2.2 "Electronic Communications Privacy Act of 1986" ('ECPA') 41
5.2.3 "The National Labor Relations Act" (NLRA) 42
5.2.4 Court decisions 43
5.3 Canada 46
5.3.1 Introduction 46
5.3.2 The Canadian Charter of Rights and Freedom 47
5.3.3 Federal and provincial privacy legislation 47
5.3.4 Court Decisions 48
5.4 The United Kingdom, Australia, and New Zealand 50
5.4.1 The UK 50
5.4.2 Australia 52
5.4.3 New Zealand 53
5.5 Summary 54
Chapter 6: 56
Social Media Misconduct in South Africa 56
6.1 Introduction 56
6.2 South African Law relating to Social Media Misconduct in the Workplace 56
6.2.1 "The Constitution" 56
6.2.2 "Labour Relations Act" ('LRA') 58
6.2.3 "Regulation of the Interception of Communications and Provision of Communication Related-Information Act 70 of 2002" (RICA) 60
6.2.4 "Electronic Communications and Transactions Act" (ECTA) 63
6.2.5 "Protection of Personal Information Act" (POPI) 63
6.2.6 Analysis of South African legal decisions 65
6.3 Summary 69
Chapter 7: 70
Concluding Comments: 70
7.1 Introduction 70
7.2 Present-day status of social media misconduct in workplaces 70
7.3 Social Media Policies (SMP) 74
7.4 Conclusion 76

ABSTRACT

This paper serves to analyse social media misconduct in the workplace. The introduction of electronic and social media has brought about significant changes to how business is conducted. Despite its widespread benefits, social media usage has the potential to cause harm to a business entity.

The aim of this dissertation is to analyse the different forms of harm that may befall a business through social media misuse, and the tools that are available and the steps that need to be taken to avert such harm.

The analysis will be undertaken by referring to South African legislative and common law principles and by drawing a comparison with the approach adopted by foreign jurisdictions in respect of social media misconduct in their workplaces.

Chapter 1
Introduction

1.1 Introduction

Humans are social animals, and they have a need to communicate with each other. Social media allows people to communicate with each other through the medium that they prefer.[1]

Communication has evolved from writing letters, sent via the postal service, to the use of the internet where communication occurs instantly. Businesses were quick to see the benefits of social media and began using it in the promotion of their goods and services, and to connect with existing and potential customers. Today it is commonplace to find, on the websites of businesses and in their advertising material, the inclusion of their Facebook and Twitter accounts.

It was inevitable, with the popularity and widespread use of social media, both by individuals and business entities alike, that conflicts would arise. One form of conflict that has arisen, and which is the subject matter of this analysis, is social media misconduct in the workplace.

Social media misconduct, which is rooted in interpersonal conflict, enters the public domain through human communications. Conflicts may have arisen from individual judgements of fairness in social exchanges, the consequent reactions to perceived unfairness, and the tactics that are chosen to deal with the perceived injustices.

1.2 Background

There is little dispute that social media has proved to be enormously beneficial, both for individuals and business entities alike. However, the benefits brought about by social media are counterbalanced, at times, by the negative attitudes of social media users. Social media used to harass and bully, promote pornography, commit fraud, post racist and sexist comments, and take part in similar anti-social conduct, is the

[1] B Hale 'The history of social media: social networking revolution' (2015) *History Co-operative* at page 6.

stark reality of our times.[2] The workplace has not been left unscathed by the negative repercussions of social media misconduct.

Van Jaarsveld observes that the negative attributes of electronic and social media, in the workplace, are numerous: it may result in reduced productivity where employees occupy themselves with updating their social media profiles, instead of working. Employees may expend work time downloading music and video recordings and engaging in other online activity, thereby, reducing the employer's bandwidth, and adding to costs; the possibility of viruses infecting workplace systems as a result of non-work-related employee activities; employees visiting pornographic sites; employees posting defamatory comments, regarding co-workers or management; employees posting confidential information on their web profiles.[3]

Conversely, employees may claim infringement of their privacy rights where employers unlawfully view their private communications, or where employers use data extracted from employees' private web profiles to make decisions relating to recruitment and remuneration.

The laws relating to social media misconduct in the workplace are in their infancy. The reason being that social media, in its present form, was unheard of until just over a decade ago. Courts have, however, in numerous instances, pronounced on social media misconduct in the workplace.

This submission is an analysis of social media misconduct in the workplace. Included in this analysis will be an assessment of legislation, both nationally and internationally; the impact of social media misconduct on organisations; and how social media misconduct cases have been decided in South Africa and foreign legal jurisdictions. The analysis will conclude with a section on the lessons learnt, and recommendations for the future.

[2] M Van Jaarsveld 'Forewarned is forearmed: some thoughts on the inappropriate use of computers in the workplace' (2004) 16 *South African Mercantile Law Journal* 651,666.
[3] Ibid 651.

1.3 Research questions

This dissertation is aimed, foremost, at analysing the impact of social media misconduct in the South African workplace. A proper and comprehensive analysis will require, in addition, that attention be paid to the different sub-components of the research topic. These include:

1.3.1 What laws have been enacted, to counteract the negative effects of social media misconduct?

1.3.2 What are the types of misconduct that could occur in the workplace?

1.3.3 What is the impact, on a business entity, of social media misconduct?

1.3.4 How is the problem of social media misconduct handled in foreign jurisdictions?

1.3.5 What lessons can be learnt?

1.4 Objectives:

The objectives of this dissertation are:

1.4.1 To identify and analyse the laws that have been enacted to counteract the negative effects of social media misconduct.

1.4.2 To investigate the types of social media misconduct that could occur in a business organisation, and the potential effects on both employers and employees.

1.4.3 To analyse the impact of social media misconduct on a business entity.

1.4.4 To determine how social media misconduct is handled in foreign jurisdictions. In this section, there will be an examination of the legislation and important court decisions of the USA, Canada, the UK, Australia and New Zealand. This section will highlight the similarities, and differences, in respect of South Africa's approach to workplace social media misconduct, in comparison to that adopted by other countries.

1.4.5 To identify lessons that can be adopted in South Africa.

1.5 Research methodology:

The research methodology used for the submission is desk-based. It involves an analysis of literature from various sources, originating both nationally and globally,

and includes journal articles, books, and case law. The material is considered within the constitutional and legal framework of South Africa.

1.6 Structure of the dissertation:

This dissertation is discussed in seven chapters.

Chapter 1 provides an introduction to the subject. It contains a broad description of social media, the aim of the study, and the research methodology used.

Chapter 2 examines, in brief, the social and psychological factors that underpin human behaviour. The conduct of employers and employees in the workplace do not occur in isolation, their conduct is influenced significantly by factors that are unrelated to the workplace, and these factors are considered. The chapter thereafter explains social networking services and social media usage, in broad society and in the workplace, while always being cognisant of the social and psychological factors that direct human behaviour.

Chapter 3 considers the three fundamental rights that are most often at issue when social media misconduct occurs in the workplace. These are the rights to dignity, privacy and freedom of expression.

Chapter 4 analyses the risks that are posed to the employer consequent to employees' misuse of social media.

Chapter 5 examines foreign law as it applies to social media usage in the workplace. This chapter analyses legislation and the decisions of courts in the USA, Canada, Australia, New Zealand, and the UK.

Chapter 6 analyses social media misconduct in the South African workplace and includes an assessment of the applicable laws and decided cases.

Chapter 7 concludes the dissertation and provides recommendations on how best to address the matter of social media misconduct in the workplace.

Chapter 2

Social and psychological factors that influence human behaviour

2.1 Introduction

Astute employee relations practitioners are required to be aware, especially in South Africa with its troubled history of legislated racial discrimination and inequality, of the diverse nature of their workforce. They need to be aware that employees and employers differ from each other in significant areas. These include differences based on gender, class, race, sexual orientation, socio-economic status, social upbringing, levels of education and other factors. The workplace is a microcosm of broad society; therefore, societal conflicts and tensions are carried into the workplace on a daily basis and may emerge as contributory factors to social media misconduct within the workplace. Employers must be conscious of these tensions and must pro-actively take steps to avoid having these tensions turn into workplace misconduct, including social media misconduct.

In this chapter, consideration will be given to the underlying causes of social media misconduct in the workplace and the tools that are most often utilised, by employers and employees, to engage in social media misconduct.

2.2 Understanding the 'social' in social media

"Social psychology is the scientific field that seeks to understand the nature and causes of individual behaviour in social situations."[4] The subject is vast and includes social perception, social cognition, attitude formation, prejudice and discrimination, social influence, aggression, group and individual behaviour, environmental influence on behaviour, and personality.[5] Space constraints prevent a comprehensive discussion of the subject, and only certain key elements will be highlighted.

The central idea of the behaviourist school of psychology is that individual behaviour is shaped by two factors: genetics, and the environment. The founder of the behaviourist school is John Watson, who stated: *"*Give me a dozen healthy infants,

[4] R Baron & D Byrne *Social Psychology: Understanding Human Interaction* 5 ed (1987) at page 11).
[5] Ibid 12.

well-formed, and my own specified world to bring them up in and I'll guarantee to take any one at random and train him to become any type of specialist I might select – doctor, lawyer, merchant, chef, and yes, even beggar-man and thief, regardless of his talents, penchants, abilities, vocation, and the race of his ancestors."[6] The essence of Watson's argument is that our behaviours, to a large extent, are shaped by our environment. It follows, therefore, that nationalism, racism, gender superiority and prejudice[7] are learned (not genetically acquired) behaviours.

Baron and Byrne have noted that there is a range of individual maladaptive behaviours[8] – these include stress and adjustment disorders, anxiety-based disorders, personality disorders, mood disorders, delusional disorders, substance abuse and other addictive disorders, sexual disorders and variants, and organic mental disorders and mental retardation.[9] Suffice it to say that every human is inflicted, to a lesser or greater extent, with one form of a psychological disorder or another.

In summary, when employees and employers enter the workplace and interact with each other continuously for the greater part of the day, there must be an awareness that the public personas presented in the workplace are hugely influenced by social and psychological factors outside of the office or factory floor.

The individual, who, for example, posts derogatory comments about other race or religious groups within the workplace community, is almost certainly giving vent to values, beliefs and learned behaviours acquired from membership of communities outside of the workplace. Employers must be cognisant of the internalised non-work-related tensions that may give rise to social media misconduct. Cilliers has correctly stated that "social media is about sociology, not technology."[10]

---

[6] PH Mussen...et al. *Child Development and Personality* (1990) 6 ed at page 16
[7] Baron & Byrne (note 4 above; 151) "An attitude, usually negative, towards members of some group based solely on their membership in that group".
[8] Baron & Byrne (note 4 above).
[9] Ibid.
[10] F Q Cilliers 'The role and effect of social media in the workplace' (2013) 40(3) *Northern Kentucky Law Review.*

2.3 Understanding social network services and social media

Advances in technology in recent years have led to significant changes in the way individuals communicate, relay information and share knowledge. This is evident through the widespread use of technological devices such as smartphones and tablets, as well as through discussions on social media networks such as Facebook and Twitter. While many of these devices originated as entertainment, their prevalence in daily life has led to their increased usage in the employment setting – companies have taken advantage of these social media platforms both externally, to advertise, and internally, to expand knowledge sharing. [11]

There are several definitions of a social networking service (hereafter referred to as SNS) and social media. Boyd and Ellison[12] define SNS's as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site".

Social networking sites impact people of varying ages and of various professional persuasions, both in the developed and non-developed world, and have quickly gained acceptance and use in education, research, the corporate world, government, politics, professional practice, and in general society.[13]

The enormity of the power of social media and social networking services are discussed by Mutula:[14] "It is instructive that the political revolution in North Africa that overthrew the regimes of Ben Ali of Tunisia, Hussein Mubarak of Egypt and Muammar Kaddafi of Libya were orchestrated through social networks, by young people using mainly Twitter and Facebook, to mobilise the masses."

---

[11] J Ireton 'Social Media: What control do employers have over employee social media Activity in the workplace' (2014) 14 *Houston Business and Tax Law Journal.*

[12] D Boyd & N Ellison 'Social network sites: definition, history, and scholarship' (2007) *Journal of Computer Mediated Communication".*

[13] SM Mutula 'Policy gaps and technological deficiencies in social networking environments: implications for information sharing' (2013) 15(1) *SA Journal of Information Management* (page 1).

[14] Ibid 6.

The power of social media and social networking services are as important in the workplace context. Aside from its positive attributes and the goodwill that it can generate, social media allows disgruntled employees to publicise their views to an unlimited number of recipients and, in the process, may cause significant reputational damage to an organisation.

2.4 Types of social networks

Mutula describes five types of social networks – these are personal networks, status update networks, location networks, content sharing networks, and shared interest networks.[15]

Personal networks allow users to create detailed online profiles and connect with other users with the emphasis being on social relationships. The best-known example is Facebook.[16] Anyone with an email account may set up a Facebook account. Users set their privacy settings at different levels. At the least restrictive public level, all two billion Facebook users can view what is on a user's account, and at an intermediate level, only the user's friends can view the content. Facebook allows users to customize their privacy settings.[17]

Facebook users create a profile on the site, and they may include information such as their age, political and religious affiliation, employment or campus information and pictures of family.[18] The user adds 'contacts' to build social relationships. Messages may be "posted on a user's wall, and everyone listed as a contact is able to view the messages."[19]

Facebook subscribers can gain access to other users' profiles depending on the privacy levels set up by the latter. Facebook's policies state that privacy settings are not fool-proof and, further, that Facebook has no means of verifying the honesty, reliability or accuracy of information uploaded to their site by users.[20]

---

[15] Ibid 3.
[16] *Heroldt v Wills* 2014 JOL 31479 (GSJ).
[17] *Heroldt supra at para 10.*
[18] *Heroldt supra at para 12.*
[19] *Heroldt supra at para 15*.
[20] *Heroldt supra at para 18.*

Status update social networks are designed to allow the users to post short status updates to communicate with other users quickly. Twitter is the best-known example. Twitter is an information sharing or micro-blogging site. Subscribers tweet their messages and share information with their followers, and these messages are publicly visible by default.[21]

Google Latitude is an example of a location network, and it allows the public or authorised contacts to view the user's real-time location.[22]

Content sharing networks allow for the sharing of verbal and text-based exchanges, music, photographs, and videos. YouTube is the best example in this sub-category. Shared interest networks, such as Linked-in, are built around the common interests of specific groups of people.[23]

Facebook is the most popular social networking site in South Africa, and in most of the countries of the world.[24] It was launched in 2003 by Harvard student Mark Zuckerberg.[25] The number of Facebook users, on June 30th, 2017, consisted of 1.98 billion subscribers. In the context of a world population of 7.51 billion people, 26.3% of the people on the planet use Facebook. In the period 2010 to 2017, Facebook subscribers increased by 282%.[26]

Statistics provided by Omnicore[27] are illustrative of the popularity of social media. As at 1st January 2018, the number of Facebook users was recorded at 2.07 billion persons, the number of active Twitter users was 330 million persons, Linked-in had 500 million active users, and YouTube had an impressive 1.57 billion active users.[28]

---

[21] *Heroldt supra at para 22.*
[22] Mutula (note 13 above).
[23] Mutula (note 13 above).
[24] Mutula (note 13 above).
[25] *Heroldt supra at para* 14.
[26] Miniwatts Marketing Group*: Internet World Stats(*2017)available at http://www.internetworldstats.com, accessed on 12 November 2017.
[27] Omnicore Group (2018) available at http://www.omnicoreagency.com, accessed on 5 March 2018.
[28] Ibid.

2.5 Summary:

The discussion above illustrates the popularity of social media, and its ability to allow the user to disseminate his or her message to a global audience. It was noted that social media is available to virtually everyone, both to those with benevolent or malevolent intentions.

In their roles as employers and employees, the players do not perform as automations. They are influenced, in everything that they do, by the sum of their life experiences that have shaped, throughout their lives, their characters and beliefs. Racial and gender superiority, nationalism, the effect of family violence and similar attributes lie within the individual, at a subliminal level, and is triggered, and surfaces, when a stress-inducing occurrence presents itself. Very often, in such moments, the individual turns to the use of a powerful weapon in his armoury: social media.

