UNIVERSITY OF KWAZULU-NATAL ™

INYUVESI YAKWAZULU-NATALI

DATA PRIVACY PROTECTION IN SOUTH AFRICA: AN ANALYSIS OF VICARIOUS LIABILITY IN LIGHT OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 ("POPIA")

A dissertation presented

by

Cammrynn-Lea Larsen

Student Number: 216 076 634

to

the College of Law and Management Studies

in partial fulfilment of the regulations

for the Master of Laws (LLM) in Business Law Degree

at the

University of KwaZulu-Natal

January 2019

Table of contents

Page No

Declaration of originality

I, Cammrynn-Lea Larsen, declare that:

i. The research report in this dissertation, except where otherwise indicated, is my original work.

ii. This dissertation has not been submitted for any degree or examination at any other university.

iii. This dissertation does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

iv. This dissertation does not contain other persons' writing, unless specifically acknowledged as being sourced have been quoted, then:

a) their words have been re-written but the general information attributed to them has been referenced;

b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

v. Where I have reproduced a publication of which I am author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

vi. This dissertation does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation and in the references section.

vii. This project is an original piece of work which is made available for photocopying and for inter-library loan.

CAMMRYNN-LEA LARSEN
216076634

Acknowledgement

First and foremost I wish to thank my supervisor, Mr Lee Swales, for his patience, motivation, sound advice, and extensive academic support. Lee's immense knowledge and guidance proved invaluable during the preparation and completion of this study.

I express my very profound gratitude to my parents who have been stable, loving presences, supporting and guiding me through my trials and tribulations and sharing in my triumphs. Thank you for providing me with continuous encouragement and inspiration throughout my years of study and through the process of undertaking this study.

A special thank you to my father, Christian, whose strong work ethic has taught me that getting what you desire in life means working hard for it and earning it.

Lastly, and most importantly, I wish to thank my husband, Zane, whose unconditional love and unfailing support has been my guiding light during this study. Thank you for putting your life on hold so I could achieve my goal. I am truly blessed to have you in my life.

Chapter 1: Introduction and overview

1.1 Introduction

Privacy is a right that is protected in terms of the common law and s 14 of Chapter 2[1] of the Constitution.[2] The Constitution recognises the right to privacy as an intrinsic and fundamental human right. This provides an indication of its importance.[3]

The right to privacy as enshrined in the Constitution[4] includes 'informational privacy',[5] which can be described as a person's right to control and decide when, how, and under what circumstances their personal information may be disclosed to the public.[6] Data protection is an important aspect of safeguarding a person's right to privacy.[7]

The common law right to privacy in South Africa was recognised in the case of *O'Keefe v Argus Printing*[8] wherein the court held that the right to dignity includes the right to privacy.[9] This was the first time that South African courts recognised the right to privacy as an independent personality right. The Constitutional Court in *Bernstein & others v Bester*[10] later endorsed this recognition and Ackerman J held that privacy relates only to a person's truly personal aspects and not to every aspect within his or her personal knowledge and experience.[11]

The judgment in *Bernstein* faced criticism from academics in South Africa. Neethling[12] argues that the restrictive interpretation of privacy by Ackerman J fails to take into

[1] Chapter 2 of the Constitution contains the Bill of Rights.
[2] Constitution of the Republic of South Africa, 1996 ("Constitution").
[3] South African Law Reform Commission Discussion Paper 109 (Project 124) *Privacy and data protection* (2005) 16.
[4] Section 14(d) of the Constitution provides that *'everyone has the right to privacy, which includes the right not to have the privacy of their communications infringed.'*
[5] I Currie & J D De Waal *The Bill of Rights handbook* 6 ed (2013) 302.
[6] *National Media Ltd v Jooste* [1996] 2 All SA 510 (A).
[7] J Neethling, JM Potgieter & PJ Visser *Neethling's Law of Personality* 2 ed (2005) 29.
[8] *O'Keeffe v Argus Printing and Publishing Co Ltd* [1954] 3 All SA 159 (C) ("*O'Keefe v Argus Printing"*).
[9] *O'Keeffe v Argus Printing and Publishing Co Ltd* [1954] 3 All SA 159 (C) at 248 – 249.
[10] *Bernstein & others v Bester & others NNO* 1996 (2) SA 751 (CC) ("*Bernstein*")
[11] *Bernstein & others v Bester & others NNO* 1996 (2) SA 751 (CC) at paragraph 79.
[12] J Neethling 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 18 - 28.

consideration other private facts of a person that are worthy of protection.[13] A wider approach is necessary in regard to data protection due to the fact that small amounts of data may not be regarded as private in terms of the approach followed in *Bernstein*, but the accumulation of the small amounts of data may be of such a nature that the person may want to keep it private.[14]

Neethling provides a convincing criticism of the right to privacy as interpreted in the *Bernstein* case, which forms a powerful argument in favour of conceptual clarity on the nature of privacy in South Africa in order to enhance the protection of privacy.

With the rapid rate of technological advancement of modern society there is a necessity to mitigate the potential threat to privacy by adopting legislation to protect personal information. Whilst it is accurate to state that the Constitution and the common law provide for the protection of privacy and a basis for data protection, there is an imperative need for the more precise regulation of a data protection regime, in harmony with international standards that seek to develop legislation in line with the vast technological advancements of the digital age, in order to properly give effect to the fundamental right to privacy.[15]

The necessity to bring South African data protection legislation in line with international trends is rooted in the desire to promote social and economic development.[16] In order to attract foreign investment it will be vital to ensure that adequate data protection legislation is enacted and strictly enforced.[17] A majority of foreign investors are reliant on data and these investors require the comfort of knowing that the processing of their data is regulated and therefore protected so as to deter any unlawful dissemination of their data.

In an attempt to bring South Africa in line with international prescripts the South

[13] J Neethling 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 20.
[14] J Neethling 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 20.
[15] Preamble to POPIA. See also A Roos 'Data Protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 400.
[16] South African Law Reform Commission Discussion Paper 109 (Project 124) *Privacy and data protection* (2005) 40.
[17] R Luck 'POPI – Is South Africa keeping up with international trends' (2014) May *De Rebus* 46. See also A Roos 'Core principles of data protection law' (2006) 39(1) *CILSA* 104.

African Law Reform Commission ("SALRC") published a Discussion Paper[18] ("SALRC Discussion Paper") on privacy and data protection in which it recommended that formal legislation on the protection of personal information be enacted in order to safeguard the right to privacy. The SALRC Discussion Paper contained proposed draft legislation that was ultimately signed into law on 19 November 2013 and known as the Protection of Personal Information Act 4 of 2013 ("POPIA").

POPIA aims to give effect to the Constitutional right to privacy by regulating the processing[19] of personal information[20] by public and private bodies.[21] At present, the majority of the provisions of POPIA are yet to commence[22] therefore the right to privacy is currently regulated in terms of the common law and the Constitution, and the remedies available to a person whose privacy has been infringed include common law remedies[23] and delictual remedies.

