Freedom of Speech, the Right to Privacy, Defamation or Misconduct:

What rights do employees have when making workplace-related statements on social networking websites, and what of the rights of the employer? A critical analysis of legislation and case law, both in South Africa and internationally.

Caroline Simoes

THCCAR001

Research dissertation presented for the approval of Senate in fulfilment of part of the requirements for the degree of MPhil (Labour Law) in approved courses and a minor dissertation. The other part of the requirement for this qualification was the completion of a programme of courses.

Supervisor: Prof Alan Rycroft

September 2011

DECLARATION

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

2. I have used the footnote convention for citation and referencing. Each contribution to, and quotation in, this assignment from the work(s) of other people has been attributed, and has been cited and referenced.

3. This assignment is my own work.

4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

5. I acknowledge that copying someone else's assignment, or part of it, is wrong and declare that this is my own work.

6. I hereby declare that I have read and understood the regulations governing the submission of MPhil (Labour Law) dissertations, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation conforms to those regulations.

Signature: Signed by candidate Student No.: **THCCAR001**

ABSTRACT

The rapid global expansion of social networking, and its impact in the workplace, is leading to increasing pressure on both employers and employees to monitor and manage their interactions on such media more carefully, in order to protect the employment relationship, and both individual and company reputations in the wider public arena. The purpose of this paper is to critically analyse the rights of both employers and employees with regards to comments and statements made on social networking sites, particularly with regards to the potential impact of such statements in the workplace. The paper will assess the tension between the individual's rights to freedom of speech and privacy, as compared to the employer's right not to be defamed, or for its employees to commit misconduct in the workplace. This analysis will consist of an assessment of both the South African and international situation – including the United States of America, United Kingdom, Australia, New Zealand and Canada; by critically analysing legislation, case law and other literature on the topic relating to these particular geographical regions. The result of the research shows that there is a complex interplay between the relevant individual and employer rights, and that the courts will be required to assess all of the facts in totality in relation to a given matter in order to determine whether or not a dismissal for comments made via social media is fair. This will include an assessment of the risks posed to both parties, including breach of employee privacy rights, through the illegitimate accessing of their postings, as well as the risk to employers of vicarious liability, for actions by their employees during the scope of their employment which may negatively impact third parties. On this basis the paper will recommend that employers implement clear and detailed policies with regards to the usage of social networking sites in, or related to, the workplace; and that employees

utilize other mechanisms available to them for airing frustrations and grievances, such as, internal grievance procedures and employee assistance programmes; in order not to be found guilty of misconduct based on comments made via social networking media.

TABLE OF CONTENTS

1. Introduction and Overview of the Topic

"While the decision to post videos, pictures, thoughts, experiences, and observations to social networking sites is personal, a single act can create far-reaching ethical consequences for individuals as well as organizations. Therefore, it is important for executives to be mindful of the implications and to elevate the discussion about the risks associated with it to the highest levels of leadership."[1]

Sharon L. Allen

Chairman of the Board

Deloitte LLP

In the last number of years, social networking has rapidly increased in popularity across the globe. Today millions of users interact on these websites with varying degrees of public accessibility to their personal information and communications.

A Social Network Service may be defined as, *'...an online service, platform, or site that focuses on building and reflecting of social networks or social relations among people...'*[2] It may also be defined as, *'...Internet-based services that provide individuals a way to interact with each other online.'*[3] The main examples of Social Network Services are Facebook, Twitter, MySpace, Linkedln, Nexopia and Bebo, although there are

[1] Available at: http://www.deloitte.com/dtt/cda/doc/content/us_2009_ethics_workplace_survey_150509.pdf [Accessed: 18 January 2010].
[2] Available at: http://en.wikipedia.org/wiki/Social_network_service [Accessed: 8 December 2010].
[3] Available at: http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm [Accessed: 18 January 2010].

numerous other such services, ranging in popularity depending on geographical location.

Social networking started with the Bulletin Board System (BBS) – online meeting places allowing users to communicate with a central system, and post messages to other users. These were often used by hobbyists with similar interests for connecting – and often technology-related.[4] BBS was closely followed by another forum – CompuServe – a business-orientated mainframe computer communication solution, which expanded into the public arena in the 1980s. This system provided for the first discussion forums; rather than being limited to the ability to send a message only.[5] And, finally, there was America Online (AOL), with member-created communities and member-profiles, which most closely mirrored social networking as we know it today.[6]

By the mid 1990s the internet had taken off, and early social networking media included Classmates.com – a service allowing users to access old school friend – and SixDegrees.com. However, it was only in 2002 that social networking really took off with the launch of Friendster, which boasted more than three million registered users a year following its launch. LinkedIn followed a year later, and focused more on networking between business people; and MySpace launched around the same time and was estimated to have approximately ninety million users by 2009.[7]

---

[4] Available at: http://www.digitaltrends.com/features/the-history-of-social-networking/ [Accessed: 13 January 2011].
[5] Available at: http://www.digitaltrends.com/features/the-history-of-social-networking/ [Accessed: 13 January 2011].
[6] Available at: http://www.digitaltrends.com/features/the-history-of-social-networking/ [Accessed: 13 January 2011].
[7] Available at: http://www.digitaltrends.com/features/the-history-of-social-networking/ [Accessed: 13 January 2011].

However, it is Facebook – launched in 2004 – that is now the social networking leader – passing the four hundred million user mark in 2010.[8] It is believed that one of the secrets to Facebook's success is that it promotes honesty and openness – available for all to see.[9] Of course, from an individual and employer-impact perspective, this could also be one of its drawbacks.

Facebook has been the predominant forum noted in workplace discipline, and other similar matters, which have recently arisen in the media. Facebook's terms of use specify that, *'...the website is available for your personal, non-commercial use only.'*[10] This has led many to the view that information from the site may not be used by police, employers, and school administration, amongst others, to conduct criminal or other investigations. However, Facebook itself has confirmed that it is a public forum, and information shared on the site is deemed accessible to the general public. Legal practitioners have generally agreed with this view.[11]

The result of the public nature of many of these social networking interactions is that various communications invariably come to the attention of employers – often with negative results in the workplace. Increasingly one hears of disciplinary and court action as a result of statements made on such websites about employers, colleagues, or the

---

[8] Available at: http://www.mashable.com/2010/02/04/ [Accessed: 14 January 2010].
[9] Available at: http://www.digitaltrends.com/features/the-history-of-social-networking/ [Accessed: 13 January 2011].
[10] Available at: http://www.facebook.com/terms.php [Accessed: 11 February 2011].
[11] Available at: http://www.browndailyherald.com/2.12231/the-facebook-not-just-for-students-1.1679665 [Accessed: 11 February 2011]; http://en.wikipedia.org/wiki/Use_of_social_network_websites_in_investigations [Accessed: 11 January 2011].

working environment, to name but a few. This research paper will, through a comparative study between South Africa and other countries, seek to identify principles that should govern the situation, and which achieve a balance between employer and employee rights and interests.

Different workplaces and countries have tackled such alleged misdemeanours in different ways – from civil litigation for defamation of character; to workplace dismissals for misconduct; and, in South Africa, even as a criminal act, specifically crimen injuria. However, various sources and individuals have retaliated by stating that this utilisation of information obtained from such sites is an invasion of privacy, and that one is entitled to freedoms of speech and expression.

This paper will critically analyse the nature of statements made on social networking sites – whether there is a right to privacy of such communications - and whether such statements amount to freedom of speech and/ or expression, or whether action for defamation and/ or workplace misconduct is justifiable in such circumstances. In addition, the paper will examine the different approaches adopted globally to such matters, including a comparison between the South African situation, and internationally.

2. Review of the Legislation and Definitions

In this section the focus will be on the review of relevant legislation with regards to issues of privacy, freedom of speech and expression, and defamation, amongst other similar matters. This will be both from the South African perspective, as well as from perspectives in various international contexts, such as, the United States of America, the United Kingdom, Australia, New Zealand and Canada. These particular countries were chosen for both their similarities and differences to South African legislation, as well as the fact that, as developed nations, they have had some of the longest histories of social networking, resulting in comparatively more developed case law in this regard, as compared to various of their counterparts. In addition, I will attempt to define some of the key concepts to be dealt with in this paper.

Starting with relevant legislation in South Africa, the *Constitution of the Republic of South Africa*[12] states in the Bill of Rights:

'14. Privacy

> *Everyone has the right to privacy, which includes the right not to have-*
>
> > *a. their person or home searched;*
> >
> > *b. their property searched;*
> >
> > *c. their possessions seized; or*

[12] Of 1996.

d. the privacy of their communications infringed.

15. Freedom of religion, belief and opinion

1. Everyone has the right to freedom of conscience, religion, thought, belief and opinion...

16. Freedom of expression

1. Everyone has the right to freedom of expression, which includes

a. freedom of the press and other media;

b. freedom to receive or impart information or ideas;

c. freedom of artistic creativity; and

d. academic freedom and freedom of research.

2. The right of subsection (1) does not extend to...

c. advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm.'

The right to privacy in South Africa includes an individual's right not to have his or her communications infringed. In addition, the right to freedom of media, and to impart information or ideas, is also protected. However, in terms of Section 36 of the Constitution, all rights may be limited on a justifiable basis, as follows:

'36. Limitation of rights

1. 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-

a. the nature of the right;

b. the importance of the purpose of the limitation;

c. the nature and extent of the limitation;

d. the relation between the limitation and its purpose; and

e. less restrictive means to achieve the purpose.'

Had Section 36 not been included in the Constitution, it might have been argued that the rights as contained in the Bill of Rights were absolute, and could not be departed from. However, Section 36 provides parameters for when these rights may be deviated from, as long as it is reasonable and justifiable to do so. The courts have determined that, in order to do so, this must involve a balancing of all the different interests at hand.[13] Each of the criteria must be carefully considered in its own right. However, in the context of the labour statutes, it is argued that one of the considerations which should weigh most heavily when determining 'the importance of the purpose of the limitation' is the extent to which such limitation promotes one or more of the objects of the Act. If able to do so, this will provide strong proof of the importance society attaches to the purpose of the limitation. In this way, for

[13] *S v Makwanyane* 1995 (6) 665 (CC) 104; Available at: http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter7.htm [Accessed: 7 February 2011].

example, with reference to the South African *Labour Relations Act* (LRA); where a statutory provision may have constituted an infringement in relation to a fundamental right (such as to freedom of expression or privacy) as contained in the Bill of Rights; such provision may re-enter the enquiry on the basis of the limitation clause of the Constitution. Should a provision in the LRA then pass the limitation tests, there will be no requirement to interpret this restrictively.[14]

In comparison to South Africa, the Bill of Rights of the United States of America states in the First Amendment with regards to Freedom of Religion, Press and Expression:

'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.'[15] As such, the First Amendment limits the actions that American Congress can impose, but this does not provide for a 'right' to demean others.[16]

In terms of a right to privacy, and unlike South Africa, the United States Constitution contains no such express right. However, the Bill of Rights does protect certain aspects of privacy, such as the privacy of beliefs as contained in the First Amendment. Further, the Ninth Amendment states that, *'...the enumeration of certain rights...shall not be construed to*

---

[14] Du Toit et al, *Labour Relations Law: A Comprehensive Guide* 5ed (2006) LexisNexis Buttorworths at 70-71.

[15] Available at: http://www.constitution.org/billofr .htm [Accessed: 8 December 2010].

[16] Available at: http://www.examiner.com/human-resources-in-jackson/free-speech-and-social-networking-sites-the-employment-issue#ixzz1Bksg1C6N [Accessed: 22 January 2011].

deny or disparage other rights retained by the people.' In addition, as early as 1923, the Supreme Court endorsed a broad reading of the 'liberty' guarantee of the Fourteenth Amendment, guaranteeing a fairly broad right to privacy.[17] It is generally agreed that the first publication advocating the right to privacy in the United States of America was an article by Samuel Warren and Louis Brandeis in 1890 entitled, *The Right to Privacy, 4 Harvard L.R. 193.*[18]

In terms of other legislation, the United States is also subject to the *Stored Communications Act, 18 U.S.C. 2701* (SCA). This Act regulates when an electronic communications service provider may or may not disclose information about a client's emails, or other electronic communications, to third parties. Disclosure of contents is strictly regulated, and may not even be disclosed to civil litigants when presented with a civil subpoena. Confidentiality is therefore of the utmost importance.[19] This Act was passed in 1986 as part of the *Electronic Communications Privacy Act,* aimed at addressing privacy issues related to the advent of the Internet. However, at this time the Internet was in its infancy and social networking as we know this today was non-existent. As such, the Act – which to date has not been amended – has failed to keep abreast of the pace of changing technology. This has resulted in a reliance on the courts to apply old statute to modern technology and electronic communication disclosure matters.[20]

---

[17] Available at: http://law.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html [Accessed: 24 January 2011].

[18] Available at: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [Accessed 11February 2011]; http://en.wikipedia.org/wiki/Privacy [Accessed: 24 January 2011].

[19] Available at: http://ilt.eff.org/index.php/Privacy:_Stored_Communications_Act [Accessed: 7 February 2011].

[20] Available at: http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id [Accessed: 7 February 2011].

Other legislation includes; the *Uniform Electronic Transactions Act* (UETA), which creates incentives for the obtaining of cyber-security by placing liability for transmission errors on the shoulders of the party without the relevant security to prevent such errors; and the *Computer Fraud and Abuse Act* (CFAA), which provides for civil and criminal liability for those who do not provide adequate safeguards on computers used in interstate commerce, and on those who intentionally access such computers. However, the *National Strategy to Secure Cyberspace* has had the most significant impact on the protection of online privacy in the USA. Its purpose is to define corporate responsibility in this field. Despite this, it focuses on voluntary partnership with the private sector, and so does not have the force of legislation.[21]

Turning to the United Kingdom, its Bill of Rights of 1689 allowed for Freedom of Speech in parliament, stating, *'That the Freedome (sic) of Speech and Debates or Proceedings in Parlyment (sic) ought not to be impeached or questioned in any Court or Place out of Parlyment (sic).'*[22]

Regarding privacy, in the United Kingdom it is not possible to bring an action for the invasion of privacy – this will usually be brought via another means, such as breach of confidence. However, it may at times be defensible that a disclosure of information was in the public interest.[23] Despite this, the coming into effect in the U.K. of the *Human Rights Act of 1998* has meant that the law has developed, and the individual has significantly more opportunity for protecting their right to

---

[21] Etsebeth, V. *Information privacy protection – legal fallacy or reality?* (2007) 70(4) *THRHR* 571.
[22] Available at: http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1518621 [Accessed: 8 December 2010].
[23] Available at: http://news.bbc.co.uk/2/hi/uk_news/4482073.stm [Accessed: 11 February 2011]; http://en.wikipedia.org/wiki/Privacy [Accessed: 24 January 2011].

privacy.[24] In this regard, Article 8 of the Act states, *'(1) Everyone has the right for his private and family life, his home and his correspondence; (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder and crime, for the protection of health and morals, or for the protection of the rights and freedoms of others.'*[25]

Similarly, this particular Act further entrenched the right to freedom of expression in the United Kingdom in Article 10, which states, *'(1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers...(2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society...'*[26]

In terms of information privacy legislation, the United Kingdom is governed mainly by two directives. The *European Union Directive 95/46/EC* aims at protecting personal data from abuse by regulating the collection of such data. It was implemented by the *Data Protection Act of 1998*, which sets out rules governing the processing of personal information. Secondly, the *Telecommunications Data Protection Directive, or European Union Directive 97/66/EC*, aims to regulate the use of

[24] Available at: http://www.yourrights.org.uk/yourrights/privacy/ [Accessed: 24 January 2011].
[25] Available at: http://news.bbc.co.uk/2/hi/uk/946400.stm [Accessed: 24 January 2011].
[26] Available at: http://news.bbc.co.uk/2/hi/uk/946400.stm [Accessed: 24 January 2011].

information which does not necessarily qualify as personal information, and the application of law to all juristic persons. As such, it aims to ensure protection for fundamental rights and freedoms, including the right to privacy, specifically regarding the processing of personal information in the telecommunications arena. It is implemented by way of the *Telecommunications Regulation 1999.*[27]

Similar to South Africa, the *New Zealand Bill of Rights Act*[28] states:

'13. Freedom of thought, conscience and religion

Everyone has the right to freedom of thought, conscience, religion, and belief, including the right to adopt and to hold opinions without interference.