In the remaining chapters, the focus will narrow, and the attention will shift gradually to social media misconduct in the workplace.

Chapter 3
Dignity, privacy, freedom of expression

3.1 Introduction

This chapter presents a discussion of three rights contained in the Bill of Rights, which often feature in disputes relating to social media misconduct in the workplace. These are the rights to dignity, privacy and freedom of expression. These rights will be discussed broadly. In the chapters that follow, it will be shown how the rights apply within the narrower field of labour law.

3.2 Dignity

The history of humankind abounds with unimaginable atrocities inflicted by human beings on fellow beings. In what is the present age of enlightenment and technological progress, the dark side of the human spirit is as prevalent today as at any time in the world's history. Wars continue but with technologically advanced weapons, slavery exists in the form of modern-day human trafficking, corporate greed for profit results in a high incidence of child labour and poor work conditions, medical care is denied to vast numbers of people as pharmaceutical companies refuse to relinquish patent rights and sell medicines at inflated prices. The resultant effect is that the dignity of a significant number of persons is compromised.

Assaults on dignity occur, both overtly and covertly, in the workplace. It is not uncommon for employees to be singled out and unfairly discriminated against, on diverse grounds including race,[29] religion,[30] gender,[31] sexual orientation[32] or disability.[33] Social media is a tool that is often used to infringe on the dignity of fellow employees. Examples of such conduct include disparaging posts about a fellow employee's race, religion or sexual orientation or creating a hostile work environment by viewing or disseminating pornographic material during work hours.

---

[29] *Govender v Mondi Kraft-Richards Bay* 1999 (20) ILJ 2881(LC).
[30] *Kievits Kroon Country Estate (Pty) Ltd v Mmoledi & Others* 2014 (35) ILJ 406(SCA).
[31] *Ekhamanzi Springs (Pty) Ltd v Mnomiya* 2014 (35) ILJ 2388 (LAC).
[32] *Ehlers v Bohler Uddeholm Africa (Pty) Ltd* 2010 (31) ILJ 2383 (LC).
[33] *IMATU & Another v City of Cape Town* 2005 (26) ILJ 1404 (LC).

An individual's dignity rights are recognised in several provisions of South Africa's Constitution.

The Constitution[34] states, in section 1 of its founding provisions, that "the Republic of South Africa is one sovereign, democratic state, founded on the following values: Human dignity, the achievement of equality and the advancement of human rights and freedom…"

In Section 7(1) it is provided that "this Bill of Rights is a cornerstone of democracy in South Africa. It enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom."

Section 10 provides that *"*everyone has inherent dignity and the right to have their dignity respected and protected.*"* The importance of human dignity prompted the Constitutional Court to describe the right to dignity and the right to life as the most important human rights."[35] In *S v Makwanyane,*[36] the Constitutional Court stated: *"*recognising a right to dignity is an acknowledgement of the intrinsic worth of human beings: human beings are entitled to be treated as worthy of respect and concern. This right, therefore, is the foundation of many of the other rights that are specifically entrenched in…. the Bill of Rights."

The Constitutional Court went further, in *S v Makhwanye*, to state that: *"*The rights to life and dignity are the most important of all human rights, and the source of all other personal rights in the Bill of Rights. By committing ourselves to a society founded on the recognition of human rights, we are required to value these two rights above all others."[37]

"Human dignity is that which gives a person their intrinsic worth, therefore, dignity is above all price and so admits of no equivalent."[38] It is the source of a person's innate rights to freedom and physical integrity, from which several other rights flow. Human

[34] The Constitution of the Republic of South Africa Act 108 of 1996.
[35] J De Waal,,I Currie & G Erasmus.*The Bill of Rights Handbook* 3 ed (2000) .
[36] *S v Makwanyane* 1995 (3) SA 391 (CC).
[37] Ibid – see also J De Waal, I Currie & G Erasmus *The Bill of Rights Handbook* 3 ed (2000) 209.
[38] Ibid 209 where the authors quote from B Jones article "Kant's Principle of Personality".

dignity accordingly also provides the basis for the right to equality since every person possesses human dignity in equal measure, everyone must be treated as equally worthy of respect.[39]

The Universal Declaration of Human Rights (UDHR) is a document held to be the bedrock of human rights law and reads:

> "Whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world ……. Now, therefore, the General Assembly proclaims the Universal Declaration of Human Rights as a common standard of achievement for all peoples and all nations …."[40]

The UDHR resulted from the experiences of the Second World War where the international community vowed never again to allow atrocities like those of that conflict to occur again.[41]

Human dignity has come to display three elements in the post-war legal context. Human beings have an equal inherent human dignity that cannot be waived or diminished; inherent human dignity must be recognised and respected; states have a positive obligation to progressively realise human dignity through the mechanism of socio-economic rights.[42]

According to Steinmann, it is widely accepted that the elements have their root in Kantian moral ethics, which hold that man's autonomy is based upon universal dignity, because of which man should never be used as a means to an end, but only as a means in himself.[43]

Inherent dignity comprises the totality of the uniqueness of a human being's nature, his intelligence and his sensibilities. Implicit in the inherent claim of dignity is the

---

[39] De Waal (note 35 above).
[40] Proclaimed by the UN General Assembly in Paris on 10th December 1948, GA Resolution 217 A.
[41] History of the Document available at http://www.un.org, accessed on 6 March 2018.
[42] R Steinmann, R 'The core meaning of human dignity' (2016) 19 *PER /PELJ.*
[43] Ibid.

acknowledgement and acceptance of diversity and differences in human beings and cultures.[44]

The concept of dignity featured prominently in the *Stransham-Ford v Minister of Justice and Correctional Services*[45] decision where, in a case relating to assisted suicide, Justice Fabricius spoke of how the effects of "unbearable and interminable suffering infringe on the categorical imperative of section 10 of the Bill of Rights".

The interpretation of dignity is not inherently and universally accepted but is often a social construct which may conflict with others' understanding of dignity. In *MEC for Education: KZN v Pillay,*[46] the Constitutional Court emphasised that "human dignity encompasses the unique set of ends of each individual, so that a Hindu female learner may wear a nose stud in school as an expression of her South Indian Tamil Hindu culture."[47]

In *Minister of Home Affairs and others v Watchenuka*[48] the SCA stated "human dignity has no nationality. It is inherent in all people – citizens and non-citizens alike – simply because they are human." The SCA stated further, "the inherent dignity of all people – like human life itself – is one of the foundational values of the Bill of Rights. It constitutes the basis and inspiration for the recognition that is given to other more specific protections that are afforded by the Bill of Rights."[49]

The impairment of employers' and employees' rights to dignity in the workplace, resulting from social media usage, is a frequently occurring global phenomenon. Bullying, disseminating sexually explicit material, harassment, racism and sexism are a few examples of social media misconduct in the workplace that may have the effect of infringing on one's right to dignity.

---

[44] Ibid.
[45] *Stransham-Ford v Minister of Justice & Correctional Services* 2015 (4) SA (GP).
[46] *MEC for Education: KZN v Pillay* 2008 (1) SA 474 (CC).
[47] Ibid.
[48] *Minister of Home Affairs and others v Watchenuka* (2003) ZASCA 142 at para 25.
[49] Ibid at para 26.

3.3 Privacy

In South Africa, privacy protection is derived from several sources, "the three major tributaries being the common or civil law (usually the law of delict or tort), a Bill of Rights, and legislation.[50] These streams do not flow independently, and, in fact, their confluence increases the potential power of the protection of privacy. The right to privacy is a guaranteed right and this right, together with the inherent right to dignity, contributes to humanity."[51]

However, a balance needs to be found between respect for a person's private spheres, and the involvement of others in individual lives. People are fully human, not only through engagement with others but also where others show respect for their private domain. The African concept of 'Ubuntu' highlights a spirit of interconnectedness, or collectivity, rather than individual privacy.[52]

Neethling[53] views privacy as "an individual condition of life characterised by isolation from the public and publicity." This means an absence of acquaintance with the individual or his personal affairs, therefore, privacy is infringed by an unauthorised acquaintance by outsiders with the individual or his personal affairs.[54]

Section 14 of the Constitution reads *"*Everyone has the right to privacy, which shall include the right not to have – (a) their person or home searched; (b) their property searched; (c) their possessions seized; (d) the privacy of their communications infringed."[55] Section 14 has two parts – "the first guarantees a general right to privacy, and the second protects against specific infringements of privacy, namely searches and seizures and infringements of the privacy of communications."[56] Protection "against searches and seizures is a subordinate element of the right to privacy," therefore, in addition to the search, seizure or interception of a communication, there

---

[50] J Burchell 'The legal protection of privacy in south africa: a transplantable hybrid' (2009*)* 13(1) *Electronic Journal of Comparative Law*
[51] Ibid.
[52] Ibid.
[53] J Neethling, J M Potgieter & P J Visser *Law of Delict* (1st ed) (1990) at 294.
[54] Ibid at 294.
[55] The Constitution of the Republic of South Africa Act 108 of 1996.
[56] De Waal (note 35 above).

must also be an infringement of the general privacy right for constitutional protection to be invoked.

The common law recognises the right to privacy as an independent personality right – breach of a person's privacy constitutes an iniuria.[57] In *Financial Mail v Sage Holdings,*[58] the court stated: "there is a public interest in preserving confidentiality in regard to private affairs and in discouraging the leaking of private and confidential information, unlawfully obtained, to the media (and others)."

In *Bernstein v Bester NO,*[59] the court cautioned against a straightforward use of common law principles to interpret fundamental rights, and the limitations thereof, in the following words:

> "Caution must be exercised when attempting to project common law principles onto the interpretation of fundamental rights and their limitation; it is important to keep in mind that at common law the determination of whether an invasion of privacy has taken place constitutes a single enquiry, including an assessment of its unlawfulness …. In constitutional adjudication under the Constitution, by contrast, a two-stage approach must be utilised …."

The scope of a person's privacy extends only to aspects of his or her life or conduct regarding which a legitimate expectation of privacy can be harboured.[60] A legitimate expectation is one that, though there exists a subjective expectation of privacy, society nonetheless considers it (objectively) reasonable. The court in *Bernstein*[61] stated:

> *"*The truism that no right is to be considered absolute, implies that from the outset of interpretation each right is always already limited by every other right accruing to another citizen. In the context of privacy, this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community.

---

[57] Ibid 243.
[58] *Financial Mail v Sage Holdings* 1993 (2) SA 451(A).
[59] *Bernstein v Bester NO* 1996 (2) SA 751 (CC).
[60] *Bernstein supra.*
[61] *Bernstein supra* at para 67.

> This implies that community rights and the rights of fellow members place a corresponding obligation on a citizen, thereby shaping the abstract notion of individualism towards identifying a concrete member of civil society. Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations, and activities such as business and social interaction, the scope of personal space shrinks accordingly."

In respect of business undertakings, it was held in *Mistry v Interim Medical and Dental Council of South Africa*[62] that the more public the undertaking and the more closely regulated, the more attenuated the right to privacy would be and the less intense any possible invasion. The greater the potential hazards that a business poses to the public, the less an inspection of the business can be considered an invasion of privacy.[63]

The aspect of privacy which relates to the right to be left alone has been considered in several court decisions. *Case v Minister of Safety and Security*[64] related to a challenge of the "Indecent or Obscene Photographic Materials Act 37 of 1967" where the court found that it was an unjustifiable invasion of privacy to prohibit possession of pornography in the privacy of one's home and the offending section was declared unconstitutional and invalid.

Notwithstanding the above, the right to personal use of erotic material in the privacy of the home may be limited where, for example, the material consists of child pornography. In such instances, possession and use may be prohibited, even if it occurs in the privacy of one's home.[65]

In the *National Coalition for Gay and Lesbian Equality v Minister of Justice,*[66] the Constitutional Court considered the constitutional validity of the common law offence of sodomy and the statutory provisions based on the offence. The court considered the matter not only in respect of the right for someone not to be subject to

---

[62] *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC).
[63] De Waal (note 35 above).
[64] *Case and Another v Minister of Safety and Security* 1996 (3) SA 617 (CC).
[65] De Waal (note 35 above; 248).
[66] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 (CC).

discrimination based on his or her sexual orientation but also in terms of the rights to privacy and dignity. The court found that the criminalisation of sodomy infringed on the individual's right to self-realisation that is contained within one's privacy rights.

Informational privacy is directed at the protection of human dignity, it guarantees the right of a person to have control over the use of private information.[67] It relates to any private information, and not only information that causes damage to one's dignity or has the potential to cause embarrassment.

Privacy rights include a person's right not to have his or her home or property searched. The meanings attached to the words property and possessions, and when a regulatory inspection of business premises becomes a search, needs to be determined on a case-by-case basis. In general, searches and seizures that invade privacy must be conducted in terms of legislation clearly defining the power to search and seize. They are only permissible to achieve compelling public objectives and, where searches and seizures violate the right to privacy, these must be authorised by a warrant. Several laws authorise searches and seizures, the most important of which is the Criminal Procedure Act 51 of 1977.[68]

It follows, therefore, after having considered the above, that privacy rights are held to be extremely important in South Africa and in progressive countries throughout the world.

Infringements of privacy rights may occur in the workplace through social media use, and the question that is often found to be perplexing is how to balance the privacy expectations of employees against employers' rights to monitor and regulate the communications of workers. The rights to privacy of employees are not extinguished on their signing of employment contracts. Conversely, the employer has the right to manage their employees' activities and take steps to prevent harm that may be caused to the business through the activities of employees. The next chapter will consider the reasons that may justify an employer's monitoring of employee social

[67] De Waal (note 35 above; 250).
[68] De Waal (note 35 above).

media conduct, and the subsequent two chapters will analyse the legal mechanisms that allow employers, in given circumstances, to intrude on employees' privacy rights.

3.4 Freedom of expression

The right to freedom of expression is expressly provided for in "Article 10 of the European Convention on Human Rights."[69] "Article 19 of the UN Declaration of Human Rights" also expressly provides for freedom of expression.[70] In the South African context, section 16[71] of the Constitution provides for the freedom of expression.

There are three main reasons[72] for giving constitutional protection to freedom of expression. Firstly, to speak or otherwise express oneself is a natural and essential part of human activity and serves as the fulfilment of one's personality. Secondly, freedom of expression allows for scientific, artistic, or cultural progress. Such progress would be impossible if people were not free to express their ideas and discoveries. Finally, the Constitutional Court stated in *South African National Defence Force Union v Minister of Defence,*[73] "freedom of expression is one of a web of mutually supporting rights in the Constitution and is closely related to section 15 (freedom of religion), section 10 (dignity), section 18 (freedom of association), the right to vote (section 19), and the right to assembly (section 17)."

---

[69] Council of Europe*, European Convention for the Protection of Human Rights and Fundamental Freedoms,* 4th November 1950.

[70] Article 19 reads "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

[71] "S16. (1) Everyone has the right to freedom of expression, which includes
- freedom of the press and other media;
- freedom to receive or impart information or ideas;
- freedom of artistic creativity; and
- academic freedom and freedom of scientific research.

(2) The right in subsection (1) does not extend to
- propaganda for war;
- incitement of imminent violence; or
- advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm".

[72] De Waal (note 35 above; 282).

[73] *South African National Defence Force Union v Minister of Defence* 1999 (4) SA 469 (CC).

There is a need to curtail the scope of freedom of expression, and this is evident in section 16(2)(c). This provision excludes "advocacy of hatred that is based on race, ethnicity, gender or religion."[74]

Defamation is frequently an issue within the context of freedom of expression. Defamation is the wrongful and intentional publication of words or behaviour concerning another person which has the effect of injuring his status, good name or reputation.[75] Grounds for justification, in respect of the purported defamation, are privilege, fair comment, truth and public interest.[76]

Freedom of expression was considered in several South African court decisions. In *Islamic Unity Convention v Independent Broadcasting Authority,*[77] the Constitutional Court considered the possibility that exercising the freedom of expression may impair the enjoyment of other rights, and of the necessity, at times, to limit the exercise of the freedom by applying the provisions of section 36(1) of the Constitution.[78] In *Heroldt v Wills,*[79] the court stated that "resolving the tensions between every human being's constitutionally enshrined rights both to freedom of expression and to dignitas is all about balance ….. need to take into account the context in which a publication occurs."