---

[18] South African Law Reform Commission Discussion Paper 109 (Project 124) *Privacy and data protection* (2005). See also A Roos 'Data Protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 433.

[19] In terms of s 1 of POPIA *'processing'* is defined as *'any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.'*

[20] In terms of s 1 of POPIA *'personal information'* means *'information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to -*
(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
(b) information relating to the education or the medical, financial, criminal or employment history of the person;
(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;'

[21] Preamble to POPIA.

[22] The sections that have come into operation at this time include: s 1 which contains the definitions; Part A of Chapter 5 which establishes the Information Regulator; s 112 which contains the Regulations and s 113 which sets out the procedure for making regulations.

[23] The accepted remedies for common law invasions of privacy include the actio iniuriarum, the actio legis Aquiliae and the interdict.

One of the sections of POPIA[24] that have come into operation is s 39 which provides for the establishment of an impartial and independent body known as the Information Regulator to exercise certain powers and to perform certain duties and functions in terms of POPIA.[25] The Information Regulator has jurisdiction throughout the Republic of South Africa, is accountable to the National Assembly, and is subject only to the Constitution.[26] The Information Regulator was established on 1 December 2016 and is tasked with *inter alia* monitoring and enforcing compliance by public and private bodies with the provisions of POPIA, and the Promotion of Access to Information Act 2 of 2000.[27]

In circumstances where an individual commits a privacy breach by unlawfully distributing the personal information of a third party, in terms of the common law, the third party can only claim against the individual if the third party can prove a wilful or negligent wrongful act or omission on the part of the individual that is causally linked to the damaged suffered.[28] However, a recent trend is for a party who suffers damage to base their claim against the employer of an individual if such wrong was committed by the individual in the course and scope of his or her employment.[29] This allows the injured party to expand liability and sue an employer who is likely in a stronger financial position than an employee.[30]

It is a well-established legal principle[31] that employers are vicariously liable for the negligent acts or omissions by their employees.[32] This is a form of strict liability, which consists of liability in the absence of fault. South African courts have accepted that the establishment of vicarious liability requires that an employee must commit a wrongful

[24] See note 22 above for list of sections that have commenced. See 'POPI commencement date or POPI effective date starts the clock' *Michalsons* 10 July 2018 available at *https://www.michalsons.com/blog/popi-commencement-date-popi-effective-date/13109,* accessed on 4 September 2018.
[25] Preamble to POPIA.
[26] Sections 39(a), 39(b) and 39(d) of POPIA.
[27] Section 40(1)(b) of POPIA.
[28] J Neethling, JM Potgieter & PJ Visser *Neethling Potgieter Visser Law of Delict* 7th ed (2015) 389.
[29] Or while engaged in any activity incidental thereto in terms of vicarious liability.
[30] J M Potgieter 'Preliminary thoughts on whether vicarious liability should be extended to the parent-child relationship' (2011) 32 *Obiter* 194.
[31] See *Minister of Safety and Security v Morudu and Others* 2016 (1) SACR 68 (SCA) where the Supreme Court of Appeal found that the doctrine of vicarious liability is deeply rooted in the South African legal system. In relying on the dictum in the case of *F v Minister of Safety and Security [2011] ZACC 37; 2012 (1) SA 536 (CC),* the Supreme Court of Appeal reiterated that *'employees are extensions of their employers.'*
[32] *Messina Associated Carriers v Kleinhaus* 2001 (3) SA 868 (SCA) at 872F-I.

act; an employer-employee relationship must exist at the time when the wrongful act is committed; and the employee must have committed the wrongful act in the course and scope of his or her employment.[33]

The injured party need not prove that the employer acted wilfully or negligently due to the fact that the rationale for vicarious liability is not based on the employer's fault, but on the employee's fault.[34] The criminal action of an employee in disclosing the personal information of a third party is beyond the scope of this dissertation.[35]

Section 99(1) of POPIA creates a form of statutory vicarious liability in that it provides that a data subject[36] has the right to institute a civil action for damages against a responsible party[37] in circumstances where the data subject's privacy has been infringed, irrespective of whether or not such infringement occurred as a result of intent or negligence.[38] An employer will be regarded as a responsible party in terms of POPIA in that it determines the purpose of and means for processing personal information.[39] Dillard and Bascerano[40] assert that *'the responsible party to whom POPIA refers will be an employer, since it is usually the employer who determines the reason for the processing of personal information.'*[41]

An employer is therefore liable if one of its employees contravenes POPIA by infringing on another person's privacy, irrespective of whether or not such infringement

[33] B E Loots 'Sexual harassment and vicarious liability: a warning to political parties' (2008) 19 *SLR* 149.
[34] J M Potgieter 'Preliminary thoughts on whether vicarious liability should be extended to the parent-child relationship' (2011) 32 *Obiter* 189. See also K Calitz 'The close connection test for vicarious liability' (2007) 18(3) *SLR* 458.
[35] See JLJ Edwards 'Vicarious liability in criminal law' (1951) 14(3) *The Modern Law Review* 334 – 340 for an expansion on this area.
[36] In terms of s 1 of POPIA *'data subject'* is defined as *'the person to whom personal information relates.'*
[37] In terms of s 1 of POPIA *'responsible person'* is defined as *'a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.'*
[38] In terms of s 99(1) the data subject, or the Regulator at the request of the data subject, may institute a civil action for damages.
[39] J van Wyk & A Van Heerden 'The Protection of Personal Information Bill from an employment perspective' (17 September 2013) *Polity.org.za* available at *http://www.polity.org.za/article/the-protection-of-personal-information-bill-from-an-employment-perspective-2013-09-17,* accessed on 4 September 2018.
[40] D Millard & E.G. Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19 *PELJ a*vailable at *http://www.scielo.org.za/pdf/pelj/v19n1/21.pdf*, accessed 21 April 2018 ("Dillard and Bascerano").
[41] D Millard & E.G. Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19 *PELJ* at 9 *a*vailable at *http://www.scielo.org.za/pdf/pelj/v19n1/21.pdf*, accessed 21 April 2018.

occurred as a result of intent or negligence.[42]

Section 99(2) of POPIA provides for the defences available to an employer against an action for damages in the event of a breach of the provisions of POPIA. The defences available to an employer include *vis major;*[43] consent of the plaintiff; fault on the part of the plaintiff; compliance was not reasonably practicable in the circumstances; and the Regulator has granted an exemption in terms of section 37 of POPIA.[44]

Currently in South Africa, due to the fact that data protection legislation essentially only exists in theory,[45] an injured party can claim against an employer in terms of the common law doctrine of vicarious liability. When practically implemented however, POPIA can have a detrimental affect on employers in that, in its attempt to strike a balance between the rights of employers and those of its employees, it imposes onerous obligations on an employer that can result in dire consequences if not implemented.