14. Freedom of expression

Everyone has the right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind and in any form.'[29]

In terms of a right to privacy in New Zealand, Article 21 of the Bill of Rights states, *'Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.'* The New Zealand Court of Appeal has interpreted this article

[27] Etsebeth, V. *Information privacy protection – legal fallacy or reality?* (2007) 70(4) *THRHR* 571.
[28] 1990 No.109.
[29] Available at: http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html [Accessed: 8 December 2010].

in a number of cases as protecting the interests that make up the right to privacy. In addition, the *New Zealand Privacy Act* came into effect in 1993, and has subsequently been amended. Its purpose is to regulate the collection, use and dissemination of personal information in both the private and public sectors. One controversial piece of legislation introduced to the New Zealand parliament in 2002 is the *Telecommunications Interception Capabilities Bill*, which would require all Internet Service Providers (ISPs) and telephone companies to upgrade their systems in order to assist law enforcement agencies to intercept communications, without the individual's permission to do so.[30]

The Australian Constitution does not have any express provision relating to free speech. However, since 1992, various decisions of the High Court have indicated an implied right to freedom of speech and communication, particularly with regards to politics and government. Despite this, Australian law in its current form does not in fact protect fundamental freedoms – although the High Court does already protect rights through its interpretation of the Constitution and the common law. This makes Australia alone amongst like-minded countries not providing for freedom of speech either in the Constitution or its legislation.[31]

In addition, Australia does not have a constitutional right to privacy, although there are some pieces of legislation which provide limited protection. For example, the *Neighbouring Land Act*[32] records the

---

[30] Available at: http://www.privacyinternational.org/survey/phr2003/countries/newzealand.htm [Accessed: 24 January 2011].
[31] Available at: http://www.aph.gov.au/LIBRARY/pubs/rn/2001-02/02rn42.htm [Accessed: 24 January 2011].
[32] (No. 2) 2000 (NSW).

desirability for people to live in harmony, but does not confer an absolute right to privacy on individuals. Similarly, the *Privacy Act, 1988* provides protections regarding the collection, use and disclosure of personal information, but does not sufficiently protect the invasion of privacy. This Act is deemed, however, to have extended the law on confidentiality.[33]

Despite this, recent case law suggests that Australians may have a common law right to privacy. For example, in the matter of *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2002) 208 CLR 199*, the court found that – despite it not being so in the particular case before them – a court was not prevented from finding that there is a tort (or legal cause of action) of unjustified invasion of privacy, although they did find that this was limited to natural persons, and did not extend to corporations or other legal entities. This view was supported by the court in the matter of *Grosse v Purvis [2003] QDC 151*.[34]

Turning to Canada, the *Canadian Bill of Rights*[35] states in Section 1, *'It is hereby recognized and declared that in Canada there have existed and continue to exist without discrimination by reason of race, national origin, colour, religion or sex, the following human rights and fundamental freedoms, namely, ...*

> *d. freedom of speech;*
>
> *f. freedom of the press.'*

[33] Available at: http://www.hrcr.org/safrica/privacy/austr_law.html [Accessed: 24 January 2011].
[34] Parliament of Australia Research Note. 14 March 2005, no. 37, 2004-05, ISSN 1449-8456.
[35] 1960, c. 44.

As regards privacy, there is no explicit right to privacy in the Canadian Constitution[36], and privacy law in Canada is federally governed by numerous Acts, including the *Canadian Charter of Rights and Freedoms*, and the *Privacy Act.* Data privacy was first addressed by means of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[37] Section 8 of Canada's Charter of Rights and Freedoms grants an individual's right against unreasonable search and seizure and, on this basis, the courts recognized an individual's right to a reasonable expectation of privacy.[38]

More generally, in 1948 the United Nations General Assembly adopted the *Universal Declaration of Human Rights*, which states in Article 19, *'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.'* In addition, Article 19 of the 1966 United Nations *International Covenant on Civil and Political Rights* states, *'Everyone shall have the right to freedom of expression...'*[39]

Further, in 1944 the International Labour Organisation (ILO) rephrased and broadened its aims and purposes in what was named the *Declaration of Philadelphia*, and which was incorporated into the amended constitution of the ILO, to include the proviso that freedom of

---

[36] Available at: http://www.privacyinternational.org/survey/phr2003/countries/canada.htm [Accessed: 24 January 2011].
[37] Available at: http://en.wikipedia.org/wiki/Privacy [Accessed: 24 January 2011].
[38] Available at: http://www.privacyinternational.org/survey/phr2003/countries/canada.htm [Accessed: 24 January 2011].
[39] Available at: http://www.aph.gov.au/LIBRARY/pubs/rn/2001-02/02rn42.htm [Accessed: 24 January 2011].

expression (and association) is essential to sustained progress.[40] In 1996 the ILO further adopted a code of good practice on the protection of employees' private information, and is regarded as the standard for the protection of employees' privacy rights. Such protections include:

- Coverage of both public and private sector employees;
- Employees should be notified of information collection processes;
- Information collected should be used lawfully and fairly;
- Employers should collect the minimum necessary information required for employment;
- Information should only be collected with the employee's consent;
- Information should only be used for purposes directly related to employment, and for the purpose for which it was initially collected;
- Information should be securely stored;
- Employees should be able to access this information;
- Information should not be provided to third parties without the employee's consent, except to comply with a legal requirement;
- Employees cannot be required to waive their right to privacy;
- Medical information is confidential;
- Certain information, such as that related to sexual orientation, political and religious beliefs, for example, should not be collected;
- Certain information collection techniques, such as polygraph testing, should be prohibited.[41]

What of the concept of 'defamation'? Defamation may be defined as, *'...the communication of a statement that makes a claim, expressly stated or implied to be factual, that may give an individual, business, product,*

[40] Available at: http://www.nationsencyclopedia.com [Accessed: 9 February 2011].
[41] Available at: http://epic.org/privacy/workplace/default.html [Accessed: 9 February 2011].

group, government, or nation a negative image." It is usually a requirement that this claim be false and that the publication is communicated to someone other than the person defamed (the claimant).[42] Similarly, *'...the act of defaming; false or unjustified injury of the good reputation of another, as by slander or libel; calumny...* [43] may further explain this concept. The term 'libel' is specifically used when referring to written, broadcast or otherwise published communication.[44]

In the United States of America – where matters relating to defamation are more regularly dealt with than in many other countries - the law defines defamation as, *'...spoken or written words that are false and/ or misleading, that gives the defamed a negative image, and/ or hurts their reputation.'*[45] The defamatory comment must be made to someone other than the person defamed by the comment, and the law also differentiates between written (libel) and spoken (slander) defamation. Under the *Communications Decency Act*, the owner of a social networking website cannot be held liable for defamatory comments made on the site, unless he or she actively gathers the relevant data from the user which ultimately leads to the defamatory comment. However, anyone making such a comment on a social networking site may be held liable for such statements.[46]

---

[42] Hankin, R. *Navigating the Legal Minefield of Private Investigations: A Career-Saving Guide for Private Investigators, Detectives, and Security Police* (2008) Looseleaf Law Publications at 59; available at: http://en.wikipedia.org/wiki/Defamation [Accessed: 13 December 2010].
[43] Available at: http://dictionary.reference.com/browse/defamation [Accessed: 13 December 2010].
[44] Available at: http://dictionary.reference.com/browse/libel [Accessed: 11 February 2011]; http://en.wikipedia.org/wiki/Defamation [Accessed: 13 December 2010].
[45] Available at: http://phillipsgivenslaw.blogspot.com/2009/06/defamation-and-social-media.html [Accessed: 19 January 2010].
[46] Available at: http://phillipsgivenslaw.blogspot.com/2009/06/defamation-and-social-media.html [Accessed: 19 January 2010].

Most jurisdictions allow for legal action in the event of alleged defamation, and this may amount to either civil or criminal litigation – or both. [47] South Africa has a unique point of law referred to as 'crimen injuria'. Crimen Injuria may be defined as the act of, *'...unlawfully, intentionally and seriously impairing the dignity of another...'*, and it is considered a criminal act, prosecutable by the state.[48]

A further concept of importance – particularly for employers – is that of vicarious liability. In South Africa, an employer may be held accountable for a delict by an employee where it can be shown that:

- The employee is liable for the delict;
- The employment relationship existed at the time the delict was committed;
- The delict was committed during the course and scope of employment.[49]

In terms of further relevant legislation, South Africa also has the *Regulation of Interception of Communications Act* (RICA), which allows employers, in certain instances, to intercept and monitor communications, including emails, phone calls, internet activity, amongst other mediums.[50] Communication includes both direct and indirect communication. Indirect communication specifically includes phone calls, intranet, Internet, fax, email messages, SMS messages,

---

[47] Available at: http://en.wikipedia.org/wiki/Defamation [Accessed: 13 December 2010].
[48] Clark, D.M. *South African Law Reform Commission Issue Paper 22 Project 130: Stalking* (2003) South African Law Commission. ISBN 0-621-34410-9; Available at: http://en.wikipedia.org/wiki/Crimen_injuria [Accessed: 11 January 2011].
[49] Available at: http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter7.htm [Accessed: 7 February 2011].
[50] Available at: http://www.itnewsafrica.com/?p=3380 [Accessed: 19 January 2010].

tracking devices on company cars, and voice-mail messages. The instances where interception of such communications is allowed include, by prior written consent, and in connection with the employer's right to carry on its business.[51] Subsequent to RICA, the *Electronic Communications and Transactions Act* (ECTA) was introduced in South Africa in 2002 – aimed at removing barriers previously hampering the validity of electronic consent.[52] It also aims to protect personal information as obtained via electronic transactions.[53]

The *Interception and Monitoring Prohibition Act 127 of 1992* prohibits the interception and monitoring of telephone conversations, postal articles and, subsequently, electronic, or Internet, communications, unless a detailed prior procedure has been met. Contravention may be criminal in serious matters. The act of interception must be intentional, and without any knowledge or consent of the sender of the communication, in order to be prohibitive.[54]

The *Protection of Personal Information Bill* is founded on eight core principles, as follows:

- Information may only be collected or stored if necessary for an explicitly defined purpose, and if this does not unreasonably intrude on the privacy of the data subject;

---

[51] Pistorius, T. *Monitoring, interception and Big Boss in the workplace: is the devil in the details? [2009] PER 1.* Available at: http://www.saflii.org/za/journals/PER/2009/1.html [Accessed: 6 January 2011].
[52] Pistorius, T. *Monitoring, interception and Big Boss in the workplace: is the devil in the details? [2009] PER 1.* Available at: http://www.saflii.org/za/journals/PER/2009/1.html [Accessed: 6 January 2011].
[53] Etsebeth, V. *Information privacy protection – legal fallacy or reality?* (2007) 70(4) *THRHR* 571.
[54] Mischke, C. *The monitoring and interception of electronic communications: Obtaining and using email and other electronic evidence* (2001) May Vol. 10(10) *CLL* 91.

- Information must be collected from, and with, the subject's consent;
- Such subjects must be informed in advance of the purpose of such collection, and the intended recipients;
- Information must not be kept for longer than necessary;
- Information must not be distributed in a manner which is incompatible with the purpose of collection;
- Reasonable steps must be taken to ensure the information is accurate, updated and complete;
- Appropriate measures must be taken to safeguard the data from loss, damage, destruction or unauthorised access;
- Data subjects are allowed access to their information, and to demand correction of inaccuracies.[55]

Finally, the *Protected Disclosures Act, 2000*[56] - also termed the 'Whistleblower's Act' – makes provision by which employees in both private and public sectors in South Africa may disclose information regarding the irregular or unlawful conduct of employers or fellow employees. Employees making such disclosures are protected by the Act from being subjected to an occupational detriment.[57]

---

[55] Etsebeth, V. *Information privacy protection – legal fallacy or reality?* (2007) 70(4) *THRHR* 571.
[56] Act 26 of 2000.
[57] Available at: http://www.workinfo.com/free/Sub_for_legres/data/Disclosure/protected.htm [Accessed: 31 January 2011].

3. Literature and Case Law Review

In general, in its 2009 survey on social networking and reputational risk in the workplace,[58] Deloitte LLP found that the rapid growth of online social networking had led to a blurring of the lines between peoples' private and professional lives, which may present ethical challenges for both individuals and businesses.[59]

74% of employed American citizens surveyed in the study expressed the view that social networking may damage a brand's reputation.[60] Despite this, it was found that only 15% of executives surveyed were addressing such risks;[61] despite 58% of those surveyed agreeing that it is important to do so. And, more importantly, only 17% had programmes in place to monitor and mitigate potential risks in the workplace related to the usage of social networking sites.[62]

Further to this - and as one would expect – it was found that employer and employee opinions on the use of social networking differed. 60% of executives felt that they had a right to know how employees were portraying themselves and the business online; while 53% of surveyed employees felt this was, *'...none of the employer's business.'*[63]

---

[58] Available at: http://www.deloitte.com/dtt/cda/doc/content/us_2009_ethics_workplace_survey_150509.pdf [Accessed: 18 January 2010].
[59] At 2.
[60] At 4.
[61] At 5.
[62] At 2.
[63] At 2.

Deloitte's findings were that organisations should establish clear policies and guidelines for social networking usage by employees. However, despite this, the survey also found that, for nearly half of the respondents, such policies would probably not change how they interacted on such networks;[64] and that attempts to mitigate the potential risks should include emphasis on culture, values and ethics within the organisation, as this was deemed to encourage good decision-making in online interactions.[65]

More specifically, in conducting this review of the relevant case history and literature, a review of the South African scenario will be conducted, as compared and contrasted to the international situations in the United States of America, United Kingdom, Australia, New Zealand and Canada.

3.1 South Africa

According to Dancaster,[66] due to the now prevalent use of computers in the workplace, new employment issues are arising for employers, who must balance potential liability and loss of productivity issues against employees' rights to privacy. McGregor[67] identified four main problems associated with the use of email and the Internet at work, namely:

---

[64] At 7.
[65] At 2.
[66] Dancaster, L. *Internet Abuse: A Survey of South African Companies* (2001) *ILJ* 862.
[67] McGregor, M. *The use of email and the Internet at work* (2003) *Juta's Business Law* Vol 11(3) at 189-192.

- Employers may face liability for employees' Internet and email usage;
- Internal company networks may contract viruses;
- Overuse causes the failure to do assigned work, delays, and system blockage;
- Disciplinary action against employees who have breached workplace rules regarding email and Internet usage increases.[68]

Hence the need for comprehensive and enforceable Internet usage policies – including regarding the accessing of social networking sites.

South Africa has to date had limited case history related specifically to the misuse of communication on social networking media in – or related to – the workplace (although this seems to be on the rise in 2011). As such, it will be largely necessary to examine matters relating to social networking outside of the workplace, as well as workplace matters utilizing other electronic media - which may provide a clue for how employers should deal with such matters specifically relating to social networking, should these arise.

However, in a recent media report in South Africa, a director of Cliffe Dekker Hofmeyr law firm, John Botes, stated, *'Employees may end up facing dismissal if what they say on social networking sites impacts on their employer's business or the relationship between them and their employer or colleagues.'* He stated that employees using such social networking sites should, as a rule, not say anything on such sites that they would hesitate to say at the 'monthly staff meeting'. He went on to

[68] At 189-190.

say that the law requires that employees refrain from acting in a manner which may destroy harmonious working relations with the employer or peers, and that they have a duty to act in good faith towards employers, including the duty to further its business interests. As such, using a social networking tool in the public arena to communicate with others could impact the employer's business – hence opening the door for an employer to take disciplinary action against the employee.[69]

Making unpleasant statements on social networking sites may be in breach of more than one of the common law duties toward the employer, including, but not limited to:

- To maintain reasonable efficiency;
- To act in the best interests of the employer;
- To act in a respectful and obedient manner;
- To refrain from general misconduct. [70]

Regarding activity on social networking media specifically, but not in the workplace, in 2009 a South African man, Duane Brady, was charged for posting defamatory statements on his Facebook profile, resulting in his arrest. He was charged with crimen injuria – a criminal offence committed when one deliberately injures another's dignity - and common assault. [71] The defamatory Facebook posts were left for a friend of his wife – alluding to her alleged use of drugs and sexual activities. Attorney, Peter Grealy, of Webber Wentzel law firm commented that

---

[69] Available at: http://www.irnetwork.co.za/nxt/gateway.dll?f=templates$fn=default.htm$vid=irnetwork:10.1048/enu [Accessed: 1 October 2010].

[70] Available at: http://www.labournet.co.za/NewsItem.aspx?ID=339f3e63-f912-4fd6-8d76-440006ffb589 [Accessed: 14 December 2010].

[71] Available at: http://www.itnewsafrica.com/?p=3380 [Accessed: 19 January 2010].

such statements could definitely be deemed defamatory. However, the difficulty lies in proving a specific individual is responsible. Further, some videos and postings could be viewed as an invasion of privacy and/ or as derogatory in nature. This case was the first of its nature in South Africa, but it is expected that similar matters will arise more frequently in the future.[72] Further, it is possible that similar activity in the workplace might result in charges not just limited to internal misconduct.

In another matter, Donn Edwards was sued for making disparaging statements on a blog about the Holiday Vacation Club. This matter, however, seems to have been a genuine expression of freedom of speech, and was ultimately settled out of court.[73]

A further matter concerning social networking specifically, but not relating to the workplace; in the matter of *Botha & Another v Creecy NO & Others*[74] a high school learner recorded various derogatory and insulting statements on Facebook about the teachers and school, following his subjection to initiation which he found traumatic, and which resulted in him dropping out of school prior to Grade 11 exams.[75] Disciplinary action resulted. However, during subsequent talks it was agreed that the learner would be promoted to Grade 12 due to his outstanding academic record. Despite this, the learner later claimed the school had reneged on this agreement, resulting in a court case against the Department of Education.

---

[72] Available at: http://mybroadband.co.za/news/Internet/6580.html [Accessed: 19 January 2010].
[73] Available at: http://saulk.co.za/2009/01/16/crimen-injuria/ [Accessed: 11 January 2011].
[74] [2010] JOL 251847GSJ.
[75] Available at: http://www.news24.com/SouthAfrica/News/Pupil-takes-dept-to-court-20100201 [Accessed: 27 January 2011].