In *Dutch Reformed Church v Rayan Sookunan t/a Glory Divine World Ministries,*[80] the court stated:

> 'Expression may often be robust, angry, vitriolic, and even abusive. One has to test the boundaries of freedom of expression each time. The court must be alive to the issues involved, the context in which the debate takes place, the protagonists to the dispute or agreement, the language used as well as the content of which is said, written and published and about whom it is published."*[81]*

---

[74] The Constitution of the Republic of South Africa Act 108 of1996.
[75] Burchell (note 50 above).
[76] Ibid.
[77] *Islamic Unity Convention v Independent Broadcasting Authority* 2002 (4) SA 294 (CC).
[78] *Islamic Unity Convention supra* at para 30.
[79] *Heroldt supra.*
[80] *Dutch Reformed Church v Rayan Sookunan t/a Glory Divine World Ministries* 2012 (3) All SA 322 (GSJ).
[81] *Dutch Reformed Church supra* at para 23.

Social media is a tool that is readily available, in society and in the workplace, which allows individuals to exercise their right to freely express themselves. However, granting employees uninhibited rights to express their views on social media may pose a great risk to the employer. The risks posed by social media misconduct will be discussed in the next chapter.

3.5 Summary:

The matter of ‘context’ is a recurring theme in the decisions of the courts, and an attempt has been made to follow a similar pattern in this submission. The broad issues of sociology and psychology that underpin human behaviour were initially considered. The focus narrowed and the rights which are most often in dispute, in respect of social media misconduct in the workplace, were then discussed. These were the rights to dignity, privacy and freedom of expression.

In the remaining chapters, the focus will narrow further, and the discussion will relate to matters exclusive to the workplace. In the next chapter, the discussion will relate to the risks posed to an employer as a result of employees’ social media misconduct.

Chapter 4:
Risks to the employer arising from social media misconduct

4.1 Introduction

The introduction of electronic communication tools into the workplace has changed the way that business is conducted. These tools provide an easy channel of communication and of access to information, but they also increase exposure to legal risks. As a result, employers may choose to increase the level of workplace monitoring, thus threatening an employee's privacy.[82]

Given that many people spend half (or more) of their waking lives at work, it is inevitable, that in utilising social media to share information about their personal lives, people will share information about their work lives as well.[83]

The increase in work outside the office has further blurred the boundary between work and home, public and private.[84]

In a survey of South African companies, 69% had experienced employees 'loafing' on the internet, 70% found employees accessing or sending discriminatory or sexually offensive jokes or pictures, and 15% cited incidents where employees violated copyright laws or posted defamatory material using the employer's computer resources.[85]

The employment relationship is characterised by an implied "duty of good faith, by the employee towards the employer."[86] An employee's duty to "act in good faith towards his or her employer is recognised as an implied term of an employment contract."[87]

---

[82] D Collier 'Workplace privacy in the cyber age' (2002) 23 *ILJ* 1743.
[83] G Pike 'Social media and the workplace' (2014) 31(9) *Information Today* .
[84] J Cavico 'Social media and employment at will: tort law and practical considerations for employees, managers and organizations' (2013) 11 *New Media and Mass Communication.*
[85] L Dancaster, 'Internet abuse: a survey of South African companies' (2001) 22 *ILJ* 862,872.
[86] Van Jaarsveld (note 2 above).
[87] *Sappi Novobord (Pty) Ltd v Bolleurs* 1998 (19) ILJ 784 (LAC) where the court stated *"It is an implied term of the contract of employment that the employee will act with good faith towards his employer and that he will serve his employer honestly and faithfully ….".*

A further aspect of the duty of good faith is that an employer enjoys the right to exercise control over the employee's activities during working hours; as such, an employee must show respect to his employer, and an employee must be obedient to his or her employer.[88]

Employee disrespect and/or disobedience may cause prejudice to the employer. The potential risks to the employer, arising from social media misconduct by employees, will now be investigated.

4.2 Vicarious liability

Employers being held vicariously liable for the conduct of employees may arise in several ways. These include employee acts of harassment, discrimination, defamatory statements, copyright infringements, and from unauthorised contract formation, all of which may arise from social media and electronic mail use.[89] The type of liability imposed on the employer depends on the type of employee misconduct, and the employer's liability may arise from criminal or civil proceedings. Criminal liability may arise where, for instance, employees view or are in possession of child pornography in the workplace in violation of the Film and Publications Board Act No 65 of 1996.

A company's employees are considered as insiders. In terms of the doctrine of vicarious liability, a company may be held liable for the acts or conduct of employees performed within the scope of their employment.[90] Historically, a company's own employees (or insiders) have been responsible for most of the security breaches, yet companies hold onto the outdated belief that the external threat is much more significant than the internal threat.[91]

The general rule in South Africa is that when a delict is committed, the perpetrator of the delict is personally liable for the loss arising from the wrongful conduct. With vicarious liability, however, another party may be held liable for the delict of the

[88] Van Jaarsveld (note 2 above; 654).
[89] V Etsebeth 'The growing expansion of vicarious liability in the information age (Part 1)' (2006) *Journal of South African Law* 564-565.
[90] Ibid 564 & 580.
[91] Ibid 566.

perpetrator that has caused loss to another party.[92] Liability, in this form, is called strict liability, or liability without fault.[93] Vicarious liability arises when there is a relationship between two persons, for example, a principal/agent relationship. For the purpose of this dissertation, the employer and employee relationship is the focus.

The principle whereby an employer may be held jointly and severally liable, with an employee, for the employee's wrongful acts committed in the course and scope of the employee's employment, was first expressed in the *Feldman (Pty) Ltd v Mall* case[94] wherein it was held:

> 'a master who does his work by the hand of a servant creates a risk of harm to others if the servant should prove to be negligent or inefficient or untrustworthy…. if the servant's acts in doing his master's work or his activities are incidental to or connected with it are carried out in a negligent or improper manner, so as to cause harm to a third party, the master is responsible for the harm."[95]

The rationale for the employer's liability is controversial. The risk or danger theory postulates that the work which is "entrusted to the employee creates certain risks of prejudice (the commission of delicts) for which the employer, on the grounds of fairness and justice, should be held liable as against prejudiced outsiders."[96]

There are three requirements for an employer to be vicariously liable for the delict of his employee: there must be an employer-employee relationship at the time of the commission of the delict, the employee must commit a delict causing loss to a third party, the employee must have been acting within the scope of his duties at the time that the delict was committed.[97]

It may happen that an employee's delictual conduct occurs while acting beyond the authority granted, not in furtherance of the employer's interests, For such cases, the

---

[92] Ibid 578.
[93] Neethling (note 53 above; 312).
[94] *Feldman (Pty) Ltd v Mall* 1945 AD 733.
[95] *Feldman supra.*
[96] Neethling (note 53 above; 312).
[97] Neethling (note 53 above; 313 & 314).

courts have developed the deviation rules. The courts will consider the degree of deviation to ascertain whether the employer may be vicariously liable.

In the *Grobler v Naspers Bpk*[98] case, the employee alleged that her employer had breached a legal duty, to its employees, to create and maintain a working environment in which, amongst other things, its employees were not sexually harassed by other employees in their working environment.[99] The court decided that an employer may be held vicariously liable where the working relationship created a risk of harassment or enhanced such a risk, and that the harassment took place in the employment relationship.[100] Therefore, employers may be held vicariously liable if there is a "sufficiently close connection between the wrongful acts of the perpetrator and the risk created by the enterprise."[101]

The sufficiently close connection test, as described in *Grobler,* is used in other legal jurisdictions, including Australia, New Zealand, and the UK.[102]

In the context of social media, the sufficiently close connection test may find application in a South African workplace where, for example, an employee views or disseminates pornographic or racist material from a work area that is also occupied by other employees. Employers need to guard against cyber-liability arising from social media use by their employees.

The employer and employee are jointly and severally liable for the delict and, though the victim has the option of pursuing a claim against the perpetrator, they often proceed against the employer because the latter has greater financial resources.

The employer may be held vicariously liable on several grounds as a result of social media use by the employees. These grounds will be considered next.

---

[98] *Grobler v Naspers Bpk* 2001 (4) SA 938 LC.
[99] *Grobler supra* at para 64.
[100] Etsebeth (note 89 above; 564,580 at 579).
[101] Etsebeth (note 89 above; 564 & 580).
[102] Etsebeth (note 89 above; 752).

4.3 Defamation

Defamation is the wrongful, intentional publication of words or behaviour concerning another person which has the effect of injuring his or her status, good name or reputation.[103] To succeed in an action for defamation, it is required to show unlawfulness, intention, publication, and impairment of the reputation of the complainant.

The publication requirement is satisfied if the words or conduct are made known or disclosed to at least one person, other than the plaintiff and the other person must be aware of the defamatory character or meaning of the words or conduct.[104] Publication will take place on the internet when the defamatory statement is read, seen or heard, and understood by the receiver.[105]

An employee's liability for defamation may result in vicarious liability for the company. A court may find that, in providing an employee with 'tools' to access the internet and email facilities, the employer is directly liable as a publisher or disseminator of the offending statement.[106]

Social media is a readily available tool for the dissemination of messages to an almost infinite number of people, it follows, therefore, that social media may be used to meet the 'publication' requirement that is necessary to prove defamatory conduct. Employers may be held vicariously liable where employees, acting in the course of his or her employment, post defamatory material or send defamatory communications via social media.

The publication requirement will be met where, for example, a defamatory Facebook post is read and understood by any other person aside from the party defamed.

In *CWU v Mobile Telephone Networks (Pty) Ltd,*[107] an employee circulated emails in which he made allegations of corruption and bias against the employer's

[103] Neethling (note 53 above; 280).
[104] Neethling (note 53 above; 281).
[105] Etsebeth (note 89 above; 756).
[106] Etsebeth (note 89 above; 757).
[107] *CWU v Mobile Telephone Networks (Pty) Ltd* 2003 (8) BLLR 741 (LC).

management. MTN charged the worker for having used company tools to send messages that exposed the employer to liability by its clients. The Labour Court found that the worker's conduct in sending the emails exposed the employer to reputational damage and, further, it exposed the employer to potential vicarious liability claims.

The risks to the employer, for being held vicariously liable for the defamatory social media posts of its employees, are real. The existence of these risks provides a sound reason to argue in favour of the monitoring of employees' social media communications.

4.4 Harassment and discrimination

Where an employer does not take steps to prevent the circulation of sexually and/or racially offensive material, this will result in discrimination and intimidation in the workplace, which may result in vicarious liability for the employer.[108]

The Code of Good Practice on the Handling of Sexual Harassment cases defines harassment as conduct that is either, physical, verbal, or non-verbal. Item 4(1)(c) includes, as a form of non-verbal conduct, the "unwelcome display of sexually explicit pictures and objects." Pornographic material can be directly or indirectly offensive. Directly is where the pornographic material may be attached to an electronic message and sent to co-workers, and indirectly where an uncomfortable working environment is created by employees downloading or viewing pornographic material at their workstations.[109] In the *Bamford v Energizer*[110] case, employees were dismissed for distributing pornography using the employer's computer system in violation of a company rule that prohibited such conduct.[111] The Arbitrator noted that while such conduct may be carried out in private, it could not be condoned in workplaces because employers could potentially be held vicariously liable for the offensive conduct of the perpetrators.[112]

---

[108] Etsebeth (note 89 above; 761).
[109] Etsebeth(note 89 above; 752).
[110] *Bamford and Others v Energizer* 2001 (12) BALR 1251 (P).
[111] Etsebeth (note 89 above; 760).
[112] V Etsebeth 'The growing expansion of vicarious liability in the information age (Part 2)' (2006, *Journal of South African Law.*

In *Cronje v Toyota Marketing,*[113] the employee's dismissal arose from his distribution of racist and/or inflammatory material, using a system that belonged to the company, while he was at work. The dismissal was upheld, and the CCMA remarked that the mail that was circulated was crude and offensive, and depicted black people as human beings of lesser intelligence and low morality.

4.5 Breach of copyright

Access to the world wide web[114] provides everyone with the ability and opportunity to download articles, journals, songs, photographs and various other data. However, if an employee downloads material that is protected by copyright, and forwards it to another, this will constitute copyright infringement.[115]

Copyright protection in South Africa is provided by the Copyright Act No. 98 of 1978. The law of copyright applies as equally in the real world as in cyberspace. Publications in electronic or digital forms (books, journals, magazines, and other forms of written publications) are protected in accordance with the law of copyright.[116]

Therefore, if employees are granted access to the internet by a business organisation, copyright infringement becomes a risk and should become a concern for the company.

4.6 Inadvertent formation of contracts

The Electronic Communications and Transactions Act 25 of 2002, discussed in paragraph 6.2.4 below, provides that "an agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages."[117] All contracts must comply with the common law requirements of consensus, contractual capacity, legality, the possibility of performance and the prescribed formalities.[118] In terms of section 22, an agreement concluded between

---

[113] *Cronje v Toyota Marketing* 2001 (3) BALR 213 (CCMA).
[114] "Means an information browsing framework that allows a user to locate and access information stored on a remote computer and to follow references from one computer to related information on another computer ": Electronic Communications and Transactions Act No 25 of 2002, S1 (definitions).
[115] Etsebeth (note 112 above; 761).
[116] Etsebeth (note 112 above).
[117] Electronic Communications and Transactions Act No 25 of 2002, section 22.
[118] Etsebeth (note 112 above; 763).

parties by means of data messages is concluded at the time and place where the acceptance of the offer was received by the offeror. Section 23(1)(b) provides that an offer will be deemed to have been received by the offeror when the complete data messages have infiltrated the information system of the offeror, and the offeror is able to retrieve or reproduce the data message.[119]

An employee, who inadvertently forms a contract via electronic mail, with another company, binds the employer to the contract. "If a recipient of a document has reasonable grounds for believing that the person sending the document has the authority to offer and agree to the undertakings and statements contained therein, and accepts these unconditionally, then by law the contract is, in all likelihood, prima facie valid and enforceable." [120]

Etsebeth[121] holds the view that the most effective method for a company to guard against the inadvertent formation of contracts would be to implement content monitoring software.

4.7 Productivity and efficiency

Dancaster's article[122] relating to internet abuse within South African companies revealed that a significant number of employees engage, during work hours, in non-work-related activities. More than two-thirds of the companies surveyed experienced 'cyberloafing' by employees. Where employees use employer-provided facilities to engage in activities not related to work, it is easy to see that assigned work will not be carried out and there will be a resultant drop in productivity.

The primary reasons for employers wanting to monitor internet and social media usage are to determine whether employees are surfing the internet instead of doing assigned work, whether employee activities are clogging the corporate network and

[119] Etsebeth (note 112 above).
[120] Etsebeth (note 112 above; 764).
[121] Etsebeth (note 112 above; 764).
[122] Dancaster (note 85 above; 862 & 872).

using up computer power needed for corporate activities, and whether company resources are being used excessively for personal gain.[123]

Approximately one hundred and sixty Johannesburg Stock Exchange-listed companies responded to the survey analysed by Dancaster and of these, 69% experienced employee internet loafing, 65% experienced degraded system performance, 70% found employees downloading and sending discriminatory and sexually offensive jokes and pictures. Of the different types of internet abuse mentioned, 84% of the respondent companies experienced at least one of the abuses.[124]

Most respondent companies had taken steps to address the problem. The steps most frequently used by the companies were to screen or block sites that were not approved, implementing internet acceptable use policies (IAUP's), monitoring employee's internet and email usage, and disciplining employees for internet and email abuse.[125]

The survey revealed that most companies were aware of the risks posed to the organisation if they allowed employees unrestricted internet and social media use. Consequently, most had implemented some form of acceptable internet use policy.