---

[42] D Millard & E.G. Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19 *PELJ* at 23 *a*vailable at *http://www.scielo.org.za/pdf/pelj/v19n1/21.pdf*, accessed 21 April 2018.

[43] Denotes a greater or superior force for which no one is responsible. Often referred to as an act of God.

[44] Section 37 of POPIA reads as follows:

'Regulator may exempt processing of personal information

37. *(1) The Regulator may, by notice in the Gazette, grant an exemption to a responsible party to process personal information, even if that processing is in breach of a condition for the processing of such information, or any measure that gives effect to such condition, if the Regulator is satisfied that, in the circumstances of the case -*

(a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or

(b) the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.

(2) The public interest referred to in subsection (1) includes—

(a) the interests of national security;

(b) the prevention, detection and prosecution of offences;

(c) important economic and financial interests of a public body;

(d) fostering compliance with legal provisions established in the interests referred to under paragraphs (b) and (c);

(e) historical, statistical or research activity; or

(f) the special importance of the interest in freedom of expression.

(3) The Regulator may impose reasonable conditions in respect of any exemption granted under subsection (1).'

[45] The sections of POPIA that have yet to commence are anticipated to commence towards the end of 2018 alternatively in 2019. See 'POPI commencement date or POPI effective date starts the clock' *Michalsons* 10 July 2018 available at *https://www.michalsons.com/blog/popi-commencement-date-popi-effective-date/13109,* accessed on 4 September 2018.

1.2 **Statement of purpose**

The purpose of this dissertation is to examine POPIA, with particular focus on section 99, and to critically consider the impact of s 99 on an employer in circumstances where an employee breaches the provisions of POPIA.

The statutory vicarious liability as created in s 99 of POPIA is in contrast to the common law doctrine of vicarious liability and the statutory vicarious liability created in terms of other South African legislation such as the Employment Equity Act No. 55 of 1998 ("Employment Equity Act"), which are more lenient on the employer and provide for adequate means[46] for an employer to escape liability.[47]

Section 99(1) of POPIA provides that a civil action for damages may be instituted against an employer, as the responsible party, whether or not there is intent or negligence on the part of the employer. This section is onerous and harsh on an employer in that it ultimately provides that the employer is obliged to ensure that its employees comply with the provisions of POPIA and should its employees breach the provisions of POPIA, the employer will be held accountable regardless of whether or not there is intent or negligence on the part of the employer.[48] Accordingly, an employer who encourages compliance with the provisions of POPIA and who actively takes all necessary steps and precautions in order to avoid any contraventions may be accountable and liable.

Furthermore the defences available to an employer resisting a civil action for damages based on vicarious liability as contained in terms of s 99(2) of POPIA are limited.[49]

---

[46] Section 60(4) of the Employment Equity Act provides that an employer will not be held liable for the conduct of an employee if that employer is able to prove that it did all that was reasonably practicable to ensure that the employee would not act in contravention the Employment Equity Act. POPIA does not provide a similar mechanism for an employer to escape liability.

[47] D Millard & E.G. Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19 *PELJ* at 4 *a*vailable at *http://www.scielo.org.za/pdf/pelj/v19n1/21.pdf*, accessed 21 April 2018.

[48] D Millard & E.G. Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19 *PELJ* at 23 *a*vailable at *http://www.scielo.org.za/pdf/pelj/v19n1/21.pdf*, accessed 21 April 2018.

[49] D Millard & E.G. Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19 *PELJ* at 4 *a*vailable at *http://www.scielo.org.za/pdf/pelj/v19n1/21.pdf*, accessed 21 April 2018.

Section 60[50] of the Employment Equity Act provides that should employees contravene any provision of the Employment Equity Act, whilst performing their duties at work, the employer will be liable unless the employer can prove that it did everything necessary to prevent the unsought conduct.

An employer can escape liability and avoid being held vicariously liable for the contraventions of the Employment Equity Act by its employees in terms of s 60(4) of the Employment Equity Act if the employer can prove that it did all that was reasonably practicable to ensure that employees would not contravene the Employment Equity Act. POPIA does not provide for such defence and as stated by Dillard and Bascerano, *'undeniably, the law-abiding employer's good deeds will not constitute an acceptable defence against retribution in terms of POPI.'*[51]

This dissertation will explore the ways in which statutory vicarious liability as provided for in terms of s 99 of POPIA can be extended and the wording thereof modified in order to provide for suitable mechanisms and defenses for an employer to adequately escape liability.

1.3 **Rationale**

With the development of the digital age technology has become more prevalent and has provided a means to readily access and transfer personal data swiftly. The rapid technological advances are increasing the ability to accumulate, store, process and

[50] Section 60 of the Employment Equity Act provides:
'Liability of employers
60.(1) If it is alleged that an employee, while at work, contravened a provision of this Act, or engaged in conduct that, if engaged in by that employee's employer, would constitute a contravention of a provision of this Act, the alleged conduct must immediately be brought to the attention of the employer.
(2) The employer must consult all relevant parties and must take the necessary steps to eliminate the alleged conduct and comply with the provisions of this Act.
(3) If the employer fails to take the necessary steps referred to in subsection 2, and it is proved that the employee has contravened the relevant provision, the employer must be deemed also to have contravened that provision.
(4) Despite subsection (3), an employer is not liable for the conduct of an employee if that employer is able to prove that it did all that was reasonably practicable to ensure that the employee would not act in contravention of this Act.'
[51] D Millard & E.G. Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19 *PELJ* at 31 *a*vailable at *http://www.scielo.org.za/pdf/pelj/v19n1/21.pdf*, accessed 21 April 2018.

disseminate personal data. The misuse of personal data can constitute an infringement of an individual's right to privacy.

Privacy consists of a state of being free from public attention and can be described as existing in an individual's truly private realm. When an individual departs from the inner sanctum of the private realm and interacts in the public realm the more challenging it is from the individual's privacy to be protected.[52]

The lack of regulation and data principles enables personal information to be readily accessible by anyone in the public domain, which in turn can be disseminated and exploited worldwide to multiple parties.

It is therefore essential that the right to privacy and personal information is regulated and that such legal framework be constantly reassessed by the courts in light of changes in technology.

Due to the fact that data protection in South Africa is a relatively new concept and POPIA is a newly promulgated piece of legislation there is currently no legal precedent in respect of its practical application. There is a wide range of scholarly writing on the topic of POPIA, however these writings merely provide views and opinions of others and do not provide a sound illustration and understanding of how POPIA will be applied.

This dissertation will therefore aim to contribute to the dialogue and interpretation of POPIA in its application with particular focus on s 99.

1.4 **Research questions**

a. How is the right to privacy currently regulated in South Africa?

b. What is vicarious liability and how is this concept currently regulated in South

[52] R Davey and L Dahms-Jansen *Social Media in the Workplace* (2017) 40.