In a workplace-specific matter in the previous year, a Durban man was dismissed after making derogatory comments about his manager on Facebook. Further to this, two other employees were suspended following comments made on Facebook – one for comments regarding his employer's laziness, and the other for promoting a competitor's product on her profile page.[76] Although these matters were dealt with utilising the employer's internal codes of conduct, it is not inconceivable that these matters might also have resulted in external claims of defamation in some of these instances.

Most recently, the CCMA has begun seeing similar matters referred for its consideration. In the matter of *Nancy Smith and Partners in Sexual Health (Non-Profit),*[77] the applicant was dismissed for breaching of confidentiality clauses contained in her contract of employment; the Respondent's code of conduct; insolent and insulting behaviour in emails; and bringing the Respondent's name into disrepute – due to internal company matters shared via email with external parties. It was found that the trust relationship between the parties had been broken. At Arbitration, the Applicant claimed that the emails had been accessed by the Respondent in breach of the right to privacy as contained in the Constitution, and the *Regulation of Interception and Provision of Communication-Related Information Act 70 of 2002.* The Commissioner found that the accessing of the employee's private email account by the employer was in breach of the Act, as the Respondent was not a party to the communications, and nor was it provided with consent to allow for such interception. In addition, the email account was a Gmail account, and thus accessible via the Internet Google domain, and not directly via

[76] Available at: http://www.proappoint.co.za/blog/2009/09 [Accessed: 19 January 2010].
[77] WECT13711-10 (CCMA).

the Respondent's servers. [78] Further, it was found that, just because the email account was left open, this does not mean the contents thereof are in the public domain, as, *'The contents of an email account cannot be compared to comments posted on an Internet blog to which access is not restricted..., or to comments posted on an Internet-based social networking site, such as Facebook, where privacy cannot be reasonably expected by any user as the site structure allows viewing...of "conversations" by persons not party to those communications.'*[79] As such, the evidence was unlawfully obtained and inadmissible in the light of the Applicant's constitutional right to privacy – barring one email which it was confirmed had been accidentally uncovered. On the basis of this email alone it was found that the dismissal was substantively unfair.

In terms of another matter specifically related to Facebook[80] the CCMA had to determine, where employees had made comments regarding the employer and management to each other on Facebook, whether such remarks were in the public domain. The Applicants were charged with bringing the company name, director, management and staff into serious disrepute in the public domain, and were dismissed. All remarks made were found to be accessible to anyone with Facebook access. The Applicants argued that the Respondent had invaded their privacy, and that the company had suffered no damage, as the relevant postings had referred to no-one by name. The Commissioner, however, found that, by neglecting to set access and privacy restrictions on their Facebook profiles, the postings were in the public domain, and the employees had thus abandoned their rights to privacy, and to the protection of RICA. In

---

[78] At 6-9.
[79] At 9.
[80] *Sedick & Another and Krisray* (Pty) Ltd (2011) 32 *ILJ* 752 (CCMA).

addition, the postings were intentionally communicated to subordinates and ex-employees of the Respondent who were, on a balance of probability, aware of about whom the derogatory comments had been made. As such, the Commissioner found that the postings had served to bring the Respondent into disrepute, and that the potential for damage to its reputation was real. As such, the dismissals were found to be substantively and procedurally fair.[81]

In a similar matter, but one where the dismissal was found to be procedurally and substantively unfair,[82] the Applicant made a statement on Facebook regarding his boss. This statement was seen by the daughter of the Respondent, as well as another manager – both of whom were 'friends' with the Applicant on Facebook. The Respondent argued that a dismissal had not occurred and, in addition, that it did not view dismissal as the appropriate sanction. The Commissioner stated that, although such a public insult to an employer may well be considered sufficient grounds for dismissal, his decision must be influenced by the Respondent's view of the seriousness of the misconduct.[83]

Duff[84] states that employees who vent frustration regarding the employer on a forum such as Facebook are opening themselves up to potential dismissal or civil action - as the employer is entitled to protect its company, and nothing can be more damaging to an employer's reputation than being defamed by its own workforce. However, the rights of the individual to free speech, as contained in the Constitution,

---

[81] *Sedick & Another and Krisray (Pty) Ltd* (2011) 32 *ILJ* 752 (CCMA).
[82] *Nathaniel Arelisky and Van Wyk Da Silva Trust t/a Ocean Basket Table View* WECT16930-10 (CCMA).
[83] At 5.
[84] Duff, A. *Can an employer dismiss due to Facebook?* (2010) *Packaging Review South Africa*, Vol. 36, Issue 2.

must be weighed against the employer's right not to be defamed. Based on recent decisions, it appears that an employee will not be able to rely on the defence of a blanket right to privacy.[85]

The employer's right to discipline its employees stems directly from the common law duties inherent in a contract of employment. The employee provides labour in return for remuneration – thereby occupying a subordinate role to the employer, and subjecting him or herself to the employer's control. However, the employer may only control an employee's actions in relation to the employment relationship.[86] Of course, when an employee's private actions impact on the employer, the latter party cannot be expected to continue an unhealthy relationship with an employee. As such, the courts have accepted that there may be a link between the employee's private activities and the relationship of employment. For example, in *Van Zyl v Duhva Opencast Services*,[87] it was found that the dismissal of an employee who assaulted his supervisor outside of working hours, and in front of another employee, was fair, and that the employee's actions made a continued working relationship intolerable. In such matters the employee's right to privacy may be trumped by the employer's right to fair labour practices, and not to have its good name besmirched. The same rationale could be applied to comments on publicly viewable forums such as Facebook – where such comments could be viewed by clients, competitors and colleagues.[88]

---

[85] At 13.
[86] Available at: http://www.proappoint.co.za/blog/2009/09 [Accessed: 19 January 2010].
[87] (Edms) Bpk (1988) 9 *ILJ* 905 (IC).
[88] Available at: http://www.proappoint.co.za/blog/2009/09 [Accessed: 19 January 2010].

However, in the case of non-work related conduct, it is for the employer to establish that it has a legitimate interest in the matter, which is sufficiently serious to justify disciplinary action against the employee.[89] In a number of other decided cases, off the job conduct was found to justify disciplinary action. In *NUM & others v East Rand Gold & Uranium Co Ltd*[90] an assault on a company bus after the completion of a shift was held to be a dismissible offence, and in *Mavumengwana v Samancor Ltd (Metalloys)*[91] there was an assault in an area of the company's premises that was accessible to the public. The court found this assault was work related. As such, it is feasible that similar logic might be applied to comments made on social networking sites outside of office hours, but which negatively impact the employer's business interests in some manner.

The offence of bringing the employer's name into disrepute is often considered separately by arbitrators and the courts, or may be considered an aggravating factor in internal disciplinary matters. For example, in the matter of *Timothy v Nampak Corrugated Containers (Pty) Ltd*,[92] wherein the Appellant misrepresented himself as an attorney acting on behalf of the Respondent, and other employees of the Respondent, in an attempt to obtain various privileged information. This resulted in the Appellant being dismissed for various charges, including bringing the Respondent into disrepute. The CCMA subsequently found the dismissal to be substantively unfair, and reinstated the Appellant to his original job. However, the Labour Court found that the decision of

---

[89] *Saaiman & another v de Beers Consolidated Mines (Finsch Mine)* (1995) 16 *ILJ* 1551 (IC) 1562H-I).

[90] (1986) 7 *ILJ* 739 (IC).
[91] (1992) 1 *LCD* 200 (IC).
[92] (201) DA 22/08 *ZALC* 56 (LAC).

the Commissioner was unreasonable; that not only did the conduct constitute a labour misconduct, but also a criminal offence, and that the Appellant had wilfully brought the name of the Respondent into disrepute – an offence in light of the Respondent's disciplinary code. Following on from this, the Labour Appeal Court considered that an objective test had to be applied, wherein all the circumstances of the matter, including the nature of the conduct and the seriousness thereof, amongst other things, should be considered in their totality. On this basis the judge in this matter concurred with the judge in the Labour Court matter. As such, the appeal was dismissed with costs.[93] On this basis, a matter relating specifically to allegedly bringing the employer's name into disrepute on a social networking site would also presumably have to be considered on the basis of the totality of facts at hand, and a decision made on that basis.

Employees are duty-bound to uphold their employer's reputation, and conduct bringing such a reputation into disrepute may justify disciplinary action. The same applies to other employees, and clients, of the employer.[94] An example of this was the matter of *Bamford & others v Energiser SA Ltd*[95] where the employees concerned stored and transmitted numerous offensive emails and, subsequent to disciplinary action being taken, appeared on radio and television and misrepresented the nature of their actions and the offensive material concerned. Should employees legitimately wish to reveal information which may damage the employer's reputation they may do so by way of the *Protected Disclosures Act, 2000*; although such disclosures are subject to certain limitations.

---

[93] *Timothy v Nampak Corrugated Containers (Pty) Ltd* (DA22/08) [2010] ZALC 56; Available at: http://www.saflii.org/za/cases/ZALC/2010/56.html [Accessed: 28 January 2011].
[94] Grogan, J. *Dismissal, Discrimination & Unfair Labour Practices* (2007) JUTA & Co Ltd.
[95] [2001] 12 *BALR* 1251.

The same argument could hold true for disclosures made via social networking media.

In the *Bamford* matter the Applicants alleged that there was not a clear workplace rule governing such computer usage, and that their right to privacy had been infringed. However, in terms of the latter argument, the Arbitrator found that the material in question was not personal in nature, but could rather be referred to as 'non-business' related. As such, the personal dignity of the employees had not been harmed. In addition, that just because there is no formal policy in place, this does not mean the employer cannot take fair and valid disciplinary action. It would seem an employer is simply required to show that it informed all users of the broad parameters governing email usage in the workplace. Mischke[96] states that, although a policy governing usage is prudent, the simple reminder to employees via email on a regular basis of the rules regarding email and Internet usage may suffice. In addition, where a policy is in place, a reminder of the contents thereof on a regular basis is also encouraged.

In a matter not concerning social networking media specifically, but stemming from comments made by a University of Kwa Zulu Natal (UKZN) employee to the more general media in 2007 – Fazel Khan was dismissed for bringing the university's name into disrepute. The disciplinary process took seven months to achieve completion, during which time Mr Khan argued his right to freedom of expression.[97] Mr Khan subsequently referred this matter to the CCMA, on the basis of the

---

[96] Mischke, C. *Dismissal for abuse of email: Arbitration award sets decisive tone on employer rights over use of email facilities* (2002) January 11(6) *CLL* 51.

[97] Available at: http://abahlali.org/node/1117 [Accessed: 19 January 2010].

substantive unfairness of the dismissal. However, the Commissioner found that Mr Khan had breached the university's policy in terms of non-disclosure of confidential information. As such, the dismissal was upheld.[98]

Further, in the matter of *Ngutshane v Ariviakom (Pty) Ltd*[99] the Applicant was dismissed following the publication of an IT Web article - which the Respondent stated had irreparably damaged the employment relationship - and for placing herself in conflict with the interests of the organisation. The Applicant was invited to make representations in order to avoid her dismissal but declined to do so. The Labour Court was required to determine the procedural fairness of the dismissal. It found that it did not have jurisdiction to review the decision of the Respondent, but considered the matter on its merits anyway, and found that – even if it had jurisdiction – the procedure followed by the Respondent was deemed a fair one. The application was accordingly dismissed with costs.

Despite this, it is Rycroft's[100] argument that bringing the employer into disrepute is both difficult to prove, and usually too vague to be reasonable. In addition, the employment relationship can no longer be considered the master-servant relationship of the Victorian age. Rather, today employees have rights, for example, to freedom of expression; to whistle-blowing under the ambit of the *Protected Disclosures Act 26 of 2000* – whereby employees may report employers who are guilty of corruption; and, further, to report violations of labour legislation –

---

[98] *Khan v University of KwaZulu Natal* (2009) 18 CCMA 8.7.1.
[99] *T/a Arivia.Kom* (J1067/08) [2008] *ZALC* 159.
[100] Rycroft, A. *Bringing the Employer into Disrepute* (2008) 29 *ILJ* 1605.

including criminalising victimisation by employers for such disclosures. In terms of the final example, reporting the employer would certainly bring the employer into disrepute, but the employee is protected from retaliation. On this basis, an employer alleging it had been brought into disrepute by an employee would have to clearly lead evidence to show this – very difficult, as few employers will be able to show evidence of how the public views them, and a subsequent change in attitude, or similar. It is suggested that a better approach would to frame a charge that accurately reflects the alleged misconduct, rather than relying on the vague wording of 'bringing the employer into disrepute'.[101]

In 2005,[102] an employee of Royal Ascot Super Spar was dismissed following an article he wrote in the newspaper of the Democratic Socialist Movement (DSM) about the poor working conditions of his employer. Upon referring the matter to the CCMA, the employee was subsequently reinstated with back pay. The employee was supported by the Freedom of Expression Institution (FXI), who touted the constitutional right of employees to freedom of expression, even if this includes expression which is critical of the employer.[103] In an earlier letter to the employer, the FXI berated the employer for allegedly victimising the employee for, *'...exercising his constitutional right to freedom of expression.'* It went on to say that, *'...workers have an inalienable right to raise public debate regarding their working conditions, and should be able to do so freely. This is especially so in the current climate of such high unemployment and inequality in South Africa, where*

[101] Rycroft, A. *Bringing the Employer into Disrepute* (2008) 29 *ILJ* 1605.
[102] *COSAWU obo Khumalo v Royal Ascot Superspar* (2006) 27 *ILJ* 2452 (CCMA).
[103] Available at: http://www.fxi.org.za/content/view/61/51/ [Accessed: 22 January 2011].

the conditions of workers are so fragile relative to the conditions of the corporate sector.'[104]

In the subsequent CCMA matter, the Commissioner found that the allegations made by the dismissed employee in his article, including the allegation that employees were underpaid, was true. As such, the article was not derogatory or defamatory – for which the employee was charged and dismissed. Further, that the employer's view - that the workplace was not the appropriate forum for the expression of the employee's opinions - was flawed; that the employer had acted in bad faith, and ignored human rights abuses of its employees; the employer should have joined the public debate initiated by the article; and that, *'...the right to freedom of expression is a sacred tenet of our Constitution and this right naturally extends to the workplace.'*[105]

It would seem feasible that the same constitutional rights to freedom of expression could be extended to the sphere of social networking – except perhaps where it was the employer's email or Internet system which was used to disseminate such opinions (if an electronic usage policy, or similar, was in place), or where such opinions were in fact not factual. As such, we turn to the issue of such usage, and how this interacts with an individual's right to privacy.

---

[104] Available at: http://www.fxi.org.za/content/view/71/51/ [Accessed: 22 January 2011].

[105] *Cosawu obo Khumalo and Royal Ascot Superspar* (2006) 27 *ILJ* 2452 (CCMA); Available at: http://www.fxi.org.za/content/view/61/51/ [Accessed: 22 January 2011].

Everyone has the right to privacy under the South African Constitution. However, McGregor[106] states that this is not an absolute right, and must be balanced with other rights – such as the employer's business necessity or operational requirements. But it would not make sense to state that employees lose their right to privacy upon entering the workplace. This right extends only to aspects of an individual's life or conduct to which a legitimate expectation of privacy can be had.[107] Collier states that, as a person moves into communal relations and activities in the workplace, so an individual's expectation of privacy diminishes – although some expectation will always remain.[108]

A recent matter in the CCMA dealt with this topic.[109] The Applicant was dismissed for sending various private emails via the Respondent's email system – including emails which referred to a fellow employee. The Applicant alleged that the Respondent had contravened her right to privacy by accessing these emails, and argued that the emails concerned were thus inadmissible. The Respondent argued that, in terms of section 6(1) of RICA an employer, in the course of carrying on its business, could intercept indirect communications relating to the business, on certain conditions. In addition, the emails were business-related, and had been sent using the Respondent's computer. The Applicant had also signed the Respondent's electronic communications usage policy, thus authorising the Respondent to monitor her electronic communications. The CCMA found in favour of the Respondent – that the accessed emails were admissible as evidence in light of RICA, and their business-relatedness.

---

[106] McGregor, M. *The Right to Privacy in the Workplace: General Case Law and Guidelines for Using the Internet and e-Mail* (2004) *SA Mercantile Law Journal = SA Tydskrif vir Handelsreg* Vol 16(4) at 638-650.
[107] At 639.
[108] Collier, D. *Workplace Privacy in the Cyber Age* (2002) 23 *ILJ* 1743.
[109] *Sharwood v Africa Business News Limited t/a CNBC Africa*. 2010 (CCMA).

Similarly, in the matter of *Van Wyk v Independent Newspapers Gauteng (Pty) Ltd & Others*[110] the Applicant was dismissed by the employer for sending emails of an allegedly malicious nature to colleagues, with the apparent intention of undermining management authority; and for making statements of an allegedly derogatory nature in another email to a colleague and friend. The CCMA found her dismissal both procedurally and substantively fair. However, on review, the Applicant argued that, in light of the *Monitoring Prohibition Act, No 127 of 1992*, the email to the friend could not be regarded by the CCMA or the court. The Respondent argued that the email had been sent using a company computer, and to another company computer; that the content of the email concerned work-related matters; and that the company's Information Technology Usage Policy declared all information stored on its system belonged to the company. The judge in the Labour Court matter found that the Applicant could not rely on the *Monitoring Prohibition Act.* It was found that the dismissal was warranted under the circumstances, and that the arbitrator in the CCMA matter reached a rational conclusion based on the facts of the matter. The application was accordingly dismissed with costs.