4.8 Summary

Allowing employees open and unmonitored access to a computer and social media facilities will, almost certainly, manifest itself in compromised productivity and compromised efficiency for the organisation and more importantly, as explained above, it leaves the organisation exposed to legal liability. On the other hand, excessive monitoring of employee activity may sow discord in the workplace, cause tensions in the employer and employee relationship, and will in equal measure contribute to decreased productivity and efficiency. How is a balance to be struck?

[123] Dancaster (note 85 above; 863).
[124] Dancaster (note 85 above; 866).
[125] Dancaster (note 85 above; 866).

The answer lies, in part, with section 23(1) of the Constitution.[126] This provision reads "Everyone has the right to fair labour practices." The term 'everyone' is interpreted to include both the employer and employee. Analysis of the law in foreign jurisdictions shows that the courts have come to the aid of employers where employee abuse of social media and electronic communications has caused harm to an organisation.

Section 39(1)(c) of the Constitution reads "When interpreting the Bill of Rights, a court, tribunal or forum may consider foreign law." Foreign law, although not binding on courts and tribunals, nonetheless has persuasive authority.

The next chapter discusses social media misconduct in the context of foreign law, and how it has been addressed in some of the leading democracies of the world. The discussion will include an analysis of the applicable laws, decided cases, and the contributions of academics.

[126] Act 108 of 1996.

Chapter 5:
Foreign Law

5.1 Introduction

Countries of the world exist in what is sometimes referred to as a global village. The main characteristic of a global village is that its members take advantage of the skills and expertise of fellow members, and they adopt international best practices. Advances in knowledge and practices in the fields of engineering, architecture, medical sciences, communications and other spheres of activity are often shared by members of the global village.

South African law is not unaffected by developments outside of its borders and, as stated in the previous chapter, section 39(1)(c) of the Constitution permits judicial officials to take foreign law into consideration.

South Africa enjoys relatively cordial relations with most countries of the world. The world's nations, however, are not homogeneous in the relationships that exist between governments and their citizens, and not all countries emphasise the democratic values that are found in the South African Constitution.[127]

This chapter will examine both the law and decided cases, relating to social media misconduct, in five countries: the USA, Canada, UK, Australia, and New Zealand. These countries have been chosen because they all have rich histories of having aspired to, or having fiercely protected, some of the fundamental rights reflected in South Africa's Constitution.

5.2 The USA

5.2.1 Introduction – Public Sector Employee

[127] The preamble of Act 108 of 1996 contains provisions that reflect South Africa's aspirations towards "establishing a society based on democratic values, social justice and fundamental rights".

The 1st and 4th amendments of the American Constitution[128] are especially important for the purposes of this dissertation. The 1st amendment[129] includes protection for freedom of speech, and the 4th amendment[130] includes the protection of citizens' privacy rights. The provisions of the American Constitution find application only in respect of relations between the government and public-sector employees. The constitutional provisions, though of persuasive value, find no application in private sector employer and employee relations.

A private employer does not have a responsibility to respect an employee's 1st Amendment rights (with a few exceptions, such as concerted speech related to working conditions, or speech relating to policy violations including discrimination or harassment).[131] Aside from these exceptions, private sector employers have the right to tell employees not to talk about issues or not to undertake practices.[132]

For public sector employees to invoke the 1st Amendment protection, their speech needs to meet a three-pronged test – first, the speech must touch on a matter of public concern; second, the speech must fall outside of the employee's job duties; finally, the employee's interest in free speech must outweigh the government's interest in efficient and effective provision of services.[133]

American courts, when considering 4th Amendment disputes, adopt a balancing test that looks at the employee's privacy rights in relation to governmental interests – the reasonableness of a search, for work-related purposes, is an important consideration.[134]

---

[128] The Constitution of the United States, signed on 17th September 1787. The 1st and 4th amendments were signed in 1791.
[129] "Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances".
[130] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".
[131] W Jacobson & S Tufts 'To post or not to post: employee rights and social media' (2014) 33(1) *Review of Public Personnel Administration* 84-107.
[132] Ibid at 91.
[133] Ibid.
[134] Ibid at 93.

Employees' off-duty conduct, which includes social media postings, can have a direct impact on the employment relationship. Where there is a connection between the behaviour and the efficiency of the public service, the off-duty conduct becomes subject to regulation and inspection.[135]

5.2.2 Electronic Communications Privacy Act of 1986 ('ECPA')

ECPA was enacted by the US Congress to extend government restrictions on wiretaps to include transmissions of electronic data by computer. Title 1 is called the Wiretap Act,[136] and it restricts interception of communications while in transit. Title 2 is known as the Stored Communications Act[137] and restricts the disclosure of communications stored on a server, or in the cloud. Title 3 is called the Pen Register Statute,[138] and it restricts the government's ability to obtain non-content information (such as a list of phone numbers dialled).

The equivalent statutes in South Africa, which will be discussed below, are the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 for the Wiretap Act, and the Protection of Personal Information Act 4 of 2013 for the Stored Communications Act.

The Wiretap Act places prohibitions on the interception or attempts to intercept wire or electronic communications, disclosing or attempting to disclose the intercepted communication, or using the content of the intercepted communication.[139] It follows, therefore, that an employer who monitors or intercepts an employee's electronic or social media communications, may be fined or imprisoned.[140] While the Wiretap Act relates to communications in transit, the Stored Communications Act finds application where communications are in storage.

There are important exceptions in ECPA. Employers may access the stored communications of employees who use the employer's systems, the business

---

[135] Ibid.
[136] Title 1, Wiretap Act, 18 U.S.C 2510-2522
[137] Title 2, Stored Communications Act ,18 U.S.C 2701-2712
[138] Title 3, Pen Registers and Track and Trap Devices Act, U.S.C 3121-3127
[139] 18 U.S.C. 2511 (1).
[140] 18 U.S.C. 2511 (4)(a).

extension exception allows employers to monitor employees' communications made in the ordinary course of business, and employees may give consent to the employer to have their communications intercepted. In these cases, the employer may avoid liability under ECPA.[141]

5.2.3 The National Labor Relations Act (NLRA)[142]

The NLRA is a federal law that grants employees the right to form or join unions, and to engage in protected concerted activities.[143] Concerted activities relate to employee conduct that addresses or strives towards improving their working conditions. The "National Labor Relations Board" (NLRB) is an agency created by the Federal Government to enforce the NLRA.

The potential negative implications of social media have caused concern among employers. As a result, employers began to institute policies to address employee social media use and have included in their policies the nature of what employees are permitted to post. Some policies were deemed by the NLRB as being overbroad or having the effect of violating the rights of workers' to engage in concerted activities.[144] Concerted activities are those activities engaged in, with or on the authority of other employees, and not solely by and on behalf of the employee himself.[145] In the South African context, concerted activities are synonymous with trade union activities that enjoy protection under the Labour Relations Act.

---

[141] F J Cavico 'Social media and the workplace: legal, ethical, and practical considerations for management' (2013) 12 *Journal of Law, Policy and Globalization*

[142] National Labor Relations Act 29 U.S.C 151-169 (2012).

[143] Section 7 reads: "Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, and shall also have the right to refrain from any or all such activities except to the extent that such right may be affected by an agreement requiring membership in a labor organization as a condition of employment as authorized in section 8(a)(3) [section 158(a)(3)".

[144] Ireton (note 11 above; 144-179).

[145] Ireton (note 11 above; 147).

Concerted activities are protected by section 8(1)(a)[146] of the NLRA. To determine section 8 violations, the courts consider whether workplace rules "would reasonably tend to chill[147] employees in exercising their Section 7 rights."[148]

Sections 7 and 8 protect employees who engage in protected concerted activity if they choose to communicate online, using social media.[149] While section 7 protects employees' collective criticism of their employer, employers may lawfully restrict their employees from making defamatory comments, or comments which are deliberately or maliciously false.[150]

Most American private sector workers are employed on an "employment-at-will" basis, and they enjoy little job security. Under this doctrine, an employer can terminate an employee (unless the employee has a contract for a fixed term) at any time, for any reason, or no reason at all.[151] The employment-at-will doctrine resembles South Africa's common law approach to employment relations. The doctrine will not withstand constitutional and LRA scrutiny in South Africa where the emphasis is on 'fair' labour practises.

In the USA, an employee may lawfully be dismissed for social media postings, except if the postings related to concerted activities. Employees enjoy protection if they are able to show a link between the postings and a legal doctrine (such as contained in the "Civil Rights Act of 1964," "Age Discrimination in Employment Act" or the "Americans with Disabilities Act)."[152]

5.2.4 Court decisions

This sub-section concludes by looking at several American court decisions. In *O'Connor v Ortega,*[153] the 4th Amendment privacy protection in the workplace was

[146] S8(a)(1) reads: (a) "It shall be an unfair labor practice for an employer-- (1) to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in section 7".
[147] The courts interpret "chill "to mean inducing a sense of caution and timidity.
[148] *Lafayette Park Hotel,* 326 N.L.R.B. 824, 825 (1998).
[149] Cavico (note 141 above).
[150] Ireton (note 11 above; 144-179 at 149).
[151] A C McGinley & R P McGinley-Stempel 'Beyond the water cooler: speech and the workplace in an era of social media' (2012) 30(1) *Hofstra Labor and Employment Law Journal*
[152] Ireton (note 11 above; 144-179).
[153] *O'Connor v Ortega* 480 U.S. 709 (1987).

considered. Hospital officials had conducted a search of the office of the employee (who was employed as a physician and psychiatrist) and removed items of a personal nature from his workstation and filing cabinets. These were subsequently used in a disciplinary hearing against the employee and led to his dismissal. The employee filed an action alleging that, in searching his office, the employer violated his 4th Amendment rights. The Supreme Court pronounced that the "operational realities of the workplace may make some public employees expectations of privacy unreasonable" and "the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." Finally, the court said that government searches to retrieve work-related materials or to investigate violations of workplace rules – searches of the sort that are regarded as reasonable and normal in the private-employer context – do not violate the 4th Amendment. The US Supreme Court's pronouncements on the "reasonable expectation of privacy" closely resemble the words of the court in the South African case of *Bernstein v Bester.*[154]

In *Smyth v Pillsbury Co,*[155] the employee's claim that his right to privacy was violated, when his emails were intercepted by the employer, was not accepted by the court. Smyth had sent threatening emails to his supervisor and was dismissed for his conduct. The court found that there was no reasonable expectation of privacy in voluntary mail communications made through the company system.

Five employees in *Hispanics United of Buffalo, Inc and Carlos Ortiz*[156] were fired for Facebook comments, purportedly for bullying a co-worker. The NLRB found that the employees' postings fell "within the protection of section 7 of the NLRA. The action of an individual is concerted if its object is to induce group action." The decision is important also because union membership is not a requirement to obtain NLRA protection.[157] Similarly, in South Africa, union membership is not a requirement to enjoy the rights and protections of the LRA and other labour law.

---

[154] *Bernstein .supra*
[155] *Smyth v Pillsbury Co* 914 F.Supp. 97 (E.D. Pa 1996).
[156] *Hispanics United of Buffalo, Inc. and Carlos Ortiz* NLRB Case 03-CA-027872 Dec 2012.
[157] C N O'Brien 'The top ten NLRB cases on facebook firings and employer social media policies' (2014) 92(2) *Oregon Law Review* 337-353.

In *Costco Wholesale Corp,*[158] the NLRB found the organisation's social media policy ('SMP') problematic in that it was a violation of section 8(1)(a) of the NLRA as the provisions in the SMP were overboard and tended to 'chill' employees in the exercise of their section 7 rights.[159] The NLRB instructed the employer to revise its social media policy. The approach of the NLRB is likely to be followed in South Africa where, for example, employers seek to prohibit employees from engaging in trade union activities via social media.

The case of *Karl Knauz Motors Inc*[160] involved an employee, a motor vehicle salesman, being dismissed for posts that he had made on Facebook. The employee posted comments in respect of the poor quality of food offered to potential buyers attending a new BMW launch. He complained that the poor hospitality would adversely affect car sales and that he would earn lower sales commissions. The employee posted pictures of the food offered (hot dogs and chips). He then also posted pictures of an accident that occurred at an adjoining Land Rover sales site, also owned by his employer. The NLRB held that segments of the employee handbook violated section 8(1)(a) of the NLRA, in that it tended to chill[161] employees in the exercise of their statutory section 7 rights. However, the employee's dismissal was found to be fair, as the dismissal was based on his unprotected Facebook postings relating to the Land Rover site accident.

In *Design Technology Group L.L.C d/b/a Bettie Page Clothing,*[162] the NLRB confirmed that employees who discuss their remuneration, their work hours and their work conditions on Facebook, are entitled to section 7 NLRA protection. In addition to ordering the reinstatement of the three dismissed workers, the NLRB ordered the employer to remove the workplace rule that forbade employees from disclosing their remuneration to fellow employees or from disclosing it to any other party. South African employers should similarly exercise caution and guard against including provisions in their social media policies that infringe the legitimate rights of employees.

---

[158] *Costco Wholesale Corp.,* 358 NLRB, No. 106, 2012 WL.
[159] O'Brien (note 157 above).
[160] *Karl Knauz Motors, Inc.,* 358 NLRB. No.164, 2012 WL 4482841 Sept 2012.
[161] Note 147 above.
[162] *Design Technology Group., L.L.C., d/b/a Bettie Page Clothing,* 359 NLRB No.96, 2013.

In concluding this section, it is noted that USA law protects both the interests of employers and employees. Section 7 and Section 8(1)(a) of the NLRA protects the interests of employees when they engage in social media activities aimed at advancing their collective interests.[163] The interests of employers are given protection by the provisions of ECPA where employees' communications may be accessed or monitored in certain circumstances.[164] The significant difference between workplace law in the USA and South Africa is that, whereas the employment-at-will doctrine permits USA employers to dismiss workers without providing reasons,[165] the LRA requires South African employers to justify employee dismissals by following a fair procedure and, in addition, providing a fair reason for the dismissal.[166]

5.3 Canada

5.3.1 Introduction

Because of the geographical proximity of Canada to the USA, it may be expected that legal developments in the one country would influence similar developments in the other. Morgan[167] writes that, in answer to the question of whether employers may legally monitor employee internet use, Canadian legal commentators have responded unequivocally: employers may monitor under any circumstances, as they see fit. The response seems to be based on two premises, both taken from American jurisprudence on the matter.[168] However, as Morgan goes on to observe, "it will be imprudent to assume that Canadian Courts will follow American jurisprudence on the subject since significant differences exist between applicable American and Canadian privacy legislation."[169]

There are two important reasons. The first reason is that the judiciary and legislature in Canada are leaning towards a greater protection of individual rights. Further, judicial interpretation of privacy principles arising from the Canadian Charter indicates that employees may expect a reasonable expectation of privacy in the workplace,

[163] Defamatory or malicious social media content are not protected.
[164] Cavico (note 141 above).
[165] McGinley (note 151 above).
[166] The Labour Relations Act 66 of 1995; section 188.
[167] C Morgan 'Employer monitoring of employee electronic mail and internet use' (1999) 44 *McGill Law Journal* 849-902.
[168] Ibid 849.
[169] Ibid.

and employer monitoring must be reasonable and performed in accordance with the employee's consent.[170]

5.3.2 The Canadian Charter of Rights and Freedom

Privacy protection is granted to citizens under section 8 of the Canadian Charter.[171] Although the provisions of the Charter apply only to government action, therefore, not being applicable in disputes between private parties, a number of Canadian Supreme Court decisions have left room for an indirect impact of the Canadian Charter on private disputes.[172] In *RWDSU v Dolphin Delivery Ltd,*[173] the Supreme Court held that "while the Canadian Charter does not apply to disputes between private parties, courts ought to apply and develop principles of common law in a manner consistent with the fundamental values enshrined in the Constitution."[174]

5.3.3 Federal and provincial privacy legislation

The Federal structure of Canada has an impact on the legislative framework. In terms of the provisions of section 91 of the Constitution, the federal government is assigned jurisdiction over certain matters (such as the military, currency and coinage, banking, postal service); and further, in terms of section 92, the provincial legislatures may exclusively make laws, amongst others, in relation to municipal institutions in the province, shop and other licenses, property and civil rights within the province.[175]

The resultant effect is that, in respect of privacy rights, the Federal Government has enacted legislation regarding matters falling within its core competency (such as banks, criminal law, Canada Post) and the provincial governments have enacted legislation in respect of their jurisdiction over matters concerning property and civil rights.[176]

In the context of the workplace, employers who view the social media sites of employees, whether in the context of pre-employment screening or to obtain

---

[170] Ibid at 854.
[171] Section 8 reads: *"Everyone has the right to be secure against unreasonable search or seizure ".*
[172] Morgan (note 167 above at 863).
[173] *RWDSU v Dolphin Delivery Ltd* 1986 (2) SCR 573.
[174] Morgan (note 167 above).
[175] Constitution Act 1867.
[176] Morgan (note 167 above at 873).

evidence of employee misconduct, may fall foul of federal or provincial privacy legislation.