Africa?

c. How will POPIA impact on vicarious liability in South Africa?

d. What are the potential difficulties that will arise as a result of POPIA with regard to vicarious liability?

e. What is the position in Canada and the United Kingdom with regard to vicarious liability in respect of privacy breaches and can South Africa derive any beneficial measures from these foreign jurisdictions?

f. Does s 99 of POPIA create a form of statutory vicarious liability, and if so, how can this section be extended and modified in order to provide for suitable mechanisms and defenses for an employer to adequately escape liability?

1.5 Research methodology

A desktop research methodology is this study's primary research approach. The reason that this approach is preferred is that it involves a review and analysis of statute, case law and literature in respect of privacy, data protection and the doctrine of vicarious liability. This desk study will aim to answer the research questions by gathering and analysing sources that are existing and available in print or electronic format.

The Internet will primarily be utilised to aid this research and create an electronic data collection of primary and secondary sources using electronic search engines such as LexisNexis, Sabinet, Juta and HeinOnline.

POPIA will be the primary piece of legislation examined in this dissertation as it regulates data protection in South Africa.

Secondary sources such as academic writings, published textbooks, journal articles and online academic research papers will be utilised to examine the strengths and weaknesses of POPIA in order to amplify the outcome and recommendations suggested

in this study.

In addition, this study will also contain traces of comparative research in terms of which data protection and privacy laws in South Africa will be compared to that of foreign law. This is necessary due to the fact that data protection is a relatively new concept in South Africa and therefore it is necessary to draw inferences from foreign law and the inefficiencies in respect thereof.

1.6 Structure of research project

This research project consists of five chapters.

Chapter one provides an overview and introduction to the topic. It describes the purpose of the study, the rationale, the research questions and the research methodology approach to be applied in answering the research questions. Chapter one further provides a literature review evaluating the current knowledge on the topic. Essentially this research proposal will form chapter one of the research project.

Chapter two provides an analysis of the right to privacy in South Africa. This chapter examines the common law right to privacy as well as the constitutional right to privacy.

Chapter three provides an in-depth examination of the doctrine of vicarious liability. This chapter focuses on the doctrine of vicarious liability under the common law and the concept of statutory vicarious liability in terms of POPIA. This chapter considers the possible implications posed on an employer in respect of the civil remedies contained in s 99 of POPIA. The legal uncertainty provided for in s 99 is explored and discussed.

Having analysed the concept of vicarious liability, chapter four then explores foreign approaches with regard to vicarious liability in respect of privacy breaches. The Personal Information Protection and Electronic Documents Act, S.C. 2000, ch. 5 in Canada, the Data Protection Act 2018 in the United Kingdom and the EU's General Data Protection Regulation (EU) 2016/679 will be explored. The approaches of Canada

and the United Kingdom will be analysed in detail and possible modifications to POPIA in light of the approaches of Canada and the United Kingdom will be discussed.

Chapter five sets out the conclusions of the dissertation and provides recommendations for the way forward by drawing and deriving measures from those adopted by foreign jurisdictions.

Chapter 2: An analysis of the right to privacy in South Africa

2.1 Introduction

> *'Privacy, like an elephant, is more readily recognised than described.'*[53]

The concept of privacy is difficult to articulate due to the fact that it *'means different things to different people.'*[54] Individuals have different privacy needs and this makes it difficult to provide a constructive conception of privacy.[55] According to sociologists and psychologists a person has a fundamental need for privacy.[56]

The absence of a particular definition of privacy does not render it of any less importance than other personality rights, however, conceptual clarity on the nature of privacy in South Africa is necessary in order to enhance the protection of privacy.[57] As Gross[58] accurately stated: -

> *'our ability to articulate and apply principles of legal protection diminishes, for we become uncertain about precisely what it is that compels us toward protective measures and wherein it differs from what has already been recognized or refused recognition under established legal theory.'*[59]

In the early nineteen hundreds the Transvaal Supreme Court in *R v Umfaan*[60] described the right to privacy as a personality right, which encompasses *'those real rights, those rights in rem related to personality, which every free man is entitled to enjoy.'*[61]

---

[53] J B Young *Privacy* (1978) 5.
[54] A Roos 'Data Privacy Law' in D P van der Merwe… et al (2ed) *Information and Communications Technology Law* (2016) 370.
[55] See *Bernstein & others v Bester & others NNO* 1996 (2) SA 751 (CC) *National Media Ltd v Jooste* 1996 (3) SA 262 (A) at 787 – 788 wherein Ackerman J stated *'The concept of privacy is an amorphous and elusive one which has been the subject of much scholarly debate.'*
[56] J Neethling, JM Potgieter & PJ Visser *Neethling's Law of Personality* 2 ed (2005) 29.
[57] J Neethling 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 27 - 28
[58] H Gross 'The concept of privacy' (1967) *New York University Law Review* at 34 – 54.
[59] H Gross 'The concept of privacy' (1967) *New York University Law Review* at 34.
[60] *R v Umfaan* 1908 TS 62 ("*R v Umfaan")*.
[61] *R v Umfaan* 1908 TS 62 at 66 – 67.

Neethling[62] describes privacy as:

> *'...a condition of human life characterized by seclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has himself determined to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private.'*[63]

Roos[64] extends on this description of privacy provided by Neethling and states: -

> *'In other words, the essence of an individual's interest in privacy is his or her power of self-determination over the scope of the information to be excluded from the knowledge of others. Therefore a person's right to privacy entails that he or she should have control over his or her personal information.'*[65]

In *Bernstein & others v Bester & others NNO*[66] Ackerman J stated that privacy relates only to a person's truly personal aspects and not to every aspect within his/her personal knowledge and experience.[67] The judgment in *Bernstein* has faced severe criticism in South Africa. Neethling,[68] for example, argues that the restrictive interpretation of privacy fails to take into consideration other private facts of a person that are worthy of protection.[69]

In *Investigating Directorate Serious Economic Offences and others v Hyundai Motor Distributors (Pty) Ltd and others: In re Hyundai Motor Distributors (Pty) Ltd and others v Smit NO and others*[70] the Constitutional Court validated the views expressed by Neethling in criticising the approach of the court in *Bernstein* and deciding that the

---

[62] J Neethling 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 18 – 28.
[63] J Neethling 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 19.
[64] A Roos 'Data Protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ.*
[65] A Roos 'Data Protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 421 – 422.
[66] *Bernstein & others v Bester & others NNO* 1996 (2) SA 751 (CC) ("*Bernstein*").
[67] *Bernstein & others v Bester & others NNO* 1996 (2) SA 751 (CC); *National Media Ltd v Jooste* 1996 (3) SA 262 (A) at 79.
[68] J Neethling 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 18 - 28.
[69] J Neethling 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 20.
[70] *Investigating Directorate: Serious Economic Offences and others v Hyundai Motor Distributors (Pty) Ltd and others: In re Hyundai Motor Distributors (Pty) Ltd and others v Smit NO and others* 2001 (1) SA 545 (CC) ("*Investigating Directorate*").