On this basis, where comments were made via social networking media, it would feasibly be important to consider whether such comments were made utilising workplace computer equipment; who had sight of the comments made – for example, was this a private or public forum; and how the employer obtained access to the relevant comments – notwithstanding the nature of the comments, and their impact on the employer. In terms of an individual's right to privacy of their communications, in his article, *'Monitoring, interception and Big Boss in*

[110] (2005) 26 *ILJ* 2433 (LC).

the workplace: is the devil in the details?'[111] Pistorius states that an employee's right to privacy must be balanced with the employer's right to protect its operational requirements and business interests.

In terms of the employer's right to intercept and view electronic communications, Modiba[112] states that, while employers do not have an automatic right, they can adopt a clearly worded email and Internet use policy which will then entitled them to do so. This will protect them from liability, and will allow them to control email and Internet use. This policy should be communicated to employees, including regular reminders, and employees should be educated on the potential recourse contravention could incite. [113]

Finally, with regards to the matter of vicarious liability and employers, and whether they may be held liable for acts committed by employees on social networking media specifically, this question has yet to be answered by South African courts. However, in principle, the law recognises that employers may create a risk to third parties through wrongful acts committed by their employees during the course of fulfilling their employment duties. In such instances, employers may be liable to parties who suffer harm from such acts. However, the result will depend on all the facts and circumstances of the matter at hand, including an examination of:

- The nature and content of the offensive material;

---

[111] [2009] PER 1. Available at: www.saflii.org/za/journals/PER/2009/1.html [Accessed: 6 January 2011].
[112] Modiba, M. *Intercepting and Monitoring Employees' e-Mail Communications and Internet Access* (2003) *SA Mercantile Law Journal = SA Tydskrif vir Handelsreg* Vol. 15(3) at 363-371.
[113] At 370-371.

- Whether the act was committed in the pursuance of the employer's business interests, or whether the employee could be considered to have engaged in a 'frolic of his own';
- The employee's position, title and scope of responsibilities; and
- The nature of the employer (for example, whether a private or public concern, partnership, or closed corporation).[114]

Collier[115] states that, as a general rule, an employer is vicariously liable in civil law for any wrongful act committed by an employee during the general scope of employment. In addition, an employer may be vicariously liable where there has been passive approval of the activities an employee is, or has been, engaged in. For example, an employer is responsible for ensuring defamatory behaviour, whether via Internet or email related activities, or otherwise, do not take place in the workplace.

However, in conclusion, South African case law specifically related to comments on social networking media which impact the employer has yet to be fully explored and developed. Despite this, international progress in this regard may provide clues of how such matters may in future be decided. As such, we turn to the international context.

---

[114] Available at: http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter7.htm [Accessed: 7 February 2011].

[115] Collier, D. *Workplace Privacy in the Cyber Age* (2002) 23 *ILJ* 1743.

3.2 United States of America

In a study conducted in the United States of America in 2009 on more than 200 companies, it was found that 8% of those surveyed reported terminating an employee's services for Facebook usage during company time. This was double the 4% dismissal rate experienced the year prior.[116] This suggests a rapid increase in usage of Facebook alone in the workplace.

In the USA, various issues regarding social networking sites and privacy – particularly with regards to patients in healthcare institutions – have over the last few years come to light. In one matter, a group of hospital workers took photographs of an injured and dying man and uploaded these to Facebook. Four of these employees were dismissed, and another three disciplined – in what was clearly a matter which would have feasibly brought the employer's name into disrepute. However, it has been stated that privacy breaches and other similar workplace matters could be more effectively prevented if employers took more proactive steps to educate employees about social media expectations.[117]

In a recent article, medical students were found to have discussed confidential patient information in online forums, prompting various disciplinary actions.[118] In subsequent studies it was found that medical students may use social networking as a means of relieving stress, leading to unintended breaches of patient confidentiality. However, it

[116] Available at: http://www.labournet.co.za/NewsItem.aspx?ID=339f3e63-f912-4fd6-8d76-440006ffb589 [Accessed: 14 December 2010].
[117] Available at: http://www.socialnetworkinglawblog.com/ [Accessed: 18 November 2010].
[118] Available at: http://msnbc.msn.com/id/32972597 [Accessed: 18 January 2010].

was found that, *'Organisations should emphasise culture, values, and ethics in order to mitigate reputational risk in these online communities.'*[119]

Despite this, in the USA, a case attracting significant media attention recently saw the National Labour Relations Board alleging that an Emergency Medical Technician was illegally dismissed in 2009 by her employer in Connecticut for criticising her supervisor on Facebook. It was expected that the outcome of this matter – which was scheduled to be heard in January 2011 – could set a precedent for employers to adhere to in such matters. The view of the Board's acting council was that such comments are akin to *'talking at the water cooler'*, and that, *'...employees have protection under the law to talk to each other about conditions at work.'*[120] The employer claimed that the employee was dismissed for violating its policy against the depiction of the employer on a social networking site. However, the Board stated that the employer's blogging and Internet posting policy was overly broad, and that the dismissal was in violation of the employee's right to engage in *'concerted activities'*. It stated that the U.S. *National Labour Relations Act* protects an employee's right to discuss work-related matters in order to improve workplace conditions.[121] This matter was subsequently postponed to February 2011. However, on the eve of the hearing, it was announced that this matter had been settled out of court. In the settlement, the employer agreed to revise its *'overly broad'* rules to ensure these do not restrict employees from legitimately discussing working conditions with colleagues and others while not at work. It further agreed not to

---

[119] Available at: http://www.geisinger.org/professionals/services/bioethics/b_notes/nov2009.pdf [Accessed: 21 December 2010].
[120] Available at: www.cleveland.com/nation/index.ssf/2010/11/feds_rule_against_employer_in.html [Accessed: 18 November 2010].
[121] Available at: http://epic.org/privacy/workplace/default.html [Accessed: 9 February 2011].

discipline or dismiss employees for engaging in such discussions. A separate and private settlement was concluded with the employee concerned. As such, it would seem that the expected setting of a precedent with regards to matters such as this on social networks will have to wait.[122]

In addition to the medical community, a spate of disciplinary actions against students resulting from activity on social networking sites has encouraged heated debate over the ethics of school and university administrators accessing such information, and taking action on this basis. In October 2005, a student of Fisher College in Boston was expelled for statements made on Facebook regarding a campus security officer – including the statement that the officer enjoyed antagonising students, *'...and needs to be eliminated.'* Such comments were viewed to be in violation of the institution's code of conduct.[123]

Further to this, in November 2005 four students at Northern Kentucky University were fined for uploading photos of a drinking party to Facebook. These pictures showed that the students were in contravention of the university's no-alcohol policy. And, in the same month, an Emory University drinking club was investigated for similar violations by university officials.[124]

---

[122] Available at: http://www.facebook.com/notes/labor-relations-today/nlrb-parties-settle-facebook-firing-case [Accessed: 10 February 2011].
[123] Available at: http://en.wikipedia.org/wiki/Use_of_social_network_websites_in_investigations [Accessed: 11 January 2011].
[124] Available at: http://en.wikipedia.org/wiki/Use_of_social_network_websites_in_investigations [Accessed: 11 January 2011].

In a key U.S. matter separate to Facebook - concerning MySpace usage in 2006 - a federal jury found that restaurant managers who had secretly monitored employee postings on the site had violated state and federal privacy laws, specifically protecting the privacy of web communications.[125] In the matter of *Pietrylo v. Hillstone Restaurant Group*[126] two waitrons were dismissed for acting, *'...contrary to the core values of the business, such as the need to exhibit professionalism and a positive attitude...'* after criticising their managers in their MySpace postings. It was found that the restaurant had maliciously violated the *Federal Stored Communications Act*, and the *New Jersey Wiretapping and Electronic Surveillance Control Act.* The MySpace group – which was started by Pietrylo, only accessible by invite, and password protected – was accessed by restaurant managers after they obtained the password from another employee. The two waitrons were awarded back pay and punitive damages to the total amount of $17 000.[127] It is questionable whether the same outcome would have resulted had the comments been freely and publicly accessible – thus more feasibly arguable as bringing the company into disrepute.

Similarly, in May 2010 a waitress was dismissed after complaining on Facebook regarding a customer's poor tipping, and mentioning her employer by name. The reason for dismissal was cited as being for violating company policy for disparaging customers, and portraying the employer in a negative light via social media sites. The employer then posted its own response on Facebook – resulting in vigorous public

---

[125] Available at: http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202431575049 [Accessed: 18 January 2010].

[126] 2:06-cv-5754. Available at: http://www.employerlawreport.com/uploads/file/PIETRYLO%20v%20%2HILLSIDE%20RESTAURANT.pdf [Accessed: 18 January 2010].

[127] Available at: http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202431575049 [Accessed: 18 January 2010].

backlash triggered by the discipline resulting from the employee's online activity. As such, employers may be able to legally justify similar terminations; however, as was evidenced in this matter, this may not prevent poor public relations.[128]

In 2001 four employees of the C.I.A were dismissed for private and unauthorised chat utilising the agency's computer network – what the agency termed, *'...wilful misuse of the agency's computer networks...'* – which sanction the dismissed employees felt was too harsh. However, they subsequently lost their internal dismissal appeals. The agency stated that it took serious action on the basis that employees had attempted to keep the chat network secret for a number of years – effectively since 1987.Various other employees received lesser disciplinary sanctions. The four employees considered the chat network harmless, and stated that it was established prior to agency regulations forbidding such forums came into effect.[129]

In another interesting matter – not centred around the use of social networking media, but dealing with privacy of communications all the same – in June 2010 the United States Supreme Court ruled that a public employer's search on a policeman's employer-issued pager, resulting in the finding of sexually explicit text messages, did not amount to an illegal invasion of privacy. It found that city employees had no expectation of privacy in communications made using employer-issued devices, and stated, *'...rapid changes in the dynamics of communication and information transmission are evident not just in the*

[128] Available at: http://www.socialnetworkinglawblog.com/ [Accessed: 18 November 2010].
[129] Available at: http://www.nytimes.com/2001/05/18/us/dismissed-for-chat-room-cia-workers-speak-out.html?pagewanted=1 [Accessed: 18 January 2010].

technology itself but in what society accepts as proper behaviour ... at present it is unclear how workplace norms, and the law's treatment of them, will evolve.'[130]

It would appear that workplace privacy in the US derives limited protection, despite the right conferred by the Fourth Amendment. The test would appear to be a legitimate expectation of privacy, as was found in the above matter. In the matter of *Smythe v Pillsbury Co*[131] an employee sued for an invasion of privacy, after being dismissed on the basis of sending inappropriate email messages – despite the employer previously having stated that email messages were confidential. The court found that all computer equipment was owned by the company and, therefore, the employee had no legitimate expectation of privacy. Further, that the employer's interest in preventing the misuse of its computer equipment outweighed the employee's expectation of privacy.[132]

What about where comments have been made on social networking media outside of working hours? A clue may be found in the 2003 USA matter of *Pay v Lancashire Probation Services*, where a probation officer employed to deal with sex offenders was dismissed after it was found that he was selling sex paraphernalia via a website outside of working hours. In this matter the court took the common-sense approach, taking the view that the dismissal was fair, as the plaintiff's extra-curricular activities directly impacted on his job and the employer. However, in another matter where an employee kept an online diary referencing

---

[130] Available at: http://www.socialnetworkinglawblog.com/ [Accessed: 18 November 2010].
[131] 914 F Supp 97 (ED) Pa 1996.
[132] Collier, D. *Workplace Privacy in the Cyber Age* (2002) 23 *ILJ* 1743.

workplace anecdotes, she was found not guilty of damaging the employer's reputation, as the diary did not sufficiently reference the employer.[133]

In terms of freedom of speech and social networking in the USA, free speech is protected by the First Amendment. However, this protection does not extend to slander or defamation. This limitation was explored in the matter of *Hustler Magazine v. Falwell* in 1988, where the line between the two was examined, including at what point the line between free speech and defamation was deemed to have been crossed. In this matter the Supreme Court found that the statements made by the magazine were not defamatory as they were too extreme to be believable, and made about public figures, who are subject to social commentary. As such, the comments made were deemed to be protected speech.[134] However, where a false statement made about someone else is likely to be believed, the same does not hold true. An example of this concerned a matter where pupils of a high school in San Antonio, Texas created a fake profile for the school's assistant principle on MySpace, containing false information regarding her sexual orientation and practices, along with other derogatory statements. The matter resulted in disciplinary action by the school, as well as litigation for alleged defamation and libel.[135]

---

[133] *Protecting your company's reputation* Available at: http://www.personneltoday.com/articles/2008/06/20/46378/protecting-your-companys-reputation.html [Accessed: 19 January 2010].

[134] Available at: http://articles.sitepoint.com/article/fake-social-networking-profiles [Accessed: 22 January 2011].

[135] Available at: http://articles.sitepoint.com/article/fake-social-networking-profiles [Accessed: 22 January 2011].

In terms of the First Amendment, other than the freedoms contained therein – specifically referring hereto, freedom of speech - not being absolute, the communication methods used may also be a factor. In the matter of *Reno v. ACLU* of 1997 it was noted by the court that the Internet is less invasive than certain other broadcast media, such as television or radio, because data is usually not encountered by accident.[136] Thus, the means by which an employer obtained access to comments on social networks could also legitimately play a role in deciding such a matter.

Finally, in terms of vicarious liability, Chevron USA Inc. were required to pay $2.2 million to settle a sexual harassment claim made by several employees, wherein it was alleged that the employer's email system had been used to transmit sexually offensive material.[137] It is feasible that the same liability would apply to claims made by third parties for material distributed by employees on the Internet and social networking sites that could be tied back to the employer.

3.3 United Kingdom

The United Kingdom has seen its fair share of matters emerging in the media in the past number of years for actions taken on social networking sites. In 2005, in a well publicised matter, an Edinburgh man lost his job after posting comments about his employer online in a blog forum. He was employed by the company for eleven years prior to

---

[136] *Freedom of Speech & Technology – the Reno, Multnomah & Baker case* Available at: http://cs.ua.edu/340/fall10/freespeech_pta.ppt [Accessed: 22 January 2011].
[137] Collier, D. *Workplace Privacy in the Cyber Age* (2002) 23 *ILJ* 1743 at 1744.

being dismissed for gross misconduct and bringing the company name into disrepute for making comments on his blog referring to his manager as *'Evil Boss'*, and to the company – Waterstone's book chain – as *'Bastardstone's'*. The dismissed employee subsequently claimed that his dismissal had breached his right to freedom of speech.[138]

In another matter in 2007 – similar to a number of the matters referred to in the United States - it was reported that Oxford University employees were logging onto social media sites – in particular Facebook – and using evidence such as photos found on student profiles to discipline them for breach of the University's code of conduct. The result was that some students' graduations were delayed pending the outcome of disciplinary hearings. The University Student Union responded to this by advising students to limit their Facebook privacy settings to 'friends only', and stated that the University had contravened students' rights to privacy, and had contravened, *'...the ethos of the site as a community for connecting friends.'*[139]

More recently, in 2010, it was reported that over seventy employees of Britain's two major law enforcement agencies had been disciplined for misuse of the Internet and, more specifically, social networking sites. This despite bans on social networking usage by both the Ministry of Justice and the Metropolitan Police Service (Met), except where employees could strongly show why access should be granted in pursuance of their official duties. Further, Scotland Yard has a guide advising officers how to conduct themselves on such sites; not to

[138] Available at: http://news.bbc.co.uk/2/hi/uk_news/scotland/4167629.stm [Accessed: 19 January 2010].
[139] Available at: http://www.guardian.co.uk/media/2007/jul/17/digitalmedia.highereducation [Accessed: 21 December 2010].

disclose their official status; or to bring themselves or the service into disrepute – including during off-duty time. The Met similarly reported that all employees were regularly reminded of the need to comply with their MPS Information Code of Conduct.[140]

In a further 2010 matter, a Bishop of the Church of England was indefinitely suspended after he made disparaging comments on Facebook regarding the then upcoming royal wedding. He predicted that the marriage would last seven years, and further described the event as being surrounded by *'nauseating tosh'*. The matter resulted in significant embarrassment to the Church, forcing the clergyman to apologise for his remarks. However, this failed to prevent his suspension.[141]

A recent matter in the United Kingdom of particular interest and importance[142] concerned two former friends – Mathew Firsht, the complainant, and the defendant, Grant Raphael (who had previously worked for the complainant). It was found that a Facebook profile in the name of the complainant was created in 2007, following which a Facebook group – entitled, *'Has Matthew Firsht lied to you?'* - was linked to the profile via hyperlink. The profile contained various personal details, including those related to the complainant's sexual orientation; and the linked group contained defamatory statements regarding the complainant and his business. The defendant claimed that he had not created the profile and group, despite this being traced back to his personal computer. However, the judge found against the defendant –

---

[140] Available at: http://www.computing.co.uk/ctg/news/1849095/police-moj-staff-disciplined-social-networking-abuse [Accessed: 13 January 2010].
[141] Available at: http://www.guardian.co.uk/world/2010/nov/23/ [Accessed: 7 February 2011].
[142] *Applause Store Productions Ltd. & Anor v Raphael* [2008] *EWHC* 1781 (QB) (24 July 2008).

finding that he had created the profile, thereby misusing private information, and that the material utilised amounted to defamation and libel. The court awarded damages in favour of the complainant.[143] This was not a workplace matter *per se*, however, had the defendant still worked for the complainant at the time that this matter came to light; it is feasible that he may have been found guilty of workplace misconduct, and particularly for bringing the company name into disrepute.