5.3.4 Court Decisions

In *R v Cole,*[177] the Supreme Court in Canada pronounced on the employees' rights to privacy with work equipment. In answering whether Mr Cole had a reasonable expectation of privacy in his employer-provided laptop, the court held that (regardless of who owns the equipment) the personal information on computers enjoys the protection given by section 8 of the Canadian Charter. Personal information reveals details about a person's private life to which there is a reasonable expectation of privacy. However, the court ruled that the improperly obtained evidence by the employer was admissible, as the matter related to child pornography. The "reasonable expectation of privacy" doctrine, as applied in the USA in *Ortega* and in South Africa in *Bernstein*, is echoed in this Canadian Supreme Court decision.

Lougheed Imports Ltd. (c.o.b. West Coast Mazda) (Re)[178] involved two employees who were dismissed for making Facebook posts that contained offensive comments about their managers. The Labour Relations Board agreed with the employer's contention that the Facebook posts constituted proper cause for termination of their employment.

In *Chatham-Kent (Municipality) National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 127(Clarke Grievance),*[179] Jessica Clarke was a caregiver at a home for the elderly. She created a blog, accessible to anyone with internet access, where she made inappropriate comments, published photographs, and posted confidential information about the residents entrusted to her care. In addition, she made disparaging remarks about her co-workers and management. The employer dismissed Ms Clarke for a serious breach of confidentiality in circumstances where there was an elevated duty to ensure

[177] *R v Cole* 2012 SCC 53 (2012) 3 SCR 34.
[178] *Lougheed Imports Ltd. (c.o.b. West Coast Mazda) (Re),* (2010) B.C.L.R.B.D. No.190 ("Lougheed Imports ").
[179] *Chatham-Kent (Municipality) v National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 127 (Clarke Grievance),* (2007) O.L.A.A. No.135 ("Chatham-Kent").

privacy. The arbitrator agreed with the employer and deemed the employee's dismissal fair.

Airline pilot John Wyndels, in *Wasaya Airways LP v Airline Pilots Assn., International (Wyndels Grievance),*[180] was dismissed for off-duty Facebook comments he made regarding the airline owners and passengers. The employer contended that the comments, although made off-duty, were derogatory and offensive, and harmed the airline's reputation. The arbitrator found that the employee's misconduct was such that it rendered the employment relationship untenable.

In *Teck Coal v U.M.W.A. Local 1656,*[181] Kyle Norman was dismissed by Teck Coal because he was often absent from work and had allegedly lied about the reasons for his absence. Norman was absent from work for 282 hours over a nine-month period. The average absenteeism rate for employees at the plant was 20 hours. The employee's union argued that the dismissal was unfair, stating that Norman suffered from a mental disability which Teck was legally bound to accommodate. The arbitrator ruled that Norman's dismissal was just and reasonable and that the Union was unable to establish that Teck had discriminated against Norman on the grounds of mental disability.

In coming to his determination, the arbitrator referenced, among other things, that Norman announced on his Facebook page that he was "in the City, ready to party" when he had told Teck that he was unable to come to work. This announcement not only reduced the employee's credibility but also pointed to his true emotional state.

In the case of *Re Walder,*[182] the British Columbia Employment Standards Tribunal (the 'BCEST'), Rebecca Walder complained that the employer dismissed her because of her pregnancy and/or maternity leave. The BCEST found that Walder had been dismissed for just cause. The reason for the termination was that Walder had

[180] *Wasaya Airways LP v Airline Pilots Assn., International (Wyndels Grievance),* (2010) C.L.A.D., No.297, 195 L.A.C. (4TH) 1 ("Wasaya ").
[181] *Teck Coal v U.M.W.A. Local 1656*, (2010) A.W.L.D. 2589.
[182] *Re Walder* (2010) B.C.E.S.T.D. No.113.

posted, on a fellow employee's Facebook page, an allegation that the other employee had stolen her job.

It was observed above[183] that the judicial and legislative trends in Canada show a leaning towards greater protection of individual rights, and that employees enjoy a reasonable expectation of privacy in the workplace. Employer monitoring must be reasonable and must be performed with the employee's consent. Analysis of court decisions reveals that the Canadian courts have condoned the censuring, including dismissal, of employees who engage in malfeasant social media conduct that has the effect of causing harm to an organization, or which may sow discord in the workplace.

5.4 The United Kingdom, Australia, and New Zealand

The chapter on foreign law concludes with a discussion of the law, insofar as it relates to misconduct in the workplace arising from social media usage, as it is applied in the United Kingdom, Australia, and New Zealand.

5.4.1 The UK

In the *Copland v United Kingdom*[184] case, the European Court of Human Rights (ECHR) ruled that the United Kingdom had violated Article 8 of the ECHR[185] for the manner in which they had monitored Ms Copland's telephone calls, electronic mail and internet use.[186] The Court ruled that, in the absence of a notification that communications may be monitored, the employee had a reasonable expectation of privacy in respect of her communications.

The Court referred to the Regulation of Investigatory Powers Act 2000[187] which sets out the circumstances in which employers may record or monitor an employee's communications without the consent of the employee or other parties to the communication. In such circumstances, employers are required to give prior

[183] Supra note 166.
[184] *Copland v United Kingdom* (2007) ECHR 253.
[185] European Convention of Human Rights (1950).
[186] Ms Copland worked for Carmarthenshire College, a State administered body. The Deputy Principal of the College requested that Ms Copland's telephone, internet, and email usage be monitored, to determine whether there was excessive personal use. The College did not, at the time, have a policy on the monitoring of employee communications.
[187] RIPA is an act which regulates the power of public bodies to carry out surveillance and investigation, including the interception of communications.

notification, to employees, that their communications may be intercepted.[188] However, the pronouncements[189] of the court led certain legal commentators to hold the view that, in certain circumstances, employers may monitor employee communications.

In the *Smith v Trafford Housing Trust*[190] case, the employee was demoted for making known, on Facebook, his opposition on gay marriages. Mr Smith's Facebook profile page identified him as a manager at the Trust. The employer held that readers would conclude that the Trust shared the employee's anti-gay sentiments. The judge dismissed the employer's argument. The court held that Mr Smith's Facebook page was a personal web page, that no reasonable reader would conclude that the postings reflected the views of the Trust and that the identification of Smith's employment at the Trust was in the context of personal information that appeared alongside other information such as his school, football team, and motor cars. The *Smith* case shows that, while workplace rules may restrict private social media use, such restrictions may not serve to negate the freedom of speech. The recent *Cantamessa and Edcon Group*[191] decision in South Africa mirrors the findings of the UK court in this case.

The House of Lords had to balance Naomi Campbell's privacy rights, against a newspaper's right to freedom of expression. The Mirror newspaper had published a series of articles relating to Ms Campbell's drug addiction and her treatment.[192] The Court considered Article 8 (privacy) and Article 10 (freedom of expression) of the ECHR. The court held by a majority, with two judges dissenting, that Campbell's privacy rights trumped the Mirror's right to freedom of expression.

In conclusion, the *Copland* case illustrates the need, where an employer intends monitoring the communications of an employee, to first obtain the employee's consent. In *Smith,* the court tempered the overzealous reaction of the employer who

[188] *Copland supra* at para 20.
[189] *Copland supra* para 48 where the court said "The Court would not exclude that the monitoring of an employee's use of a telephone, e-mail or internet at the place of work may be considered "necessary in a democratic society" in certain situations in pursuit of a legitimate aim "
[190] *Smith v Trafford Housing Trust* (2012) EWHC 3221.
[191] *Cantamessa and Edcon Group* 2017 (38) ILJ 1909 (CCMA).
[192] *Campbell v Mirror Group of Newspapers* (2004) UKHL 22.

had demoted an employee because the latter had mentioned the name of his employer on his Facebook profile. The dissenting judgements in the *Campbell* case illustrate that there is, very often, an almost indistinguishable line that separates freedom of expression from the invasion of privacy.

5.4.2 Australia

The Fair Works Act 2009 governs workplace relations in Australia. The Fair Work Commission ('FWC') oversees adherence to the Act in Australian workplaces.

In the *Damian O'Keefe v William Muir's (Pty) Ltd t/a Troy Williams The Good Guys*[193] matter, the FWC upheld the employer's dismissal of O'Keefe because the employee had made Facebook posts in which he threatened a manager. Although the comments were posted outside of work hours, they were viewed by co-workers, and the FWC held that the separation between home and work is now less pronounced than it once used to be.[194] The dismissal was considered to be fair.[195]

In *Ms Tamicka Louise Dover-Ray v Real Insurance (Pty) Ltd,*[196] the employee posted a lengthy blog, on the social networking site, Myspace, in which she accused the employer's management of corruption.[197] The employee was dismissed primarily for the offensive blog which aimed to damage Real's reputation.[198] The FWC held that the employee's conduct in publishing the blog was a valid reason for the termination of her employment.[199]

In the *Miss Sally-Ann Fitzgerald v Dianna Smith t/a Escape Hair Design*[200] matter, although the FWC found that the employee's comments made on Facebook were not valid reasons for her dismissal,[201] the FWC held that posting comments about an

---

[193] *Damian O'Keefe v William Muir's (Pty) Ltd t/a Troy Williams The Good Guys* (2011) FWA 5311.
[194] *Damian O'Keefe supra* at para 43.
[195] *Damian O'Keefe supra* at para 49 where the FWC stated "while it is accepted that the applicant was frustrated by his unresolved pay issues, the manner in which he ultimately dealt with the issue warranted his dismissal for misconduct".
[196] *Ms Tamicka Louise Dover-Ray v. Real Insurance (Pty) Ltd* (2010) FWA 8544.
[197] *Ms Tamicka Louise Dover-Ray supra* at para 22.
[198] *Ms Tamicka Louise Dover-Ray supra* at para 40.
[199] *Ms Tamicka Louise Dover-Ray supra* at para 62.
[200] *Sally-Ann Fitzgerald v. Dianna Smith t/a Escape Hair Design* (2010) FWA 7358.
[201] *Sally-Ann Fitzgerald supra* at para 66.

employer on a website (Facebook) that can be seen by an uncontrollable number of people is no longer a private matter but a public comment[202] and also "it would be foolish of employees to think they may say as they wish on their Facebook page with total immunity from any consequences."[203] In *Sedick and another and Krisray (Pty) Ltd,*[204] the CCMA was presented with similar facts and reached a decision similar to the FWC in the *Sally-Ann* matter.

5.4.3 New Zealand

The New Zealand Bill of Rights ('NZBOR')[205] provides for the freedom of expression,[206] but it makes no provision for privacy. The invasion of privacy forms part of the common law [207] and is protected by other means (such as trespass, defamation, breach of confidence, nuisance),[208] and is implicitly protected by sections 5 and 21 of the NZBOR.[209] Invasion of privacy is actionable as a tort where information or material is published in respect of which the plaintiff has a reasonable expectation of privacy.[210] The scope of privacy protection should not exceed such limits on the freedom of expression as is justified in a free and democratic society.[211]

The Employment Relations Authority (ERA) that was established in terms of the Employment Relations Act[212] helps to resolve employment-related problems.

In *Dandi Wang v New Zealand Chinese Television Ltd,*[213] the employee approached the ERA with a claim alleging her unfair dismissal by the employer. She confirmed that, after a dispute with her manager, she had published numerous abusive comments on social media site WeChat. The comments were viewable by co-

---

[202] *Sally-Ann Fitzgerald supra* at para 50.
[203] *Sally-Ann Fitzgerald supra* at para 52.
[204] *Sedick & another and Krisray (Pty) Ltd* 2011 (32) ILJ 752 (CCMA). See also Fredericks v Jo Barkett Fashion (2011) JOL 27923 (CCMA).
[205] New Zealand Bill of Rights Act No. 109 of 1990.
[206] Section 14 of NZBOR.
[207] K Evans 'Hosking v runting balancing rights in a privacy tort' (2004) 28 *Privacy Law and Policy Reporter*
[208] S Penk & R Tobin *Privacy Law in New Zealand* 2 ed (2016).
[209] Section 5 relates to limitations of rights, and Section 21 relates to unreasonable searches and seizures.
[210] A Roos 'Personal data protection in new zealand: lessons for south africa? (2008) 4 *PER.*
[211] *Hosking v Runting* (2005) 1 NZLR 1 32 (CA).
[212] Employment Relations Act No.24 of 2000.
[213] *Dandi Wang v New Zealand Chinese Television Ltd* (2015) NZERA Auckland 32.

workers.[214] The ERA held that Ms Wang had not acted in good faith when she posted the communications on WeChat and that there was contributory fault by her. As a result, the remedies granted to her were reduced by 20%.[215]

In *Rachel Blylevens v Kidicorp Limited,*[216] the employee was charged with misconduct and subsequently dismissed for her Facebook comments. She maintained that she was exercising her right to freedom of speech when she posted adverse comments about her employer, and she ignored the employer's request to remove the Facebook comments.[217] The ERA concluded that Ms Blyleven's dismissal was "within the range of appropriate responses available to a fair and reasonable employer."[218] Ms Blyleven's unjustified dismissal claim failed.

5.5 Summary

Space constraints prevent analysis of how other foreign jurisdictions, aside from those discussed above; approach the matter of social media misconduct in the workplace. The matter of how the subject matter is handled by progressive countries in Europe, Asia, and Africa will make for informative reading.

Social media misconduct cases are determined by courts and tribunals, in a particular jurisdiction, after having had regard for considerations that are unique to that specific jurisdiction. These considerations will include: is there a constitution and, if yes, does it apply vertically, or does it apply vertically and also horizontally?; does the Bill of Rights, if there is one, protect both privacy rights and freedom of expression or, does it protect only freedom of expression as in the NZBOR?; have laws been enacted that may have a bearing on the monitoring and interception of employee communications?; are there laws that govern the protection of informational privacy and, if yes, what is its impact on the workplace?; what is the jurisdiction's approach to privacy and freedom of speech – is it a value enshrined in the constitution, or has it been developed by their common law, or is the approach a combination of both?; have labour laws been enacted to incorporate equity in labour relationships?

---

[214] *Dandi Wang* at para 18.
[215] *Dandi Wang supra*.
[216] *Rachel Blylevens v. Kidicorp Limited* (2014) NZERA Auckland 373.
[217] *Rachel Blylevens supra* at para 74.
[218] *Rachel Blylevens supra* at para 81.

From a South African perspective, reference to foreign court decisions may, very often, be of anecdotal value only. While the workplace conduct of employees in foreign jurisdictions may resemble that of their counterparts in South Africa, the final decisions of the courts and tribunals will be based entirely on the provisions and the developed law of their own unique legal system. The attention shifts, in the next chapter, to a discussion of how South Africa has dealt with social media misconduct in workplaces.

Chapter 6:
Social Media Misconduct in South Africa

6.1 Introduction

In South Africa, the social media tsunami has had no less an impact than in any other country in the world. Between December 2000 and December 2017, the number of internet users in South Africa increased from 2,4 million to 30,8 million, and the country presently has over 16 million Facebook users.[219]

The first part of this chapter will discuss the law in South Africa as it may be applied to social media misconduct in the workplace. Thereafter, there will be a discussion of legal decisions relating to the subject.