Constitutional right to privacy *'does not relate solely to the individual within his or her private space'*[71] Further, the Constitutional Court further confirmed that the right to privacy is relevant when a person has the ability to decide what he or she wants to disclose to the public and the expectation that the person's decision will be respected is reasonable.[72]

Neethling provides a convincing criticism of the right to privacy as interpreted in *Bernstein,* which forms a powerful argument in favour of conceptual clarity on the nature of privacy in South Africa in order to enhance the protection of privacy. Neethling goes on to state that *'the concept of privacy should be sought in and defined in accordance with its existence and nature in factual reality.'*[73] Neethling further provides a valid critique of the tendency of the courts in South Africa to overlook other private facts relating to a person that are worthy of protection such as physical-psychological integrity, dignity, identity, autonomy, self-realisation and patrimonial interests.

Neethling states that the *'constitutional concept of privacy is, on the face of it at least, also concerned with what can briefly be described as informational privacy.'* Roos goes on to state that:

> *'the development and growth of telecommunications technology, connecting computers in networks (principally the Internet) and enabling the transmission of information between computer systems, has further lent impetus to the processing of personal information.'*[74]

A wider approach is necessary in regard to data protection due to the fact that small amounts of data may not be regarded as private in terms of the approach followed in *Bernstein*, but the accumulation of the small amounts of data may be of such a nature

[71] *Investigating Directorate: Serious Economic Offences and others v Hyundai Motor Distributors (Pty) Ltd and others: In re Hyundai Motor Distributors (Pty) Ltd and others v Smit NO and others* 2001 (1) SA 545 (CC) at 16.
[72] *Investigating Directorate: Serious Economic Offences and others v Hyundai Motor Distributors (Pty) Ltd and others: In re Hyundai Motor Distributors (Pty) Ltd and others v Smit NO and others* 2001 (1) SA 545 (CC) at 36.
[73] J Neethling 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 19.
[74] A Roos 'Data privacy law' in Van der Merwe, DP. … et al. *Information and Communications Technology Law* 2 ed (2016) 363.

that the person may want to keep it private.[75]

The SALRC Discussion Paper on privacy and data protection stated:

> '*Privacy is a valuable aspect of personality. Data or information protection forms an element of safeguarding a person's right to privacy.*'[76]

As individuals connect on social media, privacy becomes a significant area of concern. Social media has altered the way in which individuals interact with one another. It follows that technological innovation provides a threat to privacy in that it allows for personal information to be effortlessly processed and disseminated within seconds to a wide-reaching number of people.

The court in *H v W*[77] accurately held:

> *'It is in respect of the remedy where infringements of privacy take place in the social media that the common law needs to develop….The law has to take into account changing realities not only technologically but also socially or else it will lose credibility in the eyes of the people. Without credibility, law loses legitimacy. If law loses legitimacy, it loses acceptance. If it loses acceptance, it loses obedience. It is imperative that the courts respond appropriately to changing times, acting cautiously and with wisdom.'*[78]

The right to privacy in South Africa is protected in terms of the common law and the Constitution.[79] Prior to 1994[80] the right to privacy was protected under the common law only.

---

[75] J Neethling 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 20.
[76] SALRC Discussion Paper at iv.
[77] *H v W* [2013] 2 All SA 218 (GSJ) at 31.
[78] *H v W* [2013] 2 All SA 218 (GSJ) at 31.
[79] Section 14 of the Constitution of the Republic of South Africa, 1996.
[80] The Interim Constitution of the Republic of South Africa, 1993 ("the Interim Constitution") came into force on 27 April 1994. Section 13 of the Interim Constitution is the forerunner of s 14 of the Constitution which provides for the right to privacy as a fundamental human right. For more, see *Minister of Justice and Constitutional Development and Others v Prince (Clarke and Others Intervening); National Director of Public Prosecutions and Others v Rubin; National Director of Public Prosecutions and Others v Acton* (CCT108/17) [2018] ZACC 30.

In order to examine the right to privacy it is necessary to analysis the right to privacy under the common law and the Constitution. This chapter sets out to provide an understanding of the extent of the right to privacy as currently provided for in South Africa. Furthermore this chapter touches on the right to privacy in terms of POPIA and why the full promulgation of POPIA is crucial in light of the fact that the right to privacy is protected by the common law and the Constitution.

2.2 **The common law right to privacy**

2.2.1 **Definition and recognition**

The common law provides for personality rights, which includes a person's right to dignity, freedom, physical integrity, privacy and reputation.[81] The common law right to privacy is protected by the common law principles of the law of delict.[82]

The court in *O'Keefe v Argus Printing* held that the right to dignity includes the right to privacy thereby recognising the right to privacy as an independent personality right. This case was the locus classicus for the recognition of an independent right to privacy in South African law wherein Watermeyer AJ interpreted dignitas more broadly to include all personality rights and interests (with the exception of the right to a good name and bodily integrity).

The Constitutional Court in *Bernstein* later endorsed this recognition and held that the right to privacy *'relates only to the most personal aspects of a persons existence, and not to every aspect within his/her personal knowledge and experience.'*[83]

In *Jansen Van Vuuren NNO v Kruger*[84] the court held that:

> *'The actio iniuriarum protects a person's dignitas and dignitas embraces privacy . . .*

[81] J Neethling & JM Potgieter & PJ Visser *Neethling's Law of Personality* 2 ed (2005) at 51.
[82] A Roos 'Data Protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 422.
[83] *Bernstein & others v Bester & others NNO* 1996 (2) SA 751 (CC) at 79.
[84] *Jansen Van Vuuren NNO v Kruger* 1993 (4) SA 842 (A) ("*Jansen van Vuuren NNO v Kruger*").

Although the right to privacy has on occasion been referred to as a real right or ius in rem . . . it is better described as a right of personality.'[85]

It follows and has been accepted by the SALRC that:

'...despite the decisions equating privacy with dignity (or honour), it can safely be accepted that nowadays the right to privacy is recognised by the common law as an independent right of personality and that it has been delimited as such within the dignitas concept.'[86]

As stated in *Carmichele v Minister of Safety and Security and Another (Centre for Applied Legal Studies Intervening)* [87] there is a general obligation placed on the courts to develop the common law in accordance with the spirit, objects and purport of the Bill of Rights.[88] Ackermann and Goldstone JJ held:

'It needs to be stressed that the obligation of courts to develop the common law, in the context of the section 39(2) objectives, is not purely discretionary. On the contrary, it is implicit in section 39(2) read with section 173 that where the common law as it stands is deficient in promoting the section 39(2) objectives, the courts are under a general obligation to develop it appropriately. We say a 'general obligation' because we do not mean to suggest that a court must, in each and every case where the common law is involved, embark on an independent exercise as to whether the common law is in need of development and, if so, how it is to be developed under section 39(2). At the same time there might be circumstances where a court is obliged to raise the matter on its own and require full argument from the parties.'[89]

It has been accepted by the Constitutional Court that whilst the primary vehicle for law reform in South Africa should be the legislature, South African courts are under a general obligation to develop the common law when it deviates from the spirit, purport and objects of the Bill of Rights.