The issue of vicarious liability of employers in relation to the actions of their employees on social networks has also been a matter of debate in the United Kingdom. The courts have shown that they are prepared to apply the definition of vicarious liability widely, and employees who harass colleagues online; engage in 'cyber bullying'; or who defame a third party may render their employers liable for such activity.[144] For example, in a 1999 matter, a Norwich Union employee circulated a series of emails claiming one of the employer's competitors was being investigated by the Department of Trade and Industry. The competitor (Western Provident) became aware of the emails and instituted legal action, resulting in Norwich Union being required to pay compensation to the impacted competitor.[145]

Finally, in a recently reported matter, a student sued a former friend for damages and won, after the friend posted a paedophilic picture on his Facebook profile with the caption, *'Ray, you like kids and you are gay so bet you love this picture, Ha Ha'*. The complainant stated that more than 800 people had access to his profile. He duly sued his former friend for

---

[143] Available at: http://www.bailii.org/ew/cases/EWHC/QB/2008/1781.html [Accessed: 22 January 2011].
[144] Available at: http://www.walkermorris.co.uk/content.aspx?id=619 [Accessed: 9 February 2011].
[145] Collier, D. *Workplace Privacy in the Cyber Age* (2002) 23 *ILJ* 1744.

libel, the outcome of which was an award for damages, a conviction for circulating indecent images of children, and community service. Had this scenario occurred in the workplace the employer could be open to litigation, and feasibly held vicariously liable for the actions of the employee.[146]

3.4 Australia & New Zealand

In an April 2009 article in Australia, a veteran attorney cited that disciplining or dismissing employees for comments made on social networking sites such as Facebook and Twitter could be deemed illegal. He stated that contracts of employment are usually unlikely to cover usage of social networking sites, and that existing policies can often not be stretched to cover such usage. He stated, *'If an employer hasn't told people in advance what the rules are, what the conditions are, then that greatly increases the likelihood that an employee can say well, I can't be terminated for this because I wasn't aware that this is something I was not to do.'*[147] The attorney in question contrasted this with clear policies regarding workplace Internet and email usage, which most companies made new recruits aware of upon appointment. In addition, he stated that most companies have rules against speaking to the media, but that posting comments and opinions on social networking sites was different to this, and needed to be addressed on its own merit. [148]

---

[146] Available at: http://www.gadllp.co.uk/blog/?tag=vicarious-liability [Accessed: 9 February 2011].
[147] Available at: http://www.smh.com.au/articles/2009/04/03/1238261779328.html [Accessed: 18 January 2010].
[148] Available at: http://www.smh.com.au/articles/2009/04/03/1238261779328.html [Accessed: 18 January 2010].

In terms of the use of social networking sites outside of working hours, Fair Work Australia recently considered when such activity might justify workplace disciplinary action, particularly with reference to the matter of *Fitzgerald v Dianna Smith t/a Escape Hair Design.*[149] In this matter the employee was dismissed following the posting of allegedly negative comments about the employer on her Facebook status. The dismissal was found to be unfair, and the employee was awarded compensation, although she was not reinstated to her original job. However, the tribunal warned employees not to post negative statements about employers, as this is different to talking to others in person. Once comments are made on social networking sites they are in the public domain, and accessible by multiple parties – therefore, making the matter no longer a private one. As such, such negative comments might be deemed fair reason for dismissal if they are found to have caused serious damage to the relationship of employment, or to the employer's reputation.[150] This was, however, not found to be the case in this particular matter, as the employer was not identified in the Facebook posting.[151]

In commentary on this matter, the case of *Rose v Telstra* was cited, wherein the principle was deemed to have been established that employee's may be dismissed for out of working hours conduct, where such conduct is likely to damage the employment relationship, or the

---

[149] [2010] *FWA* 7358.
[150] Available at: http://www.blakedawson.com/Templates/Publications/x_publication_detail_content_page.aspx?id=60287page=1 [Accessed: 22 January 2011].
[151] Available at: http://blakedaweson.com/Templates/Publications/x_publication_content_page.aspx?id=60241 [Accessed: 22 January 2011].

interests of the employer.[152] The same would hold true for comments made on social networking media outside of the workplace.

In terms of privacy, the office of the Federal Privacy Commissioner in Australia issued best practice guidelines governing workplace email, web browsing and privacy in order to encourage compliance with the *Privacy Act 1988*. These guidelines outline that, although employees may have a general expectation of privacy in the workplace, there is no constitutional or common law right to privacy. Some expectation of privacy is, however, provided for in terms of emails concerning personal information. Also that, if employees are not made aware by employers in advance of the potential monitoring of their network activities, this could be considered unfair.[153]

In a matter in New Zealand specifically, a warehouse worker was dismissed for serious misconduct, and bringing the company into disrepute, after posting comments about her workplace on the social networking site, Bebo. The worker posted comments such as, *'...work sux...'*, and that working nightshifts was, *'...gay like the management.'*[154] In response to this, an employment lawyer wrote that employees are free to express opinions with regards to their workplaces as long as such comments did not seriously harm the employer's reputation. He referred to employees' rights to freedom of expression as contained in the *New Zealand Bill of Rights*, and stated that such freedom had been recognised in earlier rulings. However – like with defamation and libel

[152] Available at: http://blakedaweson.com/Templates/Publications/x_publication_content_page.aspx?id=60241 [Accessed: 22 January 2011].
[153] Collier, D. *Workplace Privacy in the Cyber Age* (2002) 23 *ILJ* 1743.
[154] Available at: http://www.nzherald.co.nz/email/news/article.cfm?c_id=188&objectid=10483277 [Accessed: 18 January 2010].

law – there are limitations on this right.[155] Comments which are likely to negatively affect the employer's reputation, or which may damage the employment relationship, could feasibly warrant disciplinary action, including the possibility of dismissal.[156]

3.5 Canada

Turning to Canada, in a recent matter an employee posted comments on her Internet-based blog referring to her colleagues and management as *'imbeciles'*, *'idiot savants'*, and the *'lunatic-in-charge'*. After her dismissal the matter was referred to the Canadian Arbitration Board, which found that, although the employee had the right to create personal blogs and hold opinions regarding her co-workers, publicly displaying such opinions could hold consequences for her employer and the employment relationship. It was therefore found that she was justifiably dismissed.[157]

Further, in 2009, forty-nine Canadian government employees were disciplined for the sending of inappropriate email content via their work email. Ten of these employees were dismissed. However, it was found in this matter that the public interest was not deemed compromised, or impacted, and that the matter remained an internal one.[158] Similarly, in

---

[155] Available at: http://www.nzherald.co.nz/email/news/article.cfm?c_id=188&objectid=10483277 [Accessed: 18 January 2010].
[156] Available at: http://www.nzlawyermagazine.co.za/Archives/Issue104/N3/tabid/1543/Default.aspx [Accessed: 21 December 2010].
[157] Available at: http://www.nzlawyermagazine.co.za/Archives/Issue104/N3/tabid/1543/Default.aspx [Accessed: 21 December 2010].
[158] Available at: http://www.canada.com/vancouversun/news/westcoastnews/story.html?id=fdbe705b-012 [Accessed: 24 January 2011].

2004 approximately 130 employees at an Aerospace company were deemed to have been investigated for inappropriate use of the company's email and Internet facilities. A specialist in E-Commerce law commented on this matter, stating that employer's were required to analyse employees' reasonable rights to privacy to strike a balance with the employer's legitimate workplace concerns, such as:

- Confidentiality and trade secret concerns;
- Workplace liability;
- Network performance;
- Employee productivity;
- Computer crime.[159]

It is feasible that the same would apply when investigating activity on social networking media.

The important decision in the matter of *Murphy v. Perger* saw the Ontario Superior Court finding that a person with 366 'friends' on Facebook had no reasonable expectation of privacy. Further, in the matter of *Naylor Publications Co. (Canada) v. Media Union of Manitoba, Local 191* the Arbitrator similarly found that the reality of email and Internet is that privacy may never be entirely guaranteed.[160] As such, depending on the circumstances involved, an employee may find it difficult to argue the right to privacy regarding comments made on social networking sites which can be shown to impact on the employer's business interests in some way.

---

[159] Available at: http://www.hrmguide.net/canada/law/inappropriate-use.htm [Accessed: 24 January 2011].

[160] T.S. Zurbrigg *Facebook: What Employers Need To Know About Workplace Privacy, Discipline & Dismissal* Available at: http://www.fieldlaw.com [Accessed: 24 January 2011].

Privacy was also the central theme in the matter of *Lougheed Imports Ltd (West Coast Mazda) v. United Food and Commercial Workers International Union, Local 1518* before the British Columbia Labour Relations Board. In this matter it was again found that, after an employee posted comments on Facebook regarding his employer and supervisor – who was a 'friend' on Facebook – employees have no reasonable right to privacy regarding statements made on social networking sites. In addition, where such statements are offensive to management or damaging to the employer's business, the employer may have reasonable cause for dismissal.[161]

In terms of discipline in the workplace, the matter of *Chatham-Kent (Municipality) v. National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW Canada), Local 127 (Clarke Grievance)*[162] saw the termination of an employee for insubordination and breach of confidentiality being upheld, after the employee posted comments on her blog which were deemed to undermine the authority and reputation of management. Similarly, in *Government of Alberta and Alberta Union of Provincial Employees (R. Grievance),*[163] an employee was dismissed for comments regarding management and co-workers on a blog. Of interest in this matter was that the blog was not work-related. However, the Arbitrator found that, despite the right to blog and hold opinions, the comments made undermined the employment relationship.[164]

---

[161] S.D. Todd *Facebook comments: just cause for termination?* Available at: http://www.heenen.co/fr/nouvelles/pdf/Facebook_comments_just_cause_for_termination.pdf [Accessed: 24 January 2011].

[162] [2007] O.L.A.A. No. 135, March 26, 2007.

[163] [2008] A.G.A.A. No. 20, April 11, 2008.

[164] T.S. Zurbrigg *Facebook: What Employers Need To Know About Workplace Privacy, Discipline & Dismissal* Available at: http://www.fieldlaw.com [Accessed: 24 January 2011].

Although these particular matters concern blogging and not social networks *per se*, the same principles can be considered to apply to other online activity, including comments made on social networks – which may be just as transparent and accessible as blogs.[165]

A fairly unique matter in 2009 saw an IBM employee in Quebec, who was medically booked off work for suffering from depression, subsequently realise that her sick benefits had been discontinued. Upon questioning this, her medical aid advised that they had seen photos on her Facebook profile of her at a party, and while on holiday, during the time that she was booked off for depression. They stated that, in the photos, she looked *'happy'*. [166] The medical aid confirmed that they regularly scouted social networking sites looking for those allegedly abusing medical benefits. This matter was referred to the Quebec Superior Court for review.[167] However, the plaintiff's first attempt to recoup the loss of her medical benefits failed.[168] It is feasible that an employer could access employees' social networking activity in order to take workplace disciplinary action for abuse of sick leave, and similar entitlements, however, proving such abuses on a balance of probability would be required based on the facts at hand.

In this light, the Office of the Privacy Commissioner of Canada recently warned employees, and prospective employees, that many employers and recruitment agencies were using personal social networking sites and blogs to learn more about job applicants – and, as such, guided

---

[165] Available at: http://www.hrcomplianceinsider.com/newsletter/beware-the-dangers-of-%E2%80%soc [Accessed: 24 January 2011].
[166] Available at: http://www.itnewsafrica.com/?p=3380 [Accessed: 19 January 2010].
[167] Available at: http://news.cnet.com/8301-17852_3-10404633-71.html [Accessed: 19 January 2010].
[168] Available at: http://www.cbc.ca/canada/montreal/story/2009 [Accessed: 11 January 2011].

individuals to be cautious with regards to the information they chose to share, and with their social networking site privacy settings.[169] The Office further communicated that the consequences of inappropriate disclosure of information on social networking sites could be:

- A defamation lawsuit;
- Copyright, patent or trademark infringement claims;
- Privacy or human rights complaints;
- A workplace grievance or unfair labour practice complaint;
- Criminal charges with regards to obscene or hate materials;
- Damage to the employer's reputation or business interests.

Legal accountability, in the form of damages or similar, resulting from such action could rest with individuals, management, or the wider organization.[170] As such, the Office encouraged employers to develop clear policies with regards to the use of social networking sites, specifically communicating in plain language what data should not be disclosed. [171]

Finally, in 2010 in the matter of *Sheridan College Institute of Technology and Advanced Learning v. Ontario Public Service Employees Union* an employee was dismissed for inappropriate computer use, as well as what was considered an insolent comment made in a Facebook posting – the picture of the buttocks of a mountain climber, with an arrow pointing at it, with a caption inviting his manager to, *'...kiss this.'* In arbitration the dismissal was found to be justified based on various facts, including the employee's lack of remorse; disregard for his employer's financial and business interests; his position of trust and access to highly sensitive

[169] Available at: http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm [Accessed: 18 January 2010].
[170] Available at: http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm [Accessed: 18 January 2010].
[171] Available at: http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm [Accessed: 18 January 2010].

information; and his knowledge of the employer's rules and expectations regarding personal computer usage; amongst other factors.[172]

Despite all the media attention, in Canada an employer's ability to terminate an employee for online comments – as with most jurisdictions – currently still remains largely untested.[173]

Thus, various international communities have seen different contexts, circumstances and outcomes at play in relation to the posting of comments on social networking media by employees, and the impact of such on the employer. The tension between the individual's right to free speech and privacy, when offset against the employer's right not to be defamed, or to have its business interests compromised is a complex one, which may be influenced by multiple facets. However, the importance for both employees and employers of understanding their rights and vulnerabilities in this regard is clear. As such, we turn to an examination of the findings in this regard.

[172] Available at: http://blogs.hrhero.com/northernexposure/2011/01/17/ [Accessed: 24 January 2011].
[173] S.D. Todd *Facebook comments: just cause for termination?* Available at: http://www.heenen.co/fr/nouvelles/pdf/Facebook_comments_just_cause_for_termination.pdf [Accessed: 24 January 2011].

4. Results and Findings

Reverting back to the question of this paper, this section will be used to analyse the findings in the legislation, literature and case law in order to determine the rights of employees, as opposed to those of the employer when it comes to workplace related comments aired via social networking media.

In terms of the rights to privacy and freedom of speech, of all the countries reviewed the protection of these rights are both provided for in some form or another. We see that, in the case of both South Africa and the United Kingdom, both of these rights are legislated. However, in terms of the United States, New Zealand and Canada, although the right to freedom of speech and/ or expression is legislated, there is no explicit right to privacy. However, in all three of these countries the courts have determined that there is an implied right to privacy stemming from the law. Australia is the only country of those reviewed which has no legislated right to freedom of expression or speech although, again, the courts have recognised an implied right to such. In addition, Australia does not recognise a constitutional right to privacy, although the courts have recognised a potential common law right to this.

In terms of the workplace, however, in all of the jurisdictions considered none of these rights are absolute. Where individual actions infringe upon the employer's right to protect its good name and business interests the individual's rights regarding freedom of speech and the right to privacy may no longer hold true. This is particularly the case

where the employer's name is brought into disrepute through the actions of the employee.

Further, with regards to privacy, in various jurisdictions it has been found that the individual has limited expectations of privacy on public forums, such as the Internet – particularly where the communications were publicly accessible.[174] And further, where communications have been made utilising the employer's computer equipment, the expectation of a right to privacy may further be weakened.[175]

What of defamation, and the tension with the individual's right to free speech and/ or expression? In this analysis it has been found that, in order to avoid a claim of defamation, the comment made must be factual. As such, if a comment made on a social networking site is untrue, subjective, based on opinion and/ or is derogatory of another party in some way, the individual's right to freedom of speech or expression may no longer be protected, in favour of the right of the opposing party not to be defamed – such as an employer. In such an instance, the individual – perhaps an employee – making such derogatory comments might be open to litigation. We have also seen that, in South Africa specifically, an individual might be open to a criminal charge for crimen injuria.

---

[174] *Sedick &Another and Krisray (Pty) Ltd* (2011) 32 ILJ 752 (CCMA); T.S. Zurbrigg *Facebook: What Employers Need to Know About Workplace Privacy, Discipline & Dismissal* Available at: http://www.fieldlaw.com [Accessed: 24 January 2011].

[175] Available at: http://www.nytimes.com/2001/05/18/us/dismissed-for-chat-room-cia-workers-speak-out.html?pagewanted=1. [Accessed: 18 January 2010]; *Smythe v Pillsbury Co* 914 F Supp 97 (ED) Pa 1996.