6.2 South African Law relating to Social Media Misconduct in the Workplace

6.2.1 The Constitution[220]

The South African Constitution's preamble provides that "We the people of South Africa …. adopt this Constitution as the supreme law of the Republic…."[221] The supremacy of the Constitution is further confirmed in section 2 of the founding provisions.[222]

The Bill of Rights (hereafter BOR) is part of Chapter 2 of the Constitution and it protects, amongst other rights, two rights which feature most often in disputes relating to social media misconduct in workplaces. These are privacy rights and freedom of expression rights.[223]

---

[219] Miniwatts Marketing Group*: Internet World Stats* available at http://www.internetworldstats.com, accessed on 12 January 2018.
[220] Act 108 of 1996.
[221] Act 108 of 1996.
[222] S2 reads "This Constitution is the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled."
[223] The right to privacy is contained in S14 and the right to freedom of expression in S16.

The rights contained in the BOR apply both vertically and horizontally in terms of section 8 of the Constitution. Section 8(2) read with section 8(3)(b) provides the tool that is utilised to balance the rights of the employer and the rights of the employee.[224]

Of paramount importance is section 36[225] of the Bill of Rights, frequently called the 'limitations clause' which provides that "fundamental rights and freedoms are not absolute, their boundaries are set by the rights of others, and by the legitimate needs of society."[226] Section 36, therefore, sets out specific criteria for the restriction of the fundamental rights in the BOR.[227] Any infringement of a fundamental right is not unconstitutional where it can be justified by having regard for the criteria set out in section 36.

For the purposes of social media misconduct in the workplace, infringements of employees' and employers' rights to privacy or freedom of expression may be justified in terms of section 36, in particular, the employee's right to privacy or freedom of expression must be balanced with the employer's business necessity or operational requirements.[228]

In *Moonsamy v The Mailhouse,*[229] the CCMA was required to pronounce on the admissibility of evidence that the employer had acquired by intercepting and recording the telephone calls of the employee, made at the employer's premises, which the employer had, thereafter, used at the employee's disciplinary hearing and which had contributed to the latter's dismissal.[230] The arbitrator, having decided that

---

[224] Collier (note 82 above).
[225] S36 reads: "The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including
- the nature of the right;
- the importance of the purpose of the limitation;
- the nature and extent of the limitation;
- the relation between the limitation and its purpose; and
- less restrictive means to achieve the purpose."

(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights
[226] De Waal (note 35 above; 132).
[227] De Waal (note 35 above).
[228] M McGregor 'The right to privacy in the workplace: general case law and guidelines for using the internet and e-mail' (2004) 16 *South African Mercantile Law Journal* 638,650.
[229] *Moonsamy v The Mailhouse* 1999 (20) ILJ 464 (CCMA).
[230] Collier (note 82above; 1751).

the employer's conduct had infringed the employee's privacy rights, sought to determine whether the employer's conduct could be justified in terms of section 36.

In considering the nature of the right, the arbitrator found that the employee had a reasonable expectation of privacy regarding telephone calls that he had made while at the employer's premises.[231] In respect of the importance of the purpose of the limitation, the arbitrator pointed out that while the employer "does have rights in respect of the workplace, there has to be a balancing of interests and the employee's personal rights are to be preferred to the employer's right to economic activity."[232] Regarding the nature and the extent of the limitation the arbitrator found that, whereas the employer may inquire as to the number of calls an employee had made, there has to be prior authorisation or compelling reasons of business for the employee to be required to disclose the contents of the calls.[233] The arbitrator found that in respect of the relation between the limitation and its purpose, the method of telephone tapping used by the employer was "excessively invasive" and could be justified only if it was shown that the interception of calls was the only method available to secure essential evidence.[234] If less restrictive means were available, the employer should have used these. However, if telephone tapping was the only method available, then the employee's prior consent needed to be obtained.

The arbitrator held that the employer's action in intercepting the employee's telephone calls, without prior authorisation or consent of the employee, contravened section 14 read with section 36 of the Constitution, and the evidence was deemed inadmissible.[235]

6.2.2 Labour Relations Act ('LRA')[236]

The LRA is the foremost legislation regulating the relationship between employers and employees. The Act's purpose is, inter alia, to give effect to and regulate the fundamental rights conferred by section 23 of the Constitution.[237] Section 3 of the Act

[231] Ibid at 1751.
[232] Ibid at 1752.
[233] Ibid.
[234] Ibid.
[235] *Moonsamy supra* at 474.
[236] Act 66 of 1995.
[237] Labour Relations Act 66 of 1995; section 1(a).

provides that any person applying the LRA must interpret its provisions in compliance with the Constitution. The rights to equality, privacy, freedom of expression, freedom of assembly, demonstration, picket and petition, freedom of association, freedom of trade, occupation and profession and the labour relations rights are likely to be the most relevant.[238]

Section 188 of the LRA provides that lawful dismissals may occur in three instances: when related to the employee's conduct,[239] when related to the employee's capacity,[240] and when related to the employer's operational requirements.[241] The employer bears the onus of proving that there was both substantive and procedural fairness.[242]

Section 188(2)[243] is important as it instructs that, when a person considers the fairness of a dismissal or the fairness of the procedure in effecting the dismissal, account must be taken of any relevant code of good practice which can be found in Schedule 8 of the LRA.[244]

Section 7[245] of Schedule 8 provides guidelines in cases of dismissals for misconduct. This section will be of importance in cases relating to social media misconduct in the workplace.

---

[238] Collier (note 82 above).
[239] Labour Relations Act 66 of 1995; section 188(1)(a)(1).
[240] Labour Relations Act 66 of 1995; section 188(1)(a)(1).
[241] Labour Relations Act 66 of 1995; section 188(1)(a)(2).
[242] Collier (note 82 above) and see Labour Relations Act 66 of 1995; section 188(1)(b).
[243] Labour Relations Act 66 of 1995; section 188(2) reads: "Any person considering whether or not the reason for dismissal is a fair reason or whether or not the dismissal was effected in accordance with a fair procedure must take into account any relevant code of good practice issued in terms of this Ac"t.
[244] Labour Relations Act 66 of 1995; schedule 8 is titled "Code of Good Practice: Dismissal ".
[245]Labour Relations Act 66 of 1995; section 7 reads: "Any person who is determining whether a dismissal for misconduct is unfair should consider(a) whether or not the employee contravened a rule or standard regulating conduct in, or of relevance to, the workplace; and
(b) if a rule or standard was contravened, whether or not-
(i) the rule was a valid or reasonable rule or standard;
(ii) the employee was aware, or could reasonably be expected to have been aware, of the rule or standard;
(iii) the rule or standard has been consistently applied by the employer; and
(iv) dismissal was an appropriate sanction for the contravention of the rule or standard".

The employer's Social Media Policy (SMP) may be challenged on several grounds relating to the provisions of section 7 of the Code. A critical question that would be asked is whether the SMP contained any rule regulating the conduct of the employee. It stands to reason that if there was no workplace rule prohibiting the offensive conduct, then the employee's dismissal may be challenged by claiming that the termination was effected on a non-existent and unknown rule.[246]

If an SMP rule is invalid or unreasonable, the dismissed employee is likely to be granted relief. An invalid rule would be one where, for example, employees are prohibited from discussing working conditions and benefits on Facebook. An employee who had made Facebook posts in furtherance of trade union activity and was dismissed for that reason may institute a claim for an "automatically unfair dismissal" as provided for in sections 187(1) or S 187(1)(a) of the LRA.

An unreasonable rule would be one where the company deems itself entitled to dismiss an employee, who had named the employer on a Facebook profile, and the company argues reputational damage as a fair reason to dismiss because the employee had made some controversial Facebook posts regarding non-work-related matters.[247]

Automatically unfair dismissal claims may arise, in terms of section 187(1)(f) of the LRA, if employers unfairly discriminate against employees because of information obtained from the employee's Facebook profile.

6.2.3 Regulation of the Interception of Communications and Provision of Communication Related-Information Act 70 of 2002 (RICA)[248]

RICA became operational at the end of September 2005.[249] Before the enactment of RICA, the Interception and Monitoring Prohibition Act[250] was the most important

[246] However, an employee's dismissal has been deemed to be fair notwithstanding the fact that the employer had no workplace rule prohibiting the offensive conduct – refer Warren Thomas Griffith v VWSA 2000 CCMA case number EC16714.
[247] *Smith* supra is a UK decision. *Cantamessa supra* is a South African decision.
[248] Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002.
[249] T Pistorious 'Monitoring, interception and big boss in the workplace: is the devil in the details?' (2009) 1 *PER.*
[250] Interception and Monitoring Prohibition Act 127 of 1992.

statute regarding monitoring. The IMP Act was not applicable to private spheres, such as the workplace. The reach of RICA is wider than that of the IMP Act, as it applies also to the private spheres.

Section 2[251] of RICA is a core provision. Contravening the provisions of RICA is a criminal offence[252] with severe penalties.[253]

An understanding of indirect communications[254] is important to this dissertation. Indirect communications include "telephone calls (landline and cellular), intranet, internet, facsimile facilities, private and personal email messages, SMS messages, tracking devices in company cars, and voicemail messages."[255]

The scope of section 2 is wide and aims to prevent interception of communications in any form; however, RICA makes allowance for the interception of communications in certain instances.[256]

Section 4(1)[257] makes allowance for consensual monitoring by parties to the communication. Parties to the communication include the sender, the receiver, or a party copied in. Some writers contend that the employer, as the owner of the equipment over which the message is relayed, is also a party to the communication.

---

[251] "Subject to this Act, no person may intentionally intercept or attempt to intercept or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission".
[252] RICA Section 49.
[253] RICA Section 51 provides for a fine not exceeding R2 million or imprisonment not exceeding 10 years.
[254] "means the transfer of information, including a message or any part of a message, whether (a) in the form of speech, music or other sounds; data, text, visual images, whether animated or not; signals; or radio frequency spectrum; or (b) in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system".
[255] Pistorious (note 249 above).
[256] Sections 3 to 11 set out the circumstances where there will be no contravention of S2.
[257] Section 4(1) reads: Any person, other than a law enforcement officer, may intercept any communication if he or she is a party to the communication unless such communication is intercepted by such person for purposes of committing an offence.

Section 5(1)[258] is extremely important as it provides that any person may intercept any communication if one of the parties to the communication has given prior written consent to the interception.[259]

A "general consent, contained in the conditions of employment of an employee, would amount to consent in terms of section 5(1). Some writers argue that on account of the words 'consent in writing to such interception,' consent may be required on a case by case basis."[260] Consent in writing needs to be given by only one party to the communication, whether it is the sender, the recipient, or a party copied in on the message.

Section 6(1)[261] of RICA relates directly to business enterprises. Section 6(2) sets out the requirements before any interception, in terms of section 6(1), is allowed – "the interception must be with the express or implied authority of the system controller, and the latter must have made reasonable efforts to inform users of the system of the intended interception; alternatively, the interception may take place with the express or implied consent of the users. The system must be for use in the business, and interceptions may be carried out for specific purposes (including investigating the unauthorised use of the system)."[262]

Where employers have obtained the consent of employees to intercept communications or employers have made reasonable[263] prior efforts to inform the users of the intended interceptions, then the provisions contained in RICA allow employers to lawfully monitor unsavoury employee conduct, such as cyberloafing, viewing of pornography, harassment, and sending of offensive emails.

---

[258] S5(1) reads: "Any person, other than a law enforcement officer, may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception, unless such communication is intercepted by such person for purposes of committing an offence".
[259] Pistorious (note 249 above).
[260] ibid.
[261] S6(1) reads: "Any person may, in the course of the carrying on of any business, intercept any indirect communication *(a)* by means of which a transaction is entered into in the course of that business;
(b) which otherwise relates to that business; or
(c) which otherwise takes place in the course of the carrying on of that business, in the course of its transmission over a telecommunication system".
[262] Pistorious (note 249 above).
[263] Section 6(2)(d).

6.2.4 Electronic Communications and Transactions Act[264] (ECTA)

The objective[265] of ECTA is to enable and facilitate electronic transactions and to create public confidence in electronic transacting.[266]

Where the employer uses the electronic environment to convey information to employees, such as limitations on the use of computer equipment and networks, the use of a non-paper-based method of transmission should be viewed as natural and logical. Electronic agreements may be validly concluded through 'click-wrap' agreements where the employee signifies consent by clicking on the "I agree 'icon.[267]

In this manner, the employer will be able to comply with the RICA consent requirements. Consent to monitor and intercept employee communications would have been obtained electronically. The requirement of prior consent will be met with ease if the giving of such consent is conditional for obtaining access to the workstation or other telecommunication equipment.[268]

6.2.5 Protection of Personal Information Act[269] (POPI)

The purpose of POPI is to promote the protection of data subjects' personal information.[270] Principally, the Act's goal is to protect citizens' constitutional right to privacy, by recognizing that the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.[271]

Therefore, because POPI seeks to protect individual rights to privacy, there are significant implications for employers. The personal information[272] of employees needs to be safeguarded, and the provisions of POPI complied with when such information is processed by employers. To ensure the safeguarding of personal

---

[264] Electronic Communications and Transactions Act 25 of 2002.
[265] S 2 of ECTA lists the objectives of the Act.
[266] Pistorious (note 249 above).
[267] Ibid.
[268] Ibid.
[269] Protection of Personal Information Act 4 of 2013.
[270] D Millard & EG Baskaran 'Employers' statutory vicarious liability in terms of the protection of personal information act' (2016) 19 *PER/PELJ.*
[271] LSwales 'Protection of personal information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' (2016) 49 *SA Merc Law Journal* at 49.
[272] See POPI, Chapter 1 for definition of personal information.

information by responsible parties (the employer in the present instance), personal information must be processed in a responsible and lawful manner.[273] The Act provides employees with rights and remedies to protect their personal information from unlawful and irresponsible processing.[274]

Chapter 3 of POPI[275] imposes limitations on how employers may process personal information of employees. These conditions include: the need for lawfulness of processing, the limitations of processing, processing only on receipt of the employee's consent, collection must be for a specific purpose, the limitations on the further processing of information, notification to the employee when collecting personal information, security safeguards to preserve the integrity and confidentiality of personal information, and prohibitions on the processing of special[276] personal information.

In an "organisation that consists of employers and employees, the employer will be held liable for contraventions of POPI by employees, because the employer is held to be the responsible party. Therefore, where the aggrieved party would traditionally have sued the employer for infringement of privacy based on the common law vicarious liability doctrine, there is now also the possibility to litigate based on the stipulations of POPI."[277]

In terms of section 99(1) of POPI, the data subject may institute civil action against an employer as the responsible party. Section 99(2) lists the limited defences which an employer may raise in an action brought in terms of section 99(1).[278]

---

[273] Protection of Personal Information Act 4 of 2013, Section 4.
[274] POPI, Section 2(c).
[275] "Conditions for lawful processing of information".
[276] Special personal information includes information relating to an individual's religion, race, sexual orientation, trade union membership and political affiliation.
[277] Millard (note 270 above).
[278] S 99(1) "A data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act as referred to in section 73, whether or not there is intent or negligence on the part of the responsible party. (2) In the event of a breach the responsible party may raise any of the following defences against an action for damages:(a) Vis major;(b) consent of the plaintiff;(c) fault on the part of the plaintiff;(d) compliance was not reasonably practicable in the circumstances of the case; or(e)the Regulator has granted an exemption in terms of section 37".

The defences are limited because the employer will not be able to escape statutory vicarious liability, for an employee's misconduct, even if reasonable steps had been taken to prevent the employee from contravening POPI.[279]

Employees may be guilty of misconduct if, in their use of social media platforms, they reveal personal information relating to co-workers to outside parties not entitled to the information.

6.2.6 Analysis of South African legal decisions

This section analyses important decisions that relate to social media misconduct in the workplace.