[85] *Jansen Van Vuuren NNO v Kruger* 1993 (4) SA 842 (A) at 849.
[86] South African Law Reform Commission Discussion Paper 109 (Project 124) *Privacy and data protection* (2005) 9.
[87] *Carmichele v Minister of Safety and Security and Another (Centre for Applied Legal Studies Intervening)* 2001 (4) SA 938 (CC) at 39.
[88] See also South African Law Reform Commission Discussion Paper 109 (Project 124) *Privacy and data protection* (2005) 5.
[89] *Carmichele v Minister of Safety and Security and Another* 2001 (4) SA 938 (CC) at 39.

2.2.2 Common law remedies for infringement of privacy

An infringement of privacy occurs where an individual intentionally and wrongfully interferes with another's right to seclusion in his or her private life.[90] In order to prove a claim for the invasion of privacy a plaintiff will have to show that there has been an unlawful and international infringement of the person's right to privacy.[91]

The elements of an infringement of privacy that have to be alleged and proved by a plaintiff include: -

1. an invasion of privacy;

2. wrongfulness; and

3. fault in the form of intention or negligence.[92]

The remedies available to an individual whose privacy has been infringed include common law remedies and delictual remedies. The accepted remedies for common law invasions of privacy include the *actio iniuriarum*, the *actio legis Aquiliae* and an interdict.

The most well known common law remedy is the *actio iniuriarium*, which is directed at providing satisfaction for non-patrimonial loss in the form of injury to personality. The *actio iniuriarum* is therefore used to claim satisfaction for the wrongful interference with the right to privacy. In order for an individual to succeed, she will need to allege and prove that the infringement of privacy was intentional and wrongful.[93]

The *actio legis Aquiliae* is a remedy available to a plaintiff to claim patrimonial loss

[90] Woolman and Bishop *Constitutional Law* 3.
[91] D McQuoid-Mason 'Invasion of privacy: Common law v. Constitutional delict – does it make a difference?' (2000) *Acta Juridica* 228.
[92] D McQuoid-Mason 'Invasion of privacy: Common law v. Constitutional delict – does it make a difference?' (2000) *Acta Juridica* 229.
[93] *Jansen van Vuuren and another NNO v Kruger* [1993] 2 All SA 619 (A) at 10.

sustained as a result of the wrongful, negligent processing of personal information and thereby breaching the plaintiff's right to privacy. Unlike the *actio iniuriarium* the *actio legis Aquiliae* is used where direct patrimonial loss has been sustained intentionally or negligently.

A plaintiff can apply to the court for an interdict in order to prevent and stop the invasion of his or her privacy from occurring or to prohibit the invasion from recurring. A plaintiff may seek an interdict in order to enforce a right. A plaintiff may apply for an interdict and proceed with a separate damages claim.[94]

A plaintiff will be granted an interim interdict if he or she can prove:

1. a prima facie right;

2. a reasonable apprehension of irreparable harm if the interim relief is not granted;

3. the balance of convenience favours the granting of the interim interdict; and

4. the plaintiff has no other satisfactory remedy.[95]

In order to obtain a final interdict the plaintiff will have to prove: -

1. he or she has a clear right;

2. has suffered actual injury or has a reasonable apprehension of irreparable injury;

3. no other satisfactory remedy is available.[96]

[94] *Rhodesian Printing and Publishing Co Ltd v Duggan and another* [1975] 2 All SA 125 (RA).
[95] McQuoid-Mason 'Invasion of privacy: Common law v. Constitutional delict – does it make a difference?' (2000) *Acta Juridica* 236.

2.3 **The constitutional right to privacy**

Sachs J in *Mistry v Interim National Medical and Dental Council*[97] accurately stated the following:

> *'...Generations of systematised and egregious violations of personal privacy established norms of disrespect for citizens that seeped generally into the public administration and promoted amongst a great many officials habits and practices inconsistent with the standards of conduct now required by the Bill of Rights. [The right to privacy] accordingly requires us to repudiate the past practices that were repugnant to the new constitutional values, while at the same time re-affirming and building on those that were consistent with these values.'*[98]

It is trite that the Constitution is the supreme law and any law that is inconsistent with any provision in respect thereof is invalid.[99] Privacy is not an absolute right under common law or the Constitution and accordingly it may be limited in certain circumstances.[100]

Chapter 2 of the Constitution sets out the Bill of Rights which '*is a cornerstone of democracy in South Africa. It enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom.*'[101] According to s 8(1) of Chapter 2 of the Constitution the rights enshrined in the Bill of Rights are binding on the executive, the legislature, the judiciary and all organs of state. Section 8(4) of Chapter 2 of the Constitution provides that:

> *'(4) A juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of that juristic person.'*

---

[96] McQuoid-Mason 'Invasion of privacy: Common law v. Constitutional delict – does it make a difference?' (2000) *Acta Juridica* 235 - 236.
[97] *Mistry v Interim National Medical and Dental Council and Others* [1998] ZACC 10.
[98] *Mistry v Interim National Medical and Dental Council and Others* [1998] ZACC 10 at 25.
[99] Section 172(1)(a) of the Constitution.
[100] Section 7(3) of Chapter 2 of the Constitution provides that *'The rights in the Bill of Rights are subject to the limitations contained or referred to in section 36, or elsewhere in the Bill.'*
[101] Section 7(1) of Chapter 2 of the Constitution.

In terms of s 7(2) of Chapter 2 of the Constitution the state is obliged to *'respect, protect, promote and fulfil the rights in the Bill of Rights.'* Section 7(2) of the Constitution thereby imposes a positive duty on the state not to infringe these fundamental rights.

Section 14 of Chapter 2 the Constitution entrenches the fundamental right of privacy and provides that: -

> *'14. 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*
>
> *(d) the privacy of their communications infringed.'*

The Constitution further affords the protection of the right to dignity.[102] This indicates that the right to privacy is considered as a separate right from that of dignity and it follows that a person's dignity does not need to be infringed in order for the person to enforce the right to privacy.[103]

In terms of s 36 of Chapter 2 of the Constitution:

> *'Limitation of rights*
>
> *36. (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;*

[102] Section 10 of the Constitution.
[103] R Davey and L Dahms-Jansen *Social Media in the Workplace* (2017) 40.

(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.

Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.'

A breach of the right to privacy as enshrined in s 14 of the Constitution will be regarded as an unlawful invasion of privacy. Once the plaintiff has established her claim, the onus rests on the defendant to prove that the alleged breach was justified in terms of s 36, or to show that the invasion of privacy was justified in the circumstances. Fault is not a required element for a constitutional invasion of privacy.