Turning to the workplace specifically, so what if an employee makes statements on a social networking site which the employer deems to be in conflict with its business? In such a case, we have seen that a number of factors may be of importance, such as:

- The nature of the comments made, and its impact on the employer, for example, were the comments negative in nature; and did they identify the employer, thus potentially bringing the employer into disrepute;
- How the employer came to have access to the comments, for example, were such comments freely accessible by the public, or did the employer use measures – either elicit (thus potentially breaching an individual's right to privacy) or not – to obtain access to the information;
- Were the comments made factual, and a fair reflection of an individual's right to free speech, or not.

Whether comments made via social networking media amount to a disciplinary offence is dependent on the nature of the job, as well as the potential for damage to the employer's business or reputation. In terms of comments made on such sites outside of working hours there must be a link between the damaging off duty conduct and the nature of the work or the employer's business interests. However, the employer cannot control an individual's private life. This must be respected unless an employee's private actions impact on the job or the employer in some way. All the facts of the matter at hand will be considered by the courts on a case by case basis in their totality when deciding whether a

dismissal for allegedly defamatory comments – or comments allegedly bringing the employer into disrepute – is fair or not.[176]

A derogatory comment posted on a social networking site will be considered defamatory if it contains untruths about the employer, and if it undermines the employer's reputation in the minds of 'right thinking' members of society. For the same material to be considered libellous it must be permanent in nature, and must clearly identify the employer – either directly or by inference – and the meaning of the comments made must be in some way damaging to the company's reputation. Should this be found to be the case the employer may have recourse to either one or more of the following:

- Seek to have the material removed from the social networking site;
- Bring a civil claim for damages against the author of the comments (and possibly against the site for publishing such comments);
- Demand the employee remove the comments made from the site, and invoke internal disciplinary action, or action for breach of contract.[177]

Another matter explored regarding defamation, and for consideration by employers, is that of vicarious liability. Should an employee post potentially defamatory statements on a social networking site about a third party – such as a competitor, customer or client – during the course of his or her employment, the employer could in fact be held

[176] *Protecting your company's reputation* Available at: http://www.personneltoday.com/articles/2008/06/20/46378/protecting-your-companys-reputation.html [Accessed: 6 January 2011].
[177] Available at: http://www.xperthr.co.uk/faqs/topics/15,162/negative-comments-on-social-media.aspx?articleid=104600&mode=open#104600 [Accessed: 7 February 2011].

vicariously liable for such actions. In such an instance the employer should seek to have the material removed from the site as quickly as possible – either by the employee, or by going directly to the social network. Following this, it would be imperative for the employer to determine whether it could be held liable, or whether the employee had acted outside of the scope of employment. Finally, based on the findings of an investigation, discipline of the employee may be a fair response.[178]

Turning to the case law and literature review from the various countries analysed, with reference to South Africa, it was found that case law defining where employees have made comments about their employers on social networking sites, and subsequent action taken for such, is virtually non-existent – although the CCMA has begun hearing more matters of this type, suggesting it is only a matter of time before such matters find their way in to the Labour Courts. As such, it was necessary to also look at case law where other communication mediums – such as, newspaper and web articles, and email, for example – have been used by employees for airing their views. In addition, cases involving comments made on social networks but outside an employment situation were reviewed.

It was found that, employees have a common law duty to act in good faith towards their employer, and to further its business interests.[179] It is an inherent requirement of the contract of employment that employees provide their labour in return for remuneration. As such,

---

[178] Available at: http://www.xperthr.co.uk/faqs/topics/15,162/negative-comments-on-social-media.aspx?articleid=104600&mode=open#104600 [Accessed: 7 February 2011].

[179] Grogan, J. *Dismissal, Discrimination & Unfair Labour Practices* (2007) JUTA & Co Ltd; Available at: http://www.irnetwork.co.za/nxt/gateway.dll?f=templates$fn=default.htm$vid=irnetwork:10.1048/enu [Accessed: 1 October 2010].

they are considered subordinate to the employer and are, to some extent, under the employer's control in the workplace.[180] Therefore, negative comments made via social media which can be directly linked back to the workplace could feasibly be construed to be an act warranting discipline.

However, the employer does not have the same control over an employee's private activities. That is to say, unless the employee's private activities impinge on the employer in some way. South African case law has shown that an employee's right to privacy may be trumped by the employer's right to fair labour practices, and to not have its good name besmirched.[181] On this basis, the courts would need to weigh up the individual's fundamental right to privacy in comparison to the employer's right to advance its business interests. In this instance the Section 36 limitation in the Constitution may come in to play. However, where the employer is questioning an employee's actions outside of the workplace, the employer will be required to show that it has a legitimate interest in the matter.[182] Despite this, where the employee's actions – private or otherwise – are found to have destroyed the relationship of trust and a harmonious working relationship with the employer, the latter cannot be expected to continue with such a relationship.

In terms of a charge for bringing the employer into disrepute for comments made via social networking sites, such a charge may be considered on its own, or in aggravation of other charges (such as the violation of an electronic communication policy, for example). Employees

---

[180] Available at: http://www.proappoint.co.za/blog/2009/09 [Accessed: 19 January 2010].
[181] Available at: http://www.proappoint.co.za/blog/2009/09 [Accessed: 19 January 2010].
[182] *Van Zyl v Duhva Opencast Services* (Edms) Bpk (1988) 9 ILJ 905 (IC).

are duty bound to uphold the reputation of their employer, other employees and clients.[183] However, the facts of the matter at hand will have to be considered in their totality before determining whether an employee is guilty of such. Despite this, a charge of bringing the employer into disrepute has been suggested to be a vague and difficult one to prove; and a charge reflecting the nature of the alleged offence in more detail may be a wiser and more effective choice. Employers would be required to clearly lead evidence to prove an allegation of bringing same into disrepute – often found to be difficult. Thus it may be advisable to utilise a charge which reflects the alleged transgression more accurately in order for this to pass muster.[184]

Other recourse which the South African employer might resort to outside of the ordinary internal disciplinary process might be civil charges for defamation (as has been found to apply in various other jurisdictions too), or criminal charges for crimen injuria. In addition, an employer may have to consider risks of vicarious liability where comments by employees via social media are made regarding third parties in the course and scope of the employee's work-related duties.

The only potentially legitimate reason found by which an employee could make negative statements via social networking sites regarding an employer, was if such statements were factual and/ or reflected an honest opinion in the public interest – as has been found in matters relating to other media forms.[185] In such a case, the employee would have a stronger opportunity for proving his or her right to freedom of

---

[183] Grogan, J. *Dismissal, Discrimination & Unfair Labour Practices* (2007) JUTA & Co Ltd.

[184] Rycroft, A. *Bringing the Employer into Disrepute* (2008) 29 *ILJ* 1605.

[185] *Cosawu obo Khumalo and Royal Ascot Superspar* (2006) 27 *ILJ* 2452 (CCMA).

expression. However, there will always be some risk to the employee of an alternative finding based on the limitations as contained in the Constitution and, as such, employees would be advised to rather utilise mechanisms specifically provided for in legislation, such as the *Protected Disclosures Act*, or via internal organisational mechanisms, such as grievance procedures.

Turning to the comparative situation in the United States, more case law was available specifically with regards to negative comments made by employees on social networking sites regarding their employers. Of interest, various matters relating to the medical industry were documented – highlighting an additional factor for consideration by employers; that of ethical implications for actions by employees. Related to this, one could easily envisage a claim for vicarious liability where an employee's actions (such as those of a doctor or nurse) via social networking media breached a third party's confidentiality.

Ethical considerations were also brought to light where various educational institutions had utilised student information from social networking media to take disciplinary action against students. Such information usage could feasibly be viewed as a breach of privacy rights. In relation to this, the workplace matter of *Pietrylo v. Hillstone Restaurant Group*[186] highlighted the risk posed to employers should they utilise undesirable methods of accessing such information. If information from social networking sites is accessed utilising illegal or illegitimate means, even if such information is found to be defamatory or

[186] 2:06-cv-5754. Available at: http://www.employerlawreport.com/uploads/file/PIETRYLO%20v%20%2HILLSIDE%20RESTAURANT.pdf [Accessed: 18 January 2010].

to bring the employer into disrepute, this will not prevent the courts from finding that a dismissal was unfair. In South Africa such information was found by the CCMA to be inadmissible as evidence.[187]

However, also in terms of the right to privacy, another matter saw the courts finding that, where actions were taken utilising company equipment, an employee had no expected right to privacy, and the employer's right to prevent the misuse of its property outweighed the employee's expectation of privacy.[188]

Another factor of interest from the U.S. case context considered comments made on social networking sites outside of working hours. In such matters the courts looked at the type of work concluded by the employee in relation to their social networking activities, as well as the referencing of the employer on such sites. On this basis, it was found that, where an employer was not sufficiently referenced in the postings, there was little to no damage to the employer's reputation, and a dismissal for such could therefore not be fair.[189] This approach was also deemed appropriate in the Australian context.[190]

In terms of the tension between the right to freedom of speech and defamation, U.S. courts have found that, where statements made are so

---

[187] *Nancy Smith and Partners in Sexual Health (Non-Profit)* WECT 13711-10 (CCMA).
[188] *Smythe v Pillsbury Co* 914 F Supp 97 (ED) Pa 1996.
[189] *Protecting your company's reputation* Available at: http://www.personneltoday.com/articles/2008/06/20/46378/protecting-your-companys-reputation.html [Accessed: 19 January 2010].
[190] Available at: http://blakedawson.com/Templates/Publications/x_publication_content_page.aspx?id=60241 [Accessed: 22 January 2011].

inconceivable that it is unlikely that anyone would believe them, this is not defamation but in fact equates to protected speech. However, where a statement is untrue but is likely to be believed this will constitute defamation and/ or libel.[191]

Further, the question in the United States of whether a policy governing online activities and Internet postings is too broad for a dismissal based on the violation of such a policy has come to light.[192] This suggests that employers may have to pay close attention to the wording and protections provided for in their internal policies if they do not wish to face a similar challenge.

Finally of interest from the U.S. scenario, the courts looked at the type of broadcast media used to air views or comments, and found that some broadcast media – such as, television or radio – are more invasive than others. Thus, the type of media utilised to air negative comments could also conceivably impact on the decision of a court.[193] This approach has been echoed more recently in South Africa, where it was stated specifically that the contents of an email between a limited number of parties cannot necessarily be compared to postings on a publicly accessible blog or social networking website.[194]

---

[191] Available at: http://articles.sitepoint.com/article/fake-social-networking-profiles [Accessed: 22 January 2011].
[192] Available at: http://epic.org/privacy/workplace/default.html [Accessed: 9 February 2011]; http://www.facebook.com/notes/labor-relations-today/nlrb-parties-settle-facebook-firing-case [Accessed: 10 February 2011].
[193] *Freedom of Speech & Technology – the Reno, Multnomah & Baker case* Available at: http://cs.ua.edu/340/fall10/freespeech_pta.ppt [Accessed: 22 January 2011].
[194] *Nancy Smith and Partners in Sexual Health (Non-Profit)* WECT13711-10 (CCMA).

Similar to the situation in South Africa, the United Kingdom's courts have to date also not significantly explored the matter of comments made specifically on social networking sites, although there has been slightly more guidance provided to date by this jurisdiction. As with the U.S, the U.K. has also experienced some circumstances of educational institutions utilising information obtained via such sites to discipline students. In such instances it has been argued that the accessing of this information may be viewed as a violation of an individual's right to privacy.[195]

However, in the most interesting matter reviewed from the U.K, the false creation of a Facebook profile was viewed as a misuse of private information, and found to constitute both defamation and libel.[196] Although not a workplace-specific matter, it may be argued that employers might make use of similar recourse, as well as proceeding with internal disciplinary measures for bringing the employer into disrepute.

Finally with regards to the United Kingdom, like in South Africa, concerns of employers being vicariously liable for the activities of their employees on social networks, where such activities impact a third party, have come to light.[197] The U.K. courts have shown that they are willing to apply a wide definition when it comes to vicarious liability.[198]

---

[195] Available at: http://www.guardian.co.uk/media/2007/jul/17/digitalmedia.highereducation [Accessed: 21 December 2010].
[196] *Applause Store Productions Ltd. & Anor v Raphael* [2008] *EWHC* 1781 (QB) (24 July 2008).
[197] Collier, D. *Workplace Privacy in the Cyber Age* (2002) 23 *ILJ 1744.*
[198] Available at: http://www.walkermorris.co.uk/content.aspx?id=619 [Accessed: 9 February 2011].

Australian experts have warned that discipline for comments made on social networking media could be viewed as illegal if internal company policies fail to clearly cover such usage – specifically the usage, and improper usage, of social networking sites.[199] In a particular matter in Australia, a dismissal was deemed unfair where the employer was not identified in the negative social networking posts made by the employee.[200] Again, as with the U.S. scenario,[201] this indicates that it will be important for the courts to assess the nature of the comments made, whether the employer is identified in such comments, and to what extent the employer is or is not brought into disrepute by the comments made.

Finally in the Australian context – as with findings in South Africa[202] - it was found that an employee may only be dismissed for out of work conduct if such conduct is likely to significantly damage the employment relationship, or the business interests of the employer.[203] As such, the employer will be required to establish that it is legitimately impacted by the employee's private actions.

---

[199] Available at: http://www.smh.com.au/articles/2009/04/03/1238261779328.html [Accessed: 18 January 2010].
[200] Available at: http://blakedaweson.com/Templates/Publications/x_publication_content_page.aspx?id=60241 [Accessed: 22 January 2011].
[201] *Protecting your company's reputation* Available at: http://www.personneltoday.com/articles/2008/06/20/46378/protecting-your-companys-reputation.html [Accessed: 19 January 2010].
[202] *Van Zyl v Duhva Opencast Services* (Edms) Bpk (1988) 9 *ILJ* 905 (IC); *NUM & others v East Rand Gold & Uranium Co Ltd* (1986) 7 *ILJ* 739 (IC); *Mavumengwana v Samancor Ltd (Metalloys)* (1992) 1 *LCD* 200 (IC).
[203] Available at: http://blakedaweson.com/Templates/Publications/x_publication_content_page.aspx?id=60241 [Accessed: 22 January 2011].

In New Zealand it was noted that employees are not precluded from making comments regarding their workplaces on social networking sites – resorting to their right to freedom of expression – unless such comments in any way harmed the reputation of the employer. However, this right to freedom of expression was limited, as with the limitations with regard to defamation and libel law.[204]

Finally, with regards to the Canadian context, it was found that, as with most of the other jurisdictions considered, the ability to dismiss employees for online postings still remains largely untested.[205] However, in the few matters to date, it was found that, although individuals have the right to hold opinions,[206] once such opinions are in the public domain, should they have consequences for the employer and the employment relationship, dismissal for such could be justified. Once again, it was found that employers are required to strike a balance between an individual's right to privacy, in relation to an employer's legitimate right to protect its business interests.[207] But where comments were found to be damaging to the employer this could be considered a justifiable reason for dismissal.

Interestingly, the Canadian courts found in various matters that a person with multiple 'friends' on a social networking site had no reasonable expectation of privacy; and further, that the reality of the

---

[204] Available at: http://www.nzherald.co.nz/email/news/article.cfm?c_id=188&objectid=10483277 [Accessed: 18 January 2010].

[205] S.D. Todd *Facebook comments: just cause for termination?* Available at: http://www.heenen.co/fr/nouvelles/pdf/Facebook_comments_just_cause_for_termination.pdf [Accessed: 24 January 2011].

[206] T.S. Zurbrigg *Facebook: What Employers Need To Know About Workplace Privacy, Discipline & Dismissal* Available at: http://www.fieldlaw.com [Accessed: 24 January 2011].

[207] Available at: http://www.hrmguide.net/canada/law/inappropriate-use.htm [Accessed: 24 January 2011].

Internet is that privacy may never be entirely guaranteed.[208] Further, the Canadian courts found that, even where comments were made on a non-work related blog, where this undermined the employment relationship, termination could be warranted.[209] The same would feasibly apply to comments made on a personal social network profile outside of working hours.

As with the United Kingdom and United States of America, it was found that institutions in Canada (in this case a medical insurance provider) were utilising information obtained from social networking sites to take action against individuals (in this case, the withdrawal of sick benefits),[210] posing further challenges to individuals in maintaining their individual rights to privacy. Further, the risk of vicarious liability of Canadian employers for the actions of their employees via social networking media, as with most jurisdictions, was considered a concern which should be mitigated by the development of clear internal policies governing the usage of such sites.[211]

Finally, in an arbitrated matter in Canada, the forum considered various factors to determine whether an employee had been unfairly dismissed for comments made via a social network, including:

---

[208] T.S. Zurbrigg *Facebook: What Employers Need To Know About Workplace Privacy, Discipline & Dismissal* Available at: http://www.fieldlaw.com [Accessed: 24 January 2011]; S.D. Todd *Facebook comments: just cause for termination?* Available at: http://www.heenen.co/fr/nouvelles/pdf/Facebook_comments_just_cause_for_termination.pdf [Accessed: 24 January 2011].