In *Goosen v Caroline's Yoghurt Parlour (Pty) Ltd,*[280] the court considered the admissibility of transcripts of telephone conversations, which Goosen had acquired without his employer's consent, and which he claimed showed bias on the part of the presiding officer at his disciplinary hearing. The Industrial Court ruled that the recordings were admissible. The court held that it should not be concerned with how the evidence was obtained, provided it was relevant and not obtained under duress, and there was no obligation on the accused to give self-incriminating evidence.[281]

The *Protea Technology Ltd and another v Wainer and others*[282] case was decided under the final Constitution. The employer had recorded conversations of the employee, without the latter's consent, and tendered the recordings in court to prove that the employee had breached a restraint of trade agreement. The employee claimed that the employer had breached his right to privacy in making the recordings and that the evidence should not be admitted. The court ruled that, regarding the admissibility of illegally obtained evidence, the "common law rule of relevance (applied in Goosen) was inconsistent with the Constitution, rather, the discretion must be exercised with regard to the substance of section 36(1) of the Constitution."[283] Regarding the employee's right to privacy, the court held that the right requires a

[279]Millard (note 270 above).
[280] *Goosen v. Caroline's Yoghurt Parlour (Pty) Ltd and another* 1995 (16) ILJ 396 (IC).
[281] Collier (note 82 above).
[282] *Protea Technology Ltd and another v Wainer and others* 1997 (9) BCLR 1225 (W).
[283]Collier (note 82 above).

subjective expectation of privacy which society considers objectively reasonable.[284] The court noted that the recorded calls were made during business hours, from the employer's premises, and employee conversations relating to employer affairs were not private; further, the employer had a right to know whether the employee was committing a delict. The court concluded that Wainer was not entitled to insist on his right to constitutional protection of privacy and upheld the discretion of the court to admit illegally obtained evidence.[285]

In *Moonsamy v The Mailhouse,*[286] the CCMA considered the admissibility of illegally obtained evidence. The employer had, without Moonsamy's authority, intercepted and recorded the employee's telephone conversations, which were made from the employer's premises, and the evidence obtained was relied on to dismiss the employee. The arbitrator held that the common law formulation of admitting illegally obtained evidence if it was relevant, was contrary to the right to privacy contained in the Constitution. The arbitrator found that the employee's privacy rights were infringed and, in the light of section 36 of the Constitution, the infringement could not be justified because the employer had admitted that he had already secured evidence in other ways, without having had to infringe the employee's privacy rights. The evidence was therefore deemed inadmissible.

In the *Bamford and others v Energizer (SA) Ltd*[287] matter, employees were dismissed for downloading and distributing pornographic and other non-work-related material during working hours, while using the employer's facilities. The arbitrator upheld the dismissals, remarking that even though the employer did not have in place a computer usage policy, business equipment should legitimately be used only for business purposes. Any tolerance allowed by the employer should be used circumspectly.

The *Cronje v Toyota Manufacturing*[288] matter relates to the dismissal of managerial staff for publishing racist and inflammatory material via email and hard copy, and for

---

[284] Ibid at 1750.
[285] Ibid.
[286] *Moonsamy supra*.
[287] *Bamford supra*.
[288] *Cronje supra.*

having violated the company's internet code. The material distributed was crude, offensive, and racially stereotyping. The arbitrator placed emphasis on the context in which the misdemeanour took place. The incident occurred in a factory that employed 3500 Black employees, and where money and time was spent on building a good relationship between management and labour. The commissioner considered the existence of the rule prohibiting the conduct, the consistent application of the rule and the dismissed employee's knowledge thereof and decided that dismissal was the appropriate sanction.

Sedick and another and Krisray (Pty) Ltd[289] relates to derogatory Facebook comments in respect of the employer, posted by employees, which had the potential to cause reputational damage to the organisation. In this matter, the employees did not expressly name the company, but the references were clear. The admissibility of evidence was not in dispute, as the employees had not put access restrictions on their Facebook profiles, and anyone could see the posts. The commissioner ruled that, in not making use of their privacy options, the employees had abandoned their rights to privacy. The CCMA ruled that dismissal was justified.

Smith and Partners in Sexual Health (Non-Profit)[290] considered the right of the employer to access the employee's private internet-based Gmail account. The employer had initially accessed the employee's private account accidentally and, thereafter, accessed the account intentionally. The CCMA ruled that, in intentionally accessing the private account after the accidental accessing of the account, the employee's privacy rights were infringed, the evidence obtained was inadmissible, and the employee's dismissal was deemed to be unfair.

---

[289] *Sedick & another and Krisray (Pty) Ltd* 2011 (32) ILJ 752 (CCMA). See also *Fredericks v Jo Barkett Fashion* (2011) JOL 27923 (CCMA). In *Kendrick and Nelson Mandela Metropolitan University* 2018 (39) ILJ 2383 (CCMA), the employee was dismissed for making disparaging remarks about the Muslim community- the remarks appeared on social media. *Dheaneswar and Trimedia* 2016 (37) ILJ 273 CCMA, relates to an employee receiving inappropriate WhatsApp text messages from her manager. The employee resigned after three weeks of employment and thereafter successfully pursued a constructive dismissal claim - she was awarded compensation in respect of what the arbitrator called the "predatory" behaviour of the manager. In *Du Plessis and Rickjon Mining and Engineering* 2018 (39) ILJ 1665 (CCMA) the arbitrator considered the effect of derogatory remarks on Facebook, about a female employee, that were posted by the employee's co-workers. The arbitrator held that such conduct constitutes harassment and was forbidden by the Employment Equity Act. The employer failed to take action against the perpetrators and had to pay the employee compensation.

[290] *Smith and Partners in Sexual Health (Non-Profit)* 2011 (32) ILJ 1470 (CCMA).

In *Cantamessa and Edcon Group,*[291] the employer claimed that the employee's Facebook post, made outside of working hours, tarnished its name and caused it reputational damage. The employee had linked herself, to the employer, by mentioning on her Facebook profile that she was employed at Edcon. The employee was dismissed for making racist and derogatory comments in her Facebook post. The CCMA found that the employer's "social media policy did not regulate the use of social media outside of the workplace,"[292] the employee merely stated her occupation as a fact about herself and, as such, it did not constitute a link to the employer such that she could be "disciplined for conduct outside of working hours."[293] The employee's dismissal was deemed to be unfair. The facts of this case and the decision handed down are similar to the *Smith*[294] case decided in the UK.

Experian South Africa (Pty) Ltd v Haynes and another[295] related to an employee's use of Linked-In within the context of a restraint of trade dispute. The employee's Linked-In profile mentioned the employee's tasks with his former employer, it also showed that after joining his new employer, the employee met with clients of the former employer, and the Linked-In profile also showed the employee contacting Experian's clients. The court held that because of the employee having contacted clients of his former employer via his Linked-In profile, the former employer was entitled to the relief it sought.[296]

In *Beaurain v Martin NO and others,*[297] the court considered whether publication on Facebook is a protected disclosure in terms of the Protected Disclosures Act 26 of 2000 (PDA). The employee published photographs and complaints about his employer (Groote Schuur Hospital in Cape Town) on Facebook and when asked by the employer to stop, the employee claimed that his disclosures were protected by the PDA and that he was a whistleblower. The employee refused to heed the instructions of the employer and was dismissed for gross insubordination. The court held that an objective of the PDA is to allow employees to disclose improprieties of

[291] *Cantamessa supra*.
[292] Ibid
[293] ibid
[294] *Smith supra*.
[295] *Experian South Africa (Pty) Ltd v. Haynes & another* 2013 (1) SA 135 (GSJ).
[296] *Experian supra* at para 55.
[297] *Beaurain v Martin NO and others* 2014 (35) ILJ 2443 (LC).

the employer in a reasonable manner. The court held further that the "publication of the allegations on Facebook was unlikely to solve the problem, and it was unnecessary to publish the information to the international community, who could do little to help."[298] The court ruled that the employee had contravened express rules of the employer, despite being instructed twice to cease his Facebook publications, and he was dismissed for a fair reason.

6.3 Summary

In concluding this section on social media misconduct in South Africa, it is appropriate to reflect on a statement made earlier in this presentation. South Africa is a member of the global community and, notwithstanding its unique history and independence; it will readily adopt international best practices, as displayed in specialised fields such as industries and engineering and, to no less an extent, in the field of law.

The next chapter will draw a comparison, between South Africa and other leading nations of the global community, and it will relate to their respective legal approaches toward social media misconduct in the workplace. Similarities and differences will be considered, with the aim of presenting proposals on how best to address the subject in the South African workplace.

[298] *Beaurain supra* at para 33.

Chapter 7:
Concluding Comments:

7.1 Introduction

The use of internet-based communication tools is indispensable for the modern-day employer. However, granting employees limitless and uncontrolled access to communication facilities poses serious risks to the employer.

There is, on the one hand, the employer who seeks to maximise profits, primarily from the efforts of a productive and content workforce. A disgruntled labour force is unlikely to be productive. The employer's perspective must, of necessity, be wider than the pure monitoring of employees work efficiencies or their non-compliance with contract terms or company rules. The greater risk lies in the fact that, because of employee misconduct, the employer is exposed to the risk of incurring huge financial losses (for example, through vicarious liability, reputational damage, or lower productivity).

Employees, on the other hand, are always conscious of their subordinate status to the employer and are resentful of working in claustrophobic environments where they perceive that their every action is seemingly subject to employer monitoring. They yearn for decent working conditions and respect for their common law, statutory and constitutionally entrenched rights.

How best to balance the conflicting interests of employers and their employees, in the relatively new area of social media and internet-based communications, has been the subject of much discussion and debate.

7.2 Present-day status of social media misconduct in workplaces

The discussion in the earlier chapters has shown that, notwithstanding their being members of a global community of nations, the legal systems of individual countries differ considerably; for example: some countries may have constitutions, while others do not; where constitutions exist, these may operate vertically, or both vertically and horizontally; labour legislation may strive for equitable outcomes, while others may

not. A homogeneous legal system that is common to all member states does not exist.

South Africa has drafted its Constitution having regard for its own turbulent history but, at the same time, acknowledging its membership in the world community. The Constitution acknowledges the need to abide by international law, it respects foreign law in allowing courts and tribunals to refer to such law, and fairness in labour practices is entrenched in the Bill of Rights.

Context is a paramount consideration when courts and tribunals apply the law in South Africa. This is deemed necessary by the Constitution which provides that there must be recognition of the injustices of the country's past and efforts must be made to heal divisions in an effort toward establishing a "society based on democratic values, social justice and fundamental rights." The cause of social media misconduct frequently arises from the deep-rooted societal divisions that continue to bedevil the country, and which give rise to beliefs of, for example, racial and gender superiority. This dissertation commenced with the view that astute industrial practitioners must be cognisant of the root causes of maladaptive behaviours in individuals and, in respect of the multi-racial and multi-cultural characteristic of the workplace, they must take steps to avert conflict arising from the existence of subliminal prejudices. The *Cronje* case is an example of an employer being aware of the harm that may be caused to an organisation with a multi-cultural workforce through the dissemination of racially prejudiced social media material. Deep-seated bigotry and racial prejudice often makes its way into the public domain through social media usage, both within and outside the workplace, and such conduct serves to impair the dignity of citizens and co-workers. Conduct that impairs the dignity of another person will be deemed unlawful in terms of section 10 of the Bill of Rights, and members of the workforce may justifiably be dismissed for social media conduct that impairs the dignity of others.

The right to privacy, which includes the right not to have the privacy of one's communications infringed, is protected in section 14 of the Bill of Rights. Freedom of expression is protected in section 16 of the Bill of Rights. These fundamental rights may, however, be restricted by section 36 of the Constitution which provides for the

limitation of rights in certain circumstances. Employees have not been able to successfully argue that their right to freedom of expression was infringed where, for example, they posted derogatory or defamatory comments about co-workers or management on social media sites.

An individual's right to privacy is protected in South Africa by the common law, the Constitution and legislation (including RICA, ECTA and POPI). Privacy rights are recognised, locally and globally, as being one of the most important of human rights. The House of Lords has records of a privacy dispute having been considered, in *Peter Semayne v Richard Gresham,*[299] as long ago as 1604. The courts and the legislatures, both locally and internationally, have recognised that unrestricted employee privacy rights in the workplace may endanger the wellbeing of the business, and court decisions and legislation offer a measure of protection for employer rights.

The Constitutional Court of South Africa recognised in the *Bernstein* matter that the "right to privacy is not absolute." The right to privacy extends only to those "aspects of an individual's life in respect of which the individual has a legitimate expectation of privacy" that is subjectively experienced and which society views as being objectively reasonable. As a person moves more into the public domain, including the workplace, the right to privacy diminishes. Legislation such RICA, ECTA, and POPI provide employers with lawful means to monitor their employees' communications, when such monitoring is undertaken for business purposes, thereby allowing for the infringement of the privacy rights of workers.

The potential for harm to business organisations, arising from social media or internet misconduct of employees, is vast. Decreased productivity, vicarious liability, liability for the unauthorised formation of contracts, liability for sexual harassment and discrimination are a few of the pitfalls that lie in wait for employers who do not monitor the social media and internet conduct of their employees.

[299] *Peter Semayne v Richard Gresham* (1604), 77 E.R. 194, (1588-1774) ALL E.R. Rep 62.

The analysis of cases and legislation relating to social media misconduct in foreign jurisdictions reveals two interesting phenomena. While the nature of the employee misconduct (such as defamatory social media posts, sexual and other forms of harassment, excessive private use) is largely the same throughout the world, the laws that are used to adjudicate social media misconduct disputes are different in each jurisdiction. South Africa's Constitution, for example, provides for the protection of a range of rights, including privacy and freedom of expression, and further, these rights operate both vertically and horizontally. The US Constitution protects freedom of speech and privacy rights, but it operates only vertically, that is, between the government and public-sector employees. Therefore, except to be of persuasive value, the American Constitution does not apply in private sector disputes. In the USA, the Wiretap Act (Title 1 of ECPA) protects against the interception of communications during transmission, the Stored Communications Act (Title 2 of ECPA) restricts the disclosure of information stored on a server. An employer may avoid liability under ECPA if interception of employee communications arose out of business necessity, or if the employee consented to such interception. The provisions of the Wiretap Act resemble those found in South Africa's RICA and the Stored Communications Act have similar provisions to those found in South Africa's POPI.

The 'employment-at-will' doctrine that underpins most employment relations in the USA, which allows the employer to terminate employment relationships at any time without having to provide reasons, contrasts starkly with South Africa's LRA where a fair reason for any dismissal needs to be provided by the employer.

The Canadian Charter of Rights and Freedom, like the American Constitution, operates vertically but has only persuasive value in private sector disputes. The New Zealand Bill of Rights makes provision for freedom of expression, but not for privacy.

South Africa, similar to the foreign jurisdictions discussed above, does not have legislation relating specifically to social media misconduct. However, South African courts have made pronouncements on social media misconduct in the workplace by considering the values enshrined in the Constitution and related legislation such as RICA and ECTA, and by reference to the common law. Judicial officials have heeded section 39(1)(c) of the Constitution and have frequently referred to foreign law when

considering and handing down their decisions. The legislature, in promulgating laws, such as RICA and POPI which largely replicate provisions contained in foreign legislation, have also heeded section 39(1)(c).

Business entities, both in South Africa and in other countries of the world, have begun implementing Social Media Policies (SMP's) to guard against the risks posed by employee social media misconduct. The most important component of an SMP is to obtain the consent of the employee to allow monitoring, by the employer, of the employee's communications.

The next section considers the contents of SMP's and their implementation.

7.3 Social Media Policies (SMP)

In the early years of social media, employers adopted a laissez-faire approach, adopting a minimalist interference stance. However, as the risks attached to social media misconduct became apparent, employers began introducing SMP's in the workplace.

It is submitted that the commentators and academics are correct regarding the provisions that need to be included in SMP's. These provisions, which safeguard both employers and employees interests in equal measure, and which will contribute to workplace harmony, include the following:

- It is necessary to reach agreement on the contents of SMP's, with employees or their unions, before implementing any SMP's.

- The SMP must not contain provisions that violate the rights of employees, for example, prohibiting employees from canvassing co-workers to join a union.

- Occasional private use of facilities, by employees, should be permitted. The SMP should outline the circumstances under which private use is allowed (for example, private use is allowed during lunch breaks, or before commencement and after completion of the work day).

- Remind employees that their usage of company communication systems will be monitored to identify any unauthorised, malicious, or criminal use thereof.

- Private use must be lawful, ethical, and considerate of the rights of others.