The court in *Bernstein* held as follows: -

'Caution must be exercised when attempting to project common law principles onto the interpretation of fundamental rights and their limitation; it is important to keep in mind that at common law the determination of whether an invasion of privacy has taken place constitutes a single enquiry, including an assessment of its unlawfulness. As in the case of other iniuriae the presence of a ground of justification excludes the wrongfulness of an invasion of privacy. In constitutional adjudication under the Constitution, by contrast, a two-stage approach must be employed in deciding constitutionality of a statute.'[104]

The two-stage approach referred to by the court in *Bernstein* is whereby the following questions need to be answered where a constitutional invasion of privacy is alleged:

1. has the invasive conduct infringed the right to privacy in the Constitution? and

2. if so, is such infringement justifiable in terms of the s 36 limitation clause?

[104] *Bernstein & others v Bester & others NNO* 1996 (2) SA 751 (CC) at 71.

2.4 **Data protection legislation**

It is clear from the above that the right to privacy is regarded as a fundamental human right that requires protection. Whilst it is accurate to state that the Constitution and the common law provide for the protection of privacy and a basis for data protection there is an imperative need for a legislative data protection regime in order to ensure legal certainty.

The SALRC was faced with the task of ascertaining whether data protection measures were necessary to safeguard the right to privacy or whether the judiciary should be tasked with applying the principles of the law of delict in order to protect the right to privacy. After undertaking a thorough investigation of the right to privacy the SALRC concluded that there is a need to regulate privacy and information protection by a general information statute. The SALRC Discussion Paper contained a draft Bill[105] and this Bill was signed into law in November 2013.[106]

In his analysis of the Protection of Personal Information Bill Neethling[107] agreed with the view expressed by the SALRC that there is a need for data protection legislation and stated:

> *'Thirty-five years ago the author came to the conclusion in his doctoral thesis on the right to privacy that the introduction of so-called data-protection legislation in our country was urgently necessary, in order to protect persons (natural or juristic) against the processing of their personal information by the state and private persons (individuals and corporations alike).'*[108]

Data processing poses a threat to the right to privacy as provided for under common law and the Constitution.[109] Roos provides a thorough analysis of data protection in

[105] Protection of Personal Information Bill, 2009.
[106] POPIA.
[107] J Neethling 'Features of the Protection of Personal Information Bill, 2009 and the law of delict' (2012) *THRHR* 241.
[108] J Neethling 'Features of the Protection of Personal Information Bill, 2009 and the law of delict' (2012) *THRHR* 241.
[109] A Roos 'Data Protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 421.

foreign jurisdictions and in South Africa. Roos concludes that data protection in South Africa was not in line with international standards and there is very limited law in South African protecting the vast majority of personal information.

Roos goes on to express the importance of the SALRC's proposed Bill[110] in rectifying the inefficiencies of data protection in South Africa. The Bill was signed into law on 19 November 2013 and known as POPIA.

Another reason that data protection legislation is crucial is due to that fact that when an individual's right to privacy is infringed by unlawful processing of their personal information, the individual will rely on the delictual remedies discussed above. As Roos states this is not adequate due to the following:

> *'When the privacy of a person has been infringed by the processing of personal information, he or she can rely on the law of delict for a remedy. However, the concept of 'data protection' or 'data privacy' has not been identified and discussed in any case law. Unfortunately, traditional delictual principles provide only limited protection for the individual's personal information, because they do not give the individual active control over personal information that is being processed. The traditional principles are useful in determining whether processing of personal information has taken place lawfully or not. However, the traditional principles cannot ensure, for example, that the data subject has knowledge of the fact that his or her personal information has been collected, or that he or she has access to the information, or that he or she may correct incorrect information. For this reason, the recognition of 'active control principles' is necessary.'*[111]

It follows that data protection legislation is necessary in order to set the legal parameters in respect of data processing and personal information. Conceptual clarity is necessary in order to avoid any potential communication gap and to ensure that data protection is more practically manageable.

A broad measure of agreement has been reached on the basic content and core rules that

[110] Protection of Personal Information Bill, 2009.
[111] A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 423.

should be provided for in data protection legislation.[112] Burchell[113] in his article expressed the view that South Africa should formulate legislation in line with the OECD Guidelines.[114]

POPIA has accordingly been influenced by the OECD Guidelines and the Council of Europe's (CoE) *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* ("CoE Convention").[115]

The OECD Guidelines identify eight core principal data protection principles in all influential data protection laws. These principles include: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. The OECD Guidelines do not provide for the ways in which these principles are to be enforced.

Roos[116] addresses this shortfall by providing an in-depth analysis of the core data protection principles and determining the ways in which these principles may be implemented in South Africa. Roos undertakes a thorough investigation of the data protection principles and ultimately concludes that these data protection principles should form part of South African data protection law.

Roos addressed the need for the legislature to implement data protection legislation by stating:

> *'In conclusion, the South African legislature is urged to adopt the proposals of the South African Law Reform Commission as a matter of urgency.'*[117]

Neethling submitted as follows:

---

[112] C J Bennett *Regulating privacy: data protection and public policy in Europe and the United States* (1992) 95.
[113] J Burchell 'The Legal Protection of Privacy in South Africa: A transplantable hybrid' (2009) 13(1) *EJCL* 1.
[114] Organisation for Economic Co-operation and Development (OECD) 'Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data' Paris, 1981 ("OECD Guidelines").
[115] Convention No. 108 of 1981, Strasbourg 28 Jan 1981. Available at: http://conventions.coe.int/Treaty/EN/treaties/html/108.htm, accessed on 20 April 2018.
[116] A Roos 'Core principles of data protection law' (2006) 39(1) *CILSA* 102 – 130.
[117] A Roos 'Personal data protection in New Zealand: lessons for South Africa' (2008) *PELJ* 109.

'Compared to the conclusion reached in the author's doctoral thesis thirty-five years ago, the adoption of legislation for the protection of personal information is now completely overdue. An appeal is therefore made to the legislature to finalise its scrutiny of the Protection of Personal Information Bill of 2009, recommended by the Law Reform Commission, and promulgate the Bill as soon as possible as part of the law of South Africa.'[118]

As submitted by Roos[119] the recognition of the right to privacy in the Constitution has a significant impact on the State in that *'the legislature and the executive may not pass any law or take any action which unreasonably infringes or limits the right.'*[120] Furthermore the constitutional recognition of the right to privacy places an obligation on the State to adopt legislation for the adequate protection of data privacy, *'since ordinary private-law principles provide only partial protection in this respect.'*[121]

Burns and Burger-Smidt[122] accurately address why it is important to promulgate data protection legislation in South Africa when privacy is protected by the common law and the Constitution by stating:

'The answer to this question lies in the globalisation of economies, rapid expansion of technology, the convergence of information and communications technology, the expansion of the Internet and its ability to swiftly transfer communication from one country to another. These factors, coupled with the emergence of new and challenging legal issues in a world where information (including personal information) is disseminated in a short timeframe and is open to abuse, made it quite clear that the protection of personal information is a pressing issue requiring legislative input.'[123]

Data protection legislation is necessary not only to protect a person's personal

[118] J Neethling 'Features of the Protection of Personal Information Bill, 2009 and the law of delict (2012) *THRHR* 255.
[119] A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 400 – 437.
[120] A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 423.
[121] A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 423.
[122] Y Burns & A Burger-Smidt, A *A Commentary on the Protection of Personal Information Act* (2018).
[123] Y Burns & A Burger-Smidt, A *A Commentary on the Protection of Personal Information Act* (2018) 5 – 6.

information, but also to protect the fundamental privacy rights of persons that are related to that personal information.