[209] *Government of Alberta and Albert Union of Provincial Employees (R. Grievance)* [2008] A.G.A.A. No. 20, April 11, 2008.

[210] Available at: http://www.itnewsafrica.com/?p=3380 [Accessed: 19 January 2010]; http://news.cnet.com/8301-17852_3-10404633-71.html [Accessed: 19 January 2010]; http://www.cbc.ca/canada/montreal/story/2009 [Accessed: 11 January 2011].

[211] Available at: http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm [Accessed: 18 January 2010].

- Lack of remorse shown;
- Disregard for the employer's business interests;
- The employee's position of trust;
- Access to sensitive employer information; and,
- Knowledge of the employer's internal policies and rules governing the usage of company computers, and online communication mechanisms.[212]

Once again, this indicates that the courts will be required to consider all facts relating to a particular matter in totality when deciding whether a dismissal is fair or not.

In summation, there is no one answer as to when employers will be able to fairly take action against employees for comments made on social networking sites. However, as was evidenced in all jurisdictions examined, the courts will need to look at all the facts of the matter in their totality in order to conclude whether a dismissal was fair or not on a balance of probability, including:

- The tensions between the rights of the employee – such as to privacy, and freedom of expression – and the rights of the employer not to have its reputation tarnished, and to protect its business interests;
- Did the employer access the relevant information legitimately;
- The nature of the comments made, and their impact on the workplace;
- The public nature of the comments made, for example, who would have access to such comments – including possibly an analysis of

[212] Available at: http://blogs.hrhero.com/northernexposure/2011/01/17/ [Accessed: 24 January 2011].

the type of media utilised, as well as the relevant privacy settings on the site;

- Was the employer sufficiently identified in the comments made;
- Whether the employee's actions were taken in or outside of working hours, and – if outside – can the employer show a legitimate link between the comments made and the workplace;
- In terms of the potential for vicarious liability, did the employee act within the scope of his or her employment, or did he or she engage in a 'frolic' of his or her own;
- Were the comments made factual, an honest opinion, or in the public interest, or did these amount to defamation and/ or bringing the employer's name into disrepute;
- Has the relationship of trust between the employer and employee been broken;
- Did the employer have a policy in place clearly governing the usage and comments made via social networks, and was the employee aware of the rules in this regard; and
- Any other factors relevant to the matter at hand.

Social networking in the workplace is a tool which employers might exploit as useful and cost effective – such as, as a way of encouraging teams located in different offices to communicate. However, as we have seen, there may also be various drawbacks with such a tool, such as, wasteful usage of employee time, and becoming a negative forum for employees to complain or gossip about work.[213] It is therefore important that employers set rules with regards to the usage of such forums; that they ensure that employees are aware of such rules; as well as being

[213] *Social networking sites: Networking or not working?* Available at: http://www.personneltoday.com/articles/2007/09/12/42102/social-networking-sites-networking-or-not-working.html [Accessed: 6 January 2011].

aware of the possible actions to be taken should employees break these rules.

As such, we now turn to recommendations to employers of how to manage the usage of social networking in the workplace, as well as the potential risks of misuse. In addition, recommendations will be provided for employees to manage their personal usage of such networks in relation to the workplace, and how to avoid potentially costly 'mistakes' related to this usage.

5. Recommendations

So what should employers do when faced with similar matters in the workplace? It is important that employers set parameters with regards to social networking. Any workplace online forums should be managed and monitored carefully. Employees should be reminded that they may be seen as representatives of the company in any social networking which they undertake. Existing email and Internet usage policies should be extended to include both corporate social networking, as well as the personal use of social networking media – both during and outside of working hours. Thus, any potentially defamatory statements made by employees about the company, its clients, or co-workers should be treated as a disciplinary offence, and the potential for this should be clearly indicated in the company's rules and policy documents.[214]

Many employers have implemented a total ban on social networking in the workplace. Some of the possible problems created by social networking in the workplace include:

- Productivity losses;
- Threats to business confidentiality;
- Undermining of management;
- Harm to the company's reputation[215];
- Impact on business IT systems.

---

[214] *Social networking sites: Networking or not working?* Available at: http://www.personneltoday.com/articles/2007/09/12/42102/social-networking-sites-networking-or-not-working.html [Accessed: 6 January 2011].

[215] Available at: http://www.hrcomplianceinsider.com/newsletter/beware-the-dangers-of-%E2%80%soc [Accessed: 24 January 2011].

However, in some instances, social networking media have been effectively used in commercial settings to stimulate productivity – such as, to generate ideas; share resources and knowledge; and to connect with the employer's audience and current, or potential, customers. This usage is usually industry-specific.[216] In order to protect such usage – such as usage for marketing purposes - employers could consider limiting access to a few individuals. In addition, it is advisable that employers ensure their own social media passwords are kept confidential by those with access, and to update passwords every few months or so.[217] Finally, employers might consider disabling certain Internet protocols, or installing and using Internet-use monitoring software.[218] Thus, each employer will have to decide whether to implement a total or partial ban on workplace social networking, or whether to allow free access to this. However, whatever an employer decides, clear and detailed policies governing such usage will be vital in protecting the employer from abuse.

As a guideline, company policies on social networking usage should include elements such as the following:

- Employees may not divulge information which is company sensitive (and 'company sensitive' information should be clearly defined);
- Limitations on access to social networking sites during working hours should be clearly articulated, such as, before or after work,

---

[216] Available at: http://www.labournet.co.za/NewsItem.aspx?ID=339f3e63-f912-4fd6-8d76-440006ffb589 [Accessed: 14 December 2010].

[217] Available at: http://gadllp.co.uk/blog/?tag=vicarious-liability [Accessed: 9 February 2011].

[218] Mischke, C. *Disciplinary action and the internet: Responding to employee abuse of email, network and internet access* (1999) Vol 9(5) *CLL* 41.

during lunch breaks, or not at all – whichever is relevant to the employer;

- Any blogs including content related to the workplace should be signed off, and permission for such provided in writing, by a manager with authority to do so. For example, in the case of marketing blogs;
- Employees must be made aware that private blogs which impinge on the company's business interests or reputation in any way are unacceptable, and the fact that they are private will not protect the employee from liability;[219]
- The fact that the employer monitors the usage of social networking media, and what the consequences of non-compliance with the policy may be;[220]
- Employers should also consider including the misuse of social networking, and other electronic communication mediums, in their workplace harassment policies, as several studies have indicated that these technologies are an increasing medium for harassment between colleagues;[221]
- It is important to ensure that employees have signed such policies, in order to illustrate the fact that they have read, understood, and are aware of the potential outcome should they fail to comply.[222] Of course, in South Africa in particular where we have the reality of eleven official languages, a signature is not fool-proof evidence of understanding. In such instances it is advisable that policies are explained to employees in their mother tongue, and that a witness signs attesting to this fact;

---

[219] Available at: http://www.itnewsafrica.com/?=3380 [Accessed: 6 January 2011].
[220] Available at: http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm [Accessed: 18 January 2010].

[221] Available at: http://www.hrmguide.net/canada/law/inappropriate-use.htm [Accessed: 24 January 2011].
[222] Available at: http://news.cnet.com/8301-17852_3-10404633-71.html [Accessed: 19 January 2010].

- Finally, employers should ensure that they regularly update policies in order to keep them abreast of developments in technology, legislation and enforcement decisions.[223] The communication of such changes to employees is also important.

It is important that employees are further reminded of the contents of such policies, and the implications for non-adherence, on a regular basis.[224]

Employment policies on social networking should establish best practice, and outline expectations of acceptable use clearly – as we have seen, policies which are not clearly defined or which are too broad, may come under scrutiny.[225] Policies should inform employees in plain language what the requirements are. In particular, they should determine what data should not be disclosed about employees themselves, their colleagues, clients, and the employer – including any relevant legislation governing the collection, use or disclosure of information. However, it is also important that employers themselves act according to the same code in order to ensure employee privacy – a privacy friendly workplace requires the fair use of data by all parties concerned.[226]

---

[223] Available at: http://www.hrmguide.net/canada/law/inappropriate-use.htm [Accessed: 24 January 2011].

[224] Mischke, C. *Dismissal for abuse of email: Arbitration award sets decisive tone on employer rights over use of email facilities* (2002) January 11(6) *CLL* 51.

[225] Available at: http://epic.org/privacy/workplace/default.html [Accessed: 9 February 2011]; http://www.facebook.com/notes/labor-relations-today/nlrb-parties-settle-facebook-firing-case [Accessed: 10 February 2011].

[226] Available at: http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm [Accessed: 18 January 2010].

Employees should have no expectation of privacy in relation to information stored or disseminated via computers provided by the employer. As such, the employer should state its intention to monitor online traffic, including emails sent, and access to all web pages, including social networks. In addition, the employer should state in its policy that it has the right to read messages, and under what circumstances it intends doing so. This is an important provision, as messages may only be intercepted if the sender has been made aware of such potential interception, including being made aware that the employer may read such messages – in South Africa such interception and monitoring is governed by the *Interception and Monitoring Prohibition Act 127 of 1992.*[227]

Further, it is important to tell employees why social networking usage is limited or excluded from the workplace. For example, due to bandwidth considerations; workplace productivity; or concerns regarding impacts to the employer's reputation;[228] the potential for computer viruses[229]; as well as due to risks of vicarious liability for an employee's actions.[230] This way employees may take informed responsibility for their own actions, and are not surprised if action is taken for transgressions.

In order to mitigate against the risks of vicarious liability, employers might consider the publication of their policies related to social network usage; in order to provide clients, customers and other stakeholders

---

[227] Mischke, C. *Disciplinary action and the internet: Responding to employee abuse of email, network and internet access* (1999) Vol 9(5) *CLL* 41.

[228] Available at: http://www.itnewsafrica.com/?=3380 [Accessed: 6 January 2011].

[229] Available at: http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter7.htm [Accessed: 7 February 2011].

[230] Available at: http://www.xperthr.co.uk/faqs/topics/15,162/negative-comments-on-social-media.aspx?articleid=104600&mode=open#104600 [Accessed: 7 February 2011].

with a degree of comfort that employee actions are monitored and managed with relation to such usage.[231]

Finally, there may be a need to align a new policy with regards to social networking in the workplace with existing policies, such as, confidentiality of company information; security practices; monitoring of other forms of communication; computer equipment usage; amongst others.[232] Workplace policies do not act in isolation, and if these are found to be contradictory, it will be difficult for the employer to establish that employees were aware of the rule – or that the rule was fair.

Despite the distinct advantage of introducing electronic communications policies dedicated to the regulation of social networking in the workplace, it is imperative for employers to first ascertain whether the introduction of such policies amounts to a change to terms and conditions of employment. While the South African courts have not yet been required to test this, it has been argued by many that introduction of such policies would not amount to a change in contractual terms, but would form part of the directives required for the ordinary and necessary running of a business and, as such, would be the prerogative of management. Despite this, there is a small possibility that employees could argue the fairness of the implementation of such policies as a labour practice under the Constitution. However, if there is a justifiable

[231] Available at: http://www.gadllp.co.uk/blog/?tag=vicarious-liability [Accessed: 9 February 2011].
[232] Available at: http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter7.htm [Accessed: 7 February 2011].

reason to implement such a policy from a business perspective this should pass a test for fairness.[233]

However, what if, despite taking all the relevant precautions, a matter comes to light where an employee has made comments on a social network which could have damaging consequences for the employer? If so, the employer should consider the following prior to taking disciplinary action:

- Consider whether there is a significantly close relationship between the conduct and the employee's work;
- Consider whether the conduct is likely to cause serious damage to the employment relationship;
- Consider whether the conduct could damage the employer's reputation or business interests;
- Consider whether the conduct is in conflict with the employee's duties in some way;
- Consider whether the comments made have breached the employee's implied duty of trust and confidence;
- Consider whether the conduct has contravened an employment policy, and what the possible action for such contravention could be;[234]
- Ensure that any charges to be levied against an employee are specific, and relate to reasonable rules;[235]

---

[233] Available at: http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter7.htm [Accessed: 7 February 2011].

[234] Available at: http://blakedaweson.com/Templates/Publications/x_publication_content_page.aspx?id=60241 [Accessed: 22 January 2011].

[235] Rycroft, A. *Bringing the Employer into Disrepute* (2008) 29 *ILJ* 1605.

- Finally, if it comes to the attention of the employer that there have been problematic social networking posts or comments, employers should consider proper documentation of the evidence of such, such as, by making copies of the relevant screens, in order to document the relevant date, time and content of the postings.[236] It is, however, imperative that employers access such information by lawful means – 'hacking' into an employee's Facebook account, or similar, in order to obtain such information would be considered unlawful.[237]

Employers should also be careful not to impose their personal views and opinions of what social networking and Internet misuse is. A clear and objective standard must be applied – although individual organisational culture may have an impact, and may vary, from workplace to workplace.[238]

In terms of South African law, it is a broad principle that the dismissal of an employee is only justifiable where the relevant misconduct has resulted in the irretrievable breakdown of the relationship between employee and employer. In order to do so, the employer must establish:

- That there was a rule;
- That the rule was reasonable;
- That the employee was aware of the rule.

---

[236] T.S. Zurbrigg *Facebook: What Employers Need To Know About Workplace Privacy, Discipline & Dismissal* Available at: http://www.fieldlaw.com [Accessed: 24 January 2011].

[237] Available at: http://www.xperthr.co.uk/faqs/topics/15,162/negative-comments-on-social-media.aspx?articleid=104600&mode=open#104600.[Accessed: 7 February 2011].

[238] Available at: http://www.nzlawyermagazine.co.za/Archives/Issue104/N3/tabid/1543/Default.aspx [Accessed: 21 December 2010].

If the employer is able to answer 'yes' to each of these three points, it may move to establish whether the employee is in fact guilty of breaching said rule on a balance of probabilities. Only once this has been established in the affirmative may the decision be made as to whether the misconduct warrants dismissal or not (also based on previous practice).[239] As such, the policies governing the usage of social networks in the workplace, and the details of their communication to employees, will become imperative if and when issues of misuse by employees come to light.

In a survey of South African companies it was found that most had experienced Internet abuse, and addressed this, in some form or another – usually in the form of an Internet acceptable usage policy. However, it is not good enough to write a policy. Much will focus on the application of the policy; the existence, fairness and breach of the rule; consistency of application; and severity of sanction in order to determine the fairness of a dismissal.[240]

And what of aggrieved employees who wish to air their disgruntlement? In South Africa employees may make disclosures under the *Protected Disclosures Act*, where such disclosures are deemed to be in the public interest, and where there is a legitimate wrong-doing by the employer. Such disclosures, and the individuals making them, are protected from victimisation and recourse by the employer.

---

[239] Available at: http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter7.htm [Accessed: 7 February 2011]; Van Niekerk et al, *Unfair Dismissal* 3ed (2006) SiberInk at 53-57.

[240] Dancaster, L. *Internet Abuse: A Survey of South African Companies* (2001) *ILJ* 862.

Further, with reference specifically to the matter of Royal Ascot Super Spar,[241] where employees air a genuine and factual grievance this will be protected as an act of free expression. Also, where comments are made in private, such as in private online forums, such comments may be protected under the right to privacy – as was seen in the matter in the United States of *Pietrylo v. Hillstone Restaurant Group*[242]. Similarly, if employees express frustration online in a manner which does not identify the employer, or any other party, they will usually be protected from recourse. However, there is risk associated with this if such comments come to the attention of the employer and/ or the public, thus potentially bringing the employer into disrepute.

Employees are under a common law obligation to further their employer's business interests. Thus, should they do anything which could potentially destroy harmonious working relationships with the employer or colleagues they may face dismissal.[243] Users of social networking sites should avoid personal opinions or negative statements which are not 100% accurate, or which harm another party's image or reputation.[244] However, as we have seen from the research data, potential employers and other institutions are also trawling social networking sites as a means of 'checking up' on the activities of potential employees, and thus making judgments – whether correct or not – on whether individual's are a fit to such organisations or not.

---

[241] *COSAWU obo Khumalo v Royal Ascot Superspar* (2006) 27 *ILJ* 2452 (CCMA).
[242] 2:06-cv-5754. Available at: http://www.employerlawreport.com/uploads/file/PIETRYLO%20v%20%2HILLSIDE%20RESTAURANT.pdf [Accessed: 18 January 2010].
[243] Available at: http://proappoint.co.za/blog/2009/09 [Accessed: 6 January 2011].
[244] Available at: http://phillipsgivenslaw.blogspot.com/2009/06/defamation-and-social-media.html [Accessed: 19 January 2010].

Employees must be aware that any information or comments posted on their social network profile could be accessed by any one or more of the following (depending on privacy setting set-up on the site):

- Current or potential employers;
- Recruitment agencies;
- Colleagues;
- Clients or suppliers of the employer;
- The employer's competitors;
- Government and law enforcement agencies;
- Others outside one's trusted network.[245]

As such, it is recommended that employees refrain from making comments about their employers – or any other comments which they do not wish to be public knowledge - via online media entirely if they do not wish to put themselves at risk of workplace discipline, or similar negative feedback.

However, if an employee has posted a potentially defamatory statement about his or her employer on a social networking site, he or she may be able to defend such statements if:

- The content of the comments made was true (regardless of motive for writing such);
- The statements were an honest opinion on a matter of public interest;
- The comments made were in pursuance of some kind of moral, legal or social duty in the public interest (such as, whistle-blowing); or,

[245] Available at: http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm [Accessed: 18 January 2010].