- Employee usage must not serve to expose the employer to any form of legal liability – the types of conduct must be outlined, and explained, in the SMP (explicitly state that employees may not engage in copyright infringements, make defamatory statements, view or download pornographic material, engage in cyberbullying or harassment, etc…).

- When posting personal comments, employees must explicitly state that it is their views that are being expressed and not those of the employer.

- The consequences of failing to adhere to the company's SMP, including the sanctions that may be imposed on errant employees, must be stated unambiguously.

- The management representative responsible for the company's SMP must be identified in the SMP.

- Staff training and refresher courses on social media matters must be carried out at reasonable intervals.

The employee's prior consent, to allow monitoring of their social media and internet use, grants the employer the "right not only to invade the employee's privacy in certain circumstances but also to dismiss or discipline the employee for inappropriate use of communication tools."[300]

[300] Collier (note 82 above).

“If the employment relationship is to be based on trust and its sensitivities respected, employers should be hesitant to monitor communication content, particularly without employee consent.”[301]

7.4 Conclusion

It is an accepted fact that it is only a small proportion of the workforce that are guilty of abusing social media, and employers are correct in taking steps to protect their own interests and the interests of other employees. Draconian measures to cull social media use, imposed by employers, will benefit neither themselves nor their employees. Measures to curb social media misconduct must be rooted in the Constitutional values of human dignity, equality, freedom and the other rights contained in our Bill of Rights.

[301] Collier (note 82 above).

REFERENCES

Legislation:

Age Discrimination in Employment Act

Americans with Disabilities Act

Canadian Charter of Rights and Freedoms 1982
S8

Canadian Constitution
S91
S92

Civil Rights Act 1964

Convention for the Protection of Human Rights and Fundamental Freedoms, 1950

Copyright Act 98 of 1978

Criminal Procedure Act 51 of 1977

Electronic Communications and Transactions Act 25 of 2002
S2
S22
S23(1)(b)

Employment Relations Act No.24 of 2000

European Convention for the Protection of Human Rights and Fundamental Freedoms (1950)
Article 8
Article 10.

Fair Works Act 2009

Film and Publications Board Act 65 of 1996

Human Rights Act of 1998

Interception and Monitoring Prohibition Act 127 of 1992.

National Labor Relations Act 29 U.S.C 151-169 (2012)
S7
S8(1)(a)

New Zealand Bill of Rights Act No. 109 of 1990
S5
S14
S21

Protected Disclosures Act 26 of 2000

Protection of Personal Information Act 4 of 2013
Chapter1
Chapter 3
S2(c)
S37
S99(1)
S99(2)
S73

Regulation of Investigatory Powers Act 2000

Related Information Act 70 of 2002

The Code of Good Practice on the Handling of Sexual Harassment Cases
Item 4(1)(c)

The Constitution of the Republic of South Africa Act 108 of 1996

S1

S2

S7(1)

S8(2)

S8(3)(b)

S10

S14

S15

S16

S17

S18

S19

S23(1)

S36(1)

S39(1)(c)

The Constitution of the United States, signed on 17th September 1787
1st amendment
4th amendment

The Electronic Communications Privacy Act of 1986

Title1- wiretap act

Title 2 – stored communications act

Title 3 – pen register statute

The Employment Equity Act 55 of 1998

The Labour Relations Act 66 of 1995

Schedule 7, section 8

S1(a)

S3

S187

S188

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

S2

S3

S4(1)

S5(1)

S6(1)

S6(2)

S7

S8

S9

S10

S11

S49

S51

Universal Declaration of Human Rights December 10, 1948

Article 19

Case List:

Bamford & Others v Energizer (SA) Ltd 2001 (12) BALR 1251 (P)

Beaurain v. Martin NO and others 2014 (35) ILJ 2443 (LC)

Bernstein v Bester 1996 (2) SA 751 (CC)

Campbell v Mirror Group of Newspapers (2004) UKHL 22

Cantamessa and Edcon Group 2017 (38) ILJ 1909 (CCMA)

Case & Another v Minister of Safety and Security & Others 1996 (3) SA 617 (CC)

Chatham-Kent (Municipality) v. National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 127 (Clarke Grievance), (2007) O.L.A.A. No.135 (“Chatham-Kent”)

City of Ontario v Quon 130 S.Ct. 2619, 560 U.S

Copland v. United Kingdom (2007) ECHR 25

Costco Wholesale Corp., 358 NLRB, No. 106, 2012 WL

Cronje v Toyota Manufacturing 2001 (3) BALR 213 (CCMA)

CWU v Mobile Telephone Networks (Pty) Ltd 2003 (8) BLLR 741 (LC).

Damian O’Keefe v. William Muir’s (Pty) Ltd t/a Troy Williams The Good Guys (2011) FWA 5311

Dandi Wang v. New Zealand Chinese Television Ltd (2015) NZERA Auckland 32

Design Tech. Grp., L.L.C., d/b/a Bettie Page Clothing, 359 NLRB No.96, 2013

Dutch Reformed Church v Rayan Sookunan t/a Glory Divine World Ministries 2012 (3) All SA 322 (GSJ)

Ehlers v Bohler Uddeholm Africa (Pty) Ltd 2010 (31) ILJ 2383 (LC)

Ekhamanzi Springs (Pty) Ltd v Mnomiya 2014 (35) ILJ 2388 (LAC)

Entick v. Carrington (1765), 95 E.R.807, K.B.275

Experian South Africa (Pty) Ltd v. Haynes & another 2013 (1) SA 135 (GSJ)

Feldman (Pty) Ltd v Mall 1945 AD 733

Financial Mail v Sage Holdings 1993 (2) SA 451(A)

Fredericks v Jo Barkett Fashions 2011 JOL 27923 (CCMA)

Goosen v Caroline's Frozen Yogurt Parlour 1995 (16) ILJ 396 (IC)

Govender v Mondi Kraft-Richards Bay 1999 (20) ILJ 2881(LC).

Grobler v Naspers Bpk 2001 (4) SA 938 (LC)

Heroldt v Wills 2014 JOL 31479 (GSJ)

Hispanics United of Buffalo, Inc. and Carlos Ortiz NLRB Case 03-CA-027872 Dec 2012

Hosking v. Runting 2005 (1) NZLR 1 32 (CA)

IMATU & another v City of Cape Town 2005 (26) ILJ 1404 (LC)

Investigating Directorate: Serious Economic Offences & Others v Ltd & Others: In Re Hyundai Motor Distributors (Pty) Ltd & Others v Smith NO & Others 2011 (1) SA 545 (CC)

Islamic Unity Convention v Independent Broadcasting Authority 2002 (4) SA 294 (CC)

Karl Knauz Motors, Inc., 358 NLRB. No.164, 2012 WL 4482841 Sept 2012

Katz v US 389 US (1967)

Kidson v SA Associated Newspapers Ltd 1957 (3) SA 461 (W)

Kievits Kroon Country Estate (Pty) Ltd v Mmoledi 7 others 2014 (35) ILJ 406 (SCA)

Lafayette Park Hotel, 326 N.L.R.B. 824, 825 (1998).

Lougheed Imports Ltd. (c.o.b. West Coast Mazda) (Re), (2010) B.C.L.R.B.D. No.190 ("Lougheed Imports ")

MEC for Education: KZN v Pillay 2008 (1) SA 474 (CC)

Minister of Home Affairs and others v Watchenuka 2003 ZASCA 142

Miss Sally-Ann Fitzgerald v. Dianna Smith t/a Escape Hair Design (2010) FWA 7358

Mistry v Interim Medical & Dental Council of South Africa & Others 1998 (4) SA 1127 (CC) 1127 (CC)

Moonsamy v The Mailhouse 1999 (20) ILJ 464 (CCMA)

Ms Tamicka Louise Dover-Ray v. Real Insurance (Pty) Ltd (2010) FWA 8544

National Coalition for Gay and Lesbian Equality v Minister of Justice 1999 (1) SA 6 (CC)

National Media v Bogoshi 1998 (4) SA 1995 (SCA)

O'Keeffe v Argus Printing & Publishing Co. Ltd & Others 1954 (3) SA 244 (C)

O'Connor v Ortega 480 U.S 709 (1987)

Peter Semayne v. Richard Gresham (1604), 77 E.R. 194, (1588-1774) ALL E.R. Rep 62

Protea Technology Ltd & Another v Wainer & Others 1997 (9) BCLR 1225 (W)

R V Cole, 2012 SCC 53 2012 (3) SCR 34

Rachel Blylevens v. Kidicorp Limited (2014) NZERA Auckland 373

Re Walder (2010) B.C.E.S.T.D. No.113

RWDSU v Dolphin Delivery Ltd 1986 (2) SCR 573

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

Sage Holdings Ltd & Another v Financial Mail (Pty) Ltd 1991 (2) SA 11 (W)

Sappi Novobord (Pty) Ltd v Bolleurs 1998 (19) ILJ 784 (LAC)

Sedick & Another and Krisray (Pty) Ltd 2011 (8) BALR 879 (CCMA)

Smith and Partners in Sexual Health (Non-Profit) 2011 (32) ILJ 1470 (CCMA)

Smith v. Trafford Housing Trust (2012) EWHC 3221

South African National Defence Force Union v Minister of Defence 1999 (4) SA 469 (CC)

Stransham-Ford v Minister of Justice & Correctional Services 2015 (4) SA (GP)

Smyth v Pilsbury Co 914 F.Supp. 97 (E.D Pa 1996)

Sugreen v Standard Bank of SA 2002 (7) BALR 769 (CCMA)

Teck Coal v. U.M.W.A. Local 1656, (2010) A.W.L.D. 2589

Toker Bros (Pty) Ltd &Keyser 2005 (26) ILJ 1366 (CCMA)

Warren Thomas Griffiths v VWSA CCMA, 22 June 2000

Wasaya Airways LP v. Airline Pilots Assn., International (Wyndels Grievance), (2010) C.L.A.D., No.297, 195 L.A.C. (4TH) 1 ("Wasaya ")

Books and Journals:

Baron, R., & Byrne, D. *Social Psychology: Understanding Human Interaction* 5 ed Boston: Allyn & Bacon Inc, (1987).

Beech, W 'The right of an employer to monitor employees electronic mail, telephone calls, internet usage, and other recordings' (2005) 26 *ILJ* 650.

Boyd,D and Ellison,N 'Social network sites: definition, history, and scholarship' (2007) *Journal of Computer Mediated Communication*.

Burchell, J. 'The legal protection of privacy in south africa: a transplantable hybrid' (2009) 13(1) *Electronic Journal of Comparative Law Vo*.

Carson, C., Butcher, J., Coleman, J., *Abnormal Psychology and Modern Life* 8 ed London: Scott, Foresman and Company (1988).

Cavico, J. 'Social media and employment at will: tort law and practical considerations for employees, managers and organizations' (2013) 11 *New Media and Mass Communication*.

Cavico, FJ., 'Social media and the workplace: legal, ethical, and practical considerations for management' (2013) 12 *Journal of Law, Policy and Globalization*.

Cilliers, F.Q., 'The role and effect of social media in the workplace' (2013) 40(3) *Northern Kentucky Law Review, Vol40:3*

Collier, D 'Workplace privacy in the cyber age' (2002) 23 *ILJ* 1743.

Court, L, Warmington, C. ‘The workplace privacy myth: why electronic monitoring is here to stay’ (2004) 9(1) *Oklahoma City University Law Review*

Dancaster, L ‘Internet abuse: a survey of south african companies’ (2001) 22 *ILJ* 862.

Dekker, A ‘Vices or devices: employee monitoring in the workplace’ (2004) 16(4) *SA Merc LJ* 624.

Dennis, CM., ‘Legal implications of employee social media use’ (2011) 93(4) *Massachusetts Law Review*

De Waal, J., Currie, I. Erasmus, G. *The Bill of Rights Handbook* 3 ed Cape Town: Juta (2000).

Etsebeth, V ‘The growing expansion of vicarious liability in the information age (part 1)’ (2006) 2 *TSAR* 564.

Etsebeth V, ‘The growing expansion of vicarious liability in the information age (part 2)’ (2006) (4) *TSAR* 755.

Evans, K. ‘Hosking v Runting balancing rights in a privacy tort’ (2004*)* 28 *Privacy Law and Policy Reporter*.

Fitzgerald BF, ‘Web 2.0, social networking and the courts’ (2012) *Australian Bar Review* 281-301.

Grimmelman, J. ‘Saving facebook’ (2009) 94 *IOWA LR* 1134.

Hale, B. ‘The history of social media: social networking revolution’ (2015) *History Co-operative* 6*.*

Ireton, J., ‘Social media: what control do Employers have over employee social media conduct in the workplace?’ (2014) 5(14) *Houston Business and Tax Law Journal* 144-179.

Jacobson, W., Tufts, S., ‘To post or not to post: employee rights and social media’ (2014) 33(1) *Review of Public Personnel Administration 84*-107.

McDonald P, Thompson, P. ‘Social media(tion) and reshaping of public/private boundaries in employment relations’ (2016) 18 *International Journal of Management Reviews* 69-84.

McGinley, Ann C. and McGinley-Stempel, Ryan P. ‘Beyond the water cooler: speech and the workplace in an era of social media’ (2012) 30(1) *Hofstra Labor and Employment Law Journal.*

McGregor, M ‘The right to privacy in the workplace: general case law and guidelines for using the internet and e-mail’ (2004) 16(3) *SA Merc LJ* 638.

Millard.,D and Baskaran, EG., Employers’ ‘Statutory vicarious liability in terms of the protection of personal information act’ (2016) 19 *PER/PELJ*.

Modiba, M ‘Intercepting and monitoring employees’ e-mail communication and internet access’ (2003) 15 *SA Merc L* 365.

Morgan, C., ‘Employer monitoring of employee electronic mail and internet use’ (1999) 44 *McGill Law Journal* 849-902.

Mussen, PH. ... et al. *Child Development and Personality* 6 ed New York: Harper & Row Publishers (1990)

Mutula, S.M. ‘Policy gaps and technological deficiencies in social networking environments: implications for information sharing’ (2013) 15(1) *SA Journal of Information Management*

Neethling, J., Potgieter, JM., Visser, PJ. *Law of Delict* (1st ed.) Durban: Butterworths (2000).

O'Brien., 'The national labor relations board: perspectives on social media' (2014) 8 *Charleston Law Review* 411-426.

O'Brien, CN., 'The top ten nrlb cases on facebook firings and employer social media policies' (2014) 92(2) *Oregon Law Review* 337-353.

Papandrea, M-R, 'Social media, public school teachers and the first amendment' (2012) 90 *North Carolina Law Review* 1597-1642.

Park, S. 'Employee internet privacy: a proposed act that balances legitimate employer rights and employee privacy' (2014) 51(4) *American Business Law Journal* (PAGE NUMBER/S).

Penk, S., & Tobin, R. *Privacy Law in New Zealand* 2 ed Auckland: Reuters (2016).

Pike, G., 'Social media and the workplace' (2014) 31(9) *Information Today*

Pistorius, T 'Monitoring, interception and big boss in the workplace: is the devil in the detail?*'* (2009) 1 *PER*

Roos, A., 'Personal data protection in New zealand: lessons for south africa?' (2008) 4 *PER*

Roos, A *'*Privacy in the facebook era: a south african perspective' (2012) 129 *SALJ* 378.

Steinmann, R, 'The Core Meaning of Human Dignity' (2016) *PER /PELJ (19)*

Stoddart, J. "Privacy in the era of social networking: legal obligations of social media sites "*University of Saskatchewan College of Law lecture series. Saskatoon, Saskatchewan.* November 22, 2010.

Swales, L 'Protection of personal information: south africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' (2016) 49 *SA Merc Law Journal*

Van Jaarsveld, M 'Forewarned is forearmed: some thoughts on the inappropriate use of computers in the workplace' (2004) 16 *SA Merc LJ* 651.

Internet Sources:

History of the Document (DATE) available at http://www.un.org, accessed on 6 March 2018.

Miniwatts Marketing Group*: Internet World Stats*, available at http://www.internetworldstats.com, accessed on 12 November 2017.

Omnicore Group, available at http://www.omnicoreagency.com, accessed 5th March 2018.