- The comments are covered by some form of legal privilege.[246]

In terms of employees, important guidelines for the usage of social networking in, or related to, the workplace – and in order to ensure protection - include:

- If your employer has a social media policy read it, and if you do not understand parts of this, ensure you get someone to explain this to you;
- Check your social networking posts regularly, and if there is anything questionable contained therein that you or others have written, delete it;
- Engage with your union or human resources department for advice when in doubt;
- Do not 'whistle blow' via social networks. This is not a positive method for initiating change.[247] Make use of your employer's internal grievance procedures and employee assistance programmes or, in more serious cases, follow the rules as contained in legislation such as the *Protected Disclosures Act.*

Finally, external to the employment arena, but an important recommendation none the less is the requirement for the 'beefing' up of privacy laws for users of social networks, such as Facebook. In the United States at a Congressional hearing on online privacy and social networking, lawmakers have been strongly encouraged to update U.S. law to protect the privacy of Facebook users. It was found that

---

[246] Available at: http://www.xperthr.co.uk/faqs/topics/15,162/negative-comments-on-social-media.aspx?articleid=104600&mode=open#104600 [Accessed: 7 February 2011].
[247] Available at: http://www.examiner.com/human-resources-in-jackson/free-speech-and-social-netowrking-sites-the-employment-issue#ixzz1Bksg1C6N [Accessed: 22 January 2011].

Facebook's regular changes to privacy settings have made it almost impossible for users to control who accesses their personal information.[248] This must surely offend international best practice and legislation regarding individuals' rights to privacy. As such, it is recommended that both the social networks and lawmakers consider the regulation of such sites in order not to offend against the individuals' fundamental right to privacy.

[248] Available at: http://epic.org/privacy/socialnet/ [Accessed: 9 February 2011].

6. Conclusion

The concepts dealt with in this subject matter are complex ones which cross over from the labour to the constitutional arena, and are impacted by the common law duties of employees and employers to each other. As such, all the factors of a given matter will need to be weighed up by the courts, balancing the individual's rights to freedom of speech and/ or expression, and privacy, against the employer's right not to be defamed, or have its reputation damaged, and to further its business interests.

As has been seen, in most jurisdictions, case law relating specifically to employee comments on social networking sites, and their impact on the employer and workplace, is still in its infancy. As such, a precedent has largely yet to be set and it will be interesting to see how the courts unravel the tension between employee and employer rights.

However, what does seem clear is that it is paramount that employers implement clear and detailed policies regarding employee usage of social networking sites – both in and outside the workplace – in order to protect their reputations, and to mitigate against the risks of vicarious liability. Equally, employees will need to monitor their own usage of social networks to ensure that they do not fall foul of employer rules and policies, as well as wider challenges for defamation, libel and/ or crimen injuria. The best way to ensure that this never happens would be to avoid expressing opinions and comments related to employers, and their customers, clients and other stakeholders, at all costs, and to utilise formal mechanisms available to them for the airing of grievances which

do not carry the risks associated with comments made on social networks.

7. Bibliography

Applause Store Productions Ltd. & Anor v Raphael [2008] EWHC 1781 (QB) (24 July 2008).

Available at: http://abahlali.org/node/1117 [Accessed: 19 January 2010].

Available at: http://articles.sitepoint.com/article/fake-social-networking-profiles [Accessed: 22 January 2011].

Available at: http://blakedaweson.com/Templates/Publications/x_publication_content_page.aspx?id=60241 [Accessed: 22 January 2011].

Available at: http://blogs.hrhero.com/northernexposure/2011/01/17/ [Accessed: 24 January 2011].

Available at: http://dictionary.reference.com/browse/defamation [Accessed: 13 December 2010].

Available at: http://dictionary.reference.com/browse/libel [Accessed: 11 February 2011]

Available at: http://en.wikipedia.org/wiki/Crimen_injuria [Accessed: 11 January 2011].

Available at: http://en.wikipedia.org/wiki/Defamation [Accessed: 13 December 2010].

Available at: http://en.wikipedia.org/wiki/Privacy [Accessed: 24 January 2011].

Available at: http://en.wikipedia.org/wiki/Social_network_service [Accessed: 8 December 2010].

Available at: http://en.wikipedia.org/wiki/Use_of_social_network_websites_in_investigations [Accessed: 11 January 2011].

Available at: http://epic.org/privacy/socialnet/ [Accessed: 9 February 2011].

Available at: http://epic.org/privacy/workplace/default.html [Accessed: 9 February 2011].

Available at:
http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [Accessed 11February 2011].

Available at:
http://ilt.eff.org/index.php/Privacy:_Stored_Communications_Act
[Accessed: 7 February 2011].

Available at:
http://law.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html [Accessed: 24 January 2011].

Available at: http://msnbc.msn.com/id/32972597 [Accessed: 18 January 2010].

Available at: http://mybroadband.co.za/news/Internet/6580.html [Accessed: 19 January 2010].

Available at: http://news.bbc.co.uk/2/hi/uk/946400.stm [Accessed: 24 January 2011].

Available at: http://news.bbc.co.uk/2/hi/uk_news/4482073.stm [Accessed: 11 February 2011]

Available at:
http://news.bbc.co.uk/2/hi/uk_news/scotland/4167629.stm
[Accessed: 19 January 2010].

Available at: http://news.cnet.com/8301-17852_3-10404633-71.html
[Accessed: 19 January 2010].

Available at:
http://phillipsgivenslaw.blogspot.com/2009/06/defamation-and-social-media.html [Accessed: 19 January 2010].

Available at: http://saulk.co.za/2009/01/16/crimen-injuria/
[Accessed: 11 January 2011].

Available at: http://www.aph.gov.au/LIBRARY/pubs/rn/2001-02/02rn42.htm [Accessed: 24 January 2011].

Available at:
http://www.bailii.org/ew/cases/EWHC/QB/2008/1781.html
[Accessed: 22 January 2011].

Available at:
http://www.blakedawson.com/Templates/Publications/x_publication_detail_content_page.aspx?id=60287page=1 [Accessed: 22 January 2011].

Available at: http://www.browndailyherald.com/2.12231/the-facebook-not-just-for-students-1.1679665 [Accessed: 11 February 2011].

Available at: http://www.canada.com/vancouversun/news/westcoastnews/story.html?id=fdbe705b-012 [Accessed: 24 January 2011].

Available at: http://www.cbc.ca/canada/montreal/story/2009 [Accessed: 11 January 2011].

Available at: www.cleveland.com/nation/index.ssf/2010/11/feds_rule_against_employer_in.html [Accessed: 18 November 2010].

Available at: http://www.computing.co.uk/ctg/news/1849095/police-moj-staff-disciplined-social-networking-abuse [Accessed: 13 January 2010].

Available at: http://www.constitution.org/billofr_.htm [Accessed: 8 December 2010].

Available at: http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter7.htm [Accessed: 7 February 2011].

Available at: http://www.deloitte.com/dtt/cda/doc/content/us_2009_ethics_workplace_survey_150509.pdf [Accessed: 18 January 2010].

Available at: http://www.digitaltrends.com/features/the-history-of-social-networking/ [Accessed: 13 January 2011].

Available at: http://www.examiner.com/human-resources-in-jackson/free-speech-and-social-networking-sites-the-employment-issue#ixzz1Bksg1C6N [Accessed: 22 January 2011].

Available at: http://www.facebook.com/notes/labor-relations-today/nlrb-parties-settle-facebook-firing-case [Accessed: 10 February 2011].

Available at: http://www.facebook.com/terms.php [Accessed: 11 February 2011].

Available at: http://www.fxi.org.za/content/view/61/51/ [Accessed: 22 January 2011].

Available at: http://www.fxi.org.za/content/view/71/51/ [Accessed: 22 January 2011].

Available at: http://www.gadllp.co.uk/blog/?tag=vicarious-liability [Accessed: 9 February 2011].

Available at: http://www.geisinger.org/professionals/services/bioethics/b_notes/nov2009.pdf [Accessed: 21 December 2010].

Available at: http://www.guardian.co.uk/media/2007/jul/17/digitalmedia.highereducation [Accessed: 21 December 2010].

Available at: http://www.guardian.co.uk/world/2010/nov/23/ [Accessed: 7 February 2011].

Available at: http://www.hrcomplianceinsider.com/newsletter/beware-the-dangers-of-%E2%80%soc [Accessed: 24 January 2011].

Available at: http://www.hrcr.org/safrica/privacy/austr_law.html [Accessed: 24 January 2011].

Available at: http://www.hrmguide.net/canada/law/inappropriate-use.htm [Accessed: 24 January 2011].

Available at:
http://www.irnetwork.co.za/nxt/gateway.dll?f=templates$fn=default.htm$vid=irnetwork:10.1048/enu [Accessed: 1 October 2010].

Available at: http://www.itnewsafrica.com/?p=3380 [Accessed: 19 January 2010].

Available at: http://www.labournet.co.za/NewsItem.aspx?ID=339f3e63-f912-4fd6-8d76-440006ffb589 [Accessed: 14 December 2010].

Available at:
http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id
[Accessed: 7 February 2011].

Available at:
http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202431575049 [Accessed: 18 January 2010].

Available at:
http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html [Accessed: 8 December 2010].

Available at: http://www.mashable.com/2010/02/04/ [Accessed: 14 January 2010].

Available at: http://www.nationsencyclopedia.com [Accessed: 9 February 2011].

Available at: http://www.news24.com/ SouthAfrica/News/Pupil-takes-dept-to-court-20100201 [Accessed: 27 January 2011].

Available at: http://www.nytimes.com/2001/05/18/us/dismissed-for-chat-room-cia-workers-speak-out.html?pagewanted=1 [Accessed: 18 January 2010].

Available at: http://www.nzherald.co.nz/email/news/article.cfm?c_id=188&objectid=10483277 [Accessed: 18 January 2010].

Available at: http://www.nzlawyermagazine.co.za/Archives/Issue104/N3/tabid/1543/Default.aspx [Accessed: 21 December 2010].

Available at: http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm [Accessed: 18 January 2010].

Available at: http://www.privacyinternational.org/survey/phr2003/countries/canada.htm [Accessed: 24 January 2011].

Available at: http://www.privacyinternational.org/survey/phr2003/countries/newzealand.htm [Accessed: 24 January 2011].

Available at: http://www.proappoint.co.za/blog/2009/09 [Accessed: 19 January 2010].

Available at: http://www.smh.com.au/articles/2009/04/03/1238261779328.html [Accessed: 18 January 2010].

Available at: http://www.socialnetworkinglawblog.com/ [Accessed: 18 November 2010].

Available at: http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1518621 [Accessed: 8 December 2010].

Available at: http://www.walkermorris.co.uk/content.aspx?id=619 [Accessed: 9 February 2011].

Available at: http://www.workinfo.com/free/Sub_for_legres/data/Disclosure/protected.htm [Accessed: 31 January 2011].

Available at: http://www.xperthr.co.uk/faqs/topics/15,162/negative-comments-on-social-media.aspx?articleid=104600&mode=open#104600 [Accessed: 7 February 2011].

Available at: http://www.yourrights.org.uk/yourrights/privacy/ [Accessed: 24 January 2011].

Bamford & others v Energiser SA Ltd [2001] 12 BALR 1251.

Botha & Another v Creecy NO & Others [2010] JOL 251847GSJ.

Canadian Bill of Rights 1960, c. 44.

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, March 26, 2007.

Clark, D.M. *South African Law Reform Commission Issue Paper 22 Project 130: Stalking* (2003) South African Law Commission. ISBN 0-621-34410-9.

Collier, D. *Workplace Privacy in the Cyber Age* (2002) 23 *ILJ* 1743.

Constitution of the Republic of South Africa of 1996.

COSAWU obo Khumalo v Royal Ascot Superspar (2006) 27 *ILJ* 2452 (CCMA).

Dancaster, L. *Internet Abuse: A Survey of South African Companies* (2001) *ILJ* 862.

Duff, A. *Can an employer dismiss due to Facebook?* (2010) Packaging Review South Africa, Vol. 36, Issue 2.

Du Toit et al, *Labour Relations Law: A Comprehensive Guide* 5ed (2006) LexisNexis Buttorworths.

Etsebeth, V. *Information privacy protection – legal fallacy or reality?* (2007) 70(4) *THRHR* 571.

Freedom of Speech & Technology – the Reno, Multnomah & Baker case Available at: http://cs.ua.edu/340/fall10/freespeech_pta.ppt [Accessed: 22 January 2011].

Government of Alberta and Alberta Union of Provincial Employees (R. Grievance) [2008] A.G.A.A. No. 20, April 11, 2008.

Grogan, J. *Dismissal, Discrimination & Unfair Labour Practices* (2007) JUTA & Co Ltd.

Hankin, R. *Navigating the Legal Minefield of Private Investigations: A Career-Saving Guide for Private Investigators, Detectives, and Security Police* (2008) Looseleaf Law Publications.

Khan v University of KwaZulu Natal (2009) 18 CCMA 8.7.1.

Mavumengwana v Samcor Ltd (Metalloys) (1992) 1 LCD 200 (IC).

New Zealand Bill of Rights Act 1990 No.109.

McGregor, M. *The Right to Privacy in the Workplace: General Case Law and Guidelines for Using the Internet and e-Mail* (2004) *SA Mercantile Law Journal = SA Tydskrif vir Handelsreg* Vol 16(4). P638-650.

McGregor, M. *The use of email and the Internet at work* (2003) *Juta's Business Law* Vol 11(3).

Mischke, C. *Disciplinary action and the internet: Responding to employee abuse of email, network and internet access* (1999) Vol 9(5) *CLL* 41.

Mischke, C. *Dismissal for abuse of email: Arbitration award sets decisive tone on employer rights over use of email facilities* (2002) January 11(6) *CLL* 51.

Mischke, C. *The monitoring and interception of electronic communications: Obtaining and using email and other electronic evidence* (2001) May Vol. 10(10) *CLL* 91.

Modiba, M. *Intercepting and Monitoring Employees' e-Mail Communications and Internet Access* (2003) *SA Mercantile Law Journal = SA Tydskrif vir Handelsreg* Vol. 15(3). P 363-371.

Nancy Smith and Partners in Sexual Health (Non-Profit) WECT13711-10 (CCMA).

Nathaniel Arelisky and Van Wyk Da Silva Trust t/a Ocean Basket Table View WECT16930-10 (CCMA).

Ngutshane v Ariviakom (Pty) Ltd t/a Arivia.Kom (J1067/08) [2008] ZALC 159.

NUM & others v East Rand Gold & Uranium Co Ltd (1986) 7 *ILJ* 739 (IC).

Parliament of Australia Research Note. 14 March 2005, no. 37, 2004-05, ISSN 1449-8456.

Pietrylo v. Hillstone Restaurant Group, 2:06-cv-5754. Available at: http://www.employerlawreport.com/uploads/file/PIETRYLO%20v%20%2HILLSIDE%20RESTAURANT.pdf [Accessed: 18 January 2010].

Pistorius, T. *Monitoring, interception and Big Boss in the workplace: is the devil in the details?* [2009] PER 1 Available at: http://www.saflii.org/za/journals/PER/2009/1.html [Accessed: 6 January 2011].

Protecting your company's reputation Available at: http://www.personneltoday.com/articles/2008/06/20/46378/protecting-your-companys-reputation.html [Accessed: 19 January 2010].

Rycroft, A. *Bringing the Employer into Disrepute* (2008) 29 *ILJ* 1605.

Saaiman & another v de Beers Consolidated Mines (Finsch Mine) (1995) 16 *ILJ* 1551 (IC) 1562H-I.

S.D. Todd *Facebook comments: just cause for termination?* Available at: http://www.heenen.co/fr/nouvelles/pdf/Facebook_comments_just_cause_for_termination.pdf [Accessed: 24 January 2011].

Sedick & Another and Krisray (Pty) Ltd (2011) 32 *ILJ* 752 (CCMA).

Sharwood v Africa Business News Limited t/a CNBC Africa 2010 (CCMA).

Smythe v Pillsbury Co 914 F Supp 97 (ED) Pa 1996.

Social networking sites: Networking or not working? Available at: http://www.personneltoday.com/articles/2007/09/12/42102/social-networking-sites-networking-or-not-working.html [Accessed: 6 January 2011].

S v Makwanyane 1995 (6) 665 (CC) 104.

Timothy v Nampak Corrugated Containers (Pty) Ltd (DA22/08) [2010] ZALC 56 Available at: http://www.saflii.org/za/cases/ZALC/2010/56.html [Accessed: 28 January 2011].

T.S. Zurbrigg *Facebook: What Employers Need To Know About Workplace Privacy, Discipline & Dismissal* Available at: http://www.fieldlaw.com.[Accessed: 24 January 2011].

Van Niekerk et al, *Unfair Dismissal* 3ed (2006) SiberInk.

Van Wyk v Independent Newspapers Gauteng (Pty) Ltd and Others (2005) 26 *ILJ* 2433 (LC).

Van Zyl v Duhva Opencast Services (Edms) Bpk (1988) 9 *ILJ* 905 (IC).