2.5 **POPIA**

Roos[124] accurately summarises the aim of POPIA as follows:

> *'The Act sets out to establish mechanisms or procedures in harmony with international prescripts to protect the privacy of personal information.'*[125]

POPIA aims to give effect to the Constitutional right to privacy by providing for data protection and thereby safeguarding personal information. Only limited sections of POPIA have come into operation with the majority of the sections to commence at a later date to be proclaimed by the President.[126]

The purpose of POPIA is set out in s 2(1), which reads as follows: -

> *'(a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at –*
>
> *(i) balancing the right to privacy against other rights, particularly the right of access to information; and*
>
> *(ii) protecting important interests, including the free flow of information within the Republic and across international borders.'*

POPIA defines, in s 1, the term *'processing*' as:

---

[124] A Roos 'Data privacy law' in Van der Merwe, DP. … et al. *Information and Communications Technology Law* 2 ed (2016).
[125] A Roos 'Data privacy law' in Van der Merwe, DP. … et al. *Information and Communications Technology Law* 2 ed (2016) 478.
[126] The sections that have come into operation at this time include: s 1 which contains the definitions; Part A of Chapter 5 which establishes the Information Regulator; s 112 which contains the Regulations and s 113 which sets out the procedure for making regulations.

'any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;'

In terms of s 3(1) POPIA applies to the processing of personal information –

'(a) entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and

(b) where the responsible party is –

(i) domiciled in the Republic; or

(ii) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.'

In line with the recommendations expressed by Roos,[127] POPIA has incorporated conditions for the lawful processing of personal information in line with international standards. POPIA aims to guarantee the protection of privacy and to this end it can be considered a codification of the common law and Constitutional principles in respect of privacy.[128]

Due to the fact that POPIA is not yet fully operational it cannot be determined as to

[127] A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 433.
[128] R Davey and L Dahms-Jansen *Social Media in the Workplace* (2017) 55.

whether it fulfils its objectives in safeguarding the right to privacy. The sections of POPIA that have come into operation at the time of writing are s 1 which contains the definitions; Part A of Chapter 5 which establishes the Information Regulator; s 112 which contains the Regulations and s 113 which sets out the procedure for making regulations.

The office of the Information Regulator is established in accordance with s 39 of POPIA and the President appointed the Chairperson and the members of the Information Regulator with effect from 1 December 2016 in accordance with s 41 of POPIA. The Information Regulator gazetted draft Regulations in terms of s 112(2) of POPIA on 8 September 2017 for comment by 7 November 2017. It is believed that the Information Regulator is in the process of reviewing the comments submitted to it.

Following the implementation of POPIA, albeit limited sections,[129] Roos accurately summarises POPIA as follows:

> *'The Act complies in all important aspects with international standards. It is a comprehensive, general law that governs the processing of personal information by both the public and the private sectors. It provides for a set of data privacy principles; provides heightened protection for sensitive information; establishes an independent oversight body to ensure compliance; and gives data subjects such rights as the right to be informed of the processing of personal information relating to them, of access to that information and to have incorrect information rectified, and provides subjects with civil remedies to enforce their rights.'*[130]

It follows that POPIA conforms to international standards and is an effective and comprehensive statute that aims to protect the integrity and sensitivity of personal informational.

[129] See note 126.
[130] A Roos 'Data privacy law' in Van der Merwe, DP. … et al. *Information and Communications Technology Law* 2 ed (2016) 478.

2.6 **Concluding remarks**

The State is obliged in terms of s 7(2) of the Constitution to respect, protect, promote and fulfill the right to privacy as provided for in the Bills of Rights. It follows that the State is attempting to fulfill this obligation in light of the promulgation of POPIA following the views and recommendations expressed in the SALRC Discussion Paper.[131]

The President appointed the Chairperson and members of the Information Regulator with effect from 1 December 2016, this being the juristic body created in terms of s 39 of POPIA to *inter alia* monitor and enforce compliance by public and private bodies with the provisions of POPIA. This appointment is a further indication of an attempt on the part of the State to fulfill its obligation to protect the right to privacy.

Although enacted, POPIA is not yet fully operational[132] and the sections that have commenced are of no import when applied in isolation to the remaining provisions. POPIA requires full promulgation in order to be of any influence on the right to privacy. The delay on the part of the legislature in fully promulgating POPIA provides a serious threat to the right to privacy it expressly sets out to protect. This requires urgent attention.

[131] J Neethling 'Features of the Protection of Personal Information Bill, 2009 and the law of delict (2012) *THRHR* 243.
[132] See note 126.

Chapter 3: An examination of vicarious liability in South Africa

3.1 Introduction

It is common cause, that in terms of the doctrine of vicarious liability, an employer is held accountable for the actions or omissions of its employees if such action or omission was committed by the employee in the course and scope of the his or her employment.[133]

Mogoeng J defines vicarious liability as:

> *' ... a person may be held liable for the wrongful act or omission of another even though the former did not, strictly speaking, engage in any wrongful conduct. This would arise where there is a particular relationship between those persons, such as employment. As a general rule, an employer is vicariously liable for the wrongful acts or omissions of an employee committed within the course and scope of employment, or whilst the employee was engaged in any activity reasonably incidental to it.'*[134]

The doctrine of vicarious liability stems from considerations of public policy and the notion that an individual whose rights have been wrongfully breached should not be left without a claim.[135]

In *Minister of Safety and Security v Morudu*[136] the Supreme Court of Appeal held that the doctrine of vicarious liability is deeply rooted in the South African legal system. In relying on the dictum in *F v Minister of Safety and Security,*[137] the court reiterated that *'employees are extensions of their employers.'*[138]

---

[133] T.J. Scott 'Some reflections on vicarious liability and dishonest employees' 2000 *Acta Juridica* 266.
[134] *F v Minister of Safety and Security [2011] ZACC 37; 2012 (1) SA 536 (CC)* at paragraph 40.
[135] R Le Roux 'Vicarious liability: revisiting an old acquaintance' 2003 *ILJ* 1879.
[136] *Minister of Safety and Security v Morudu and Others* 2016 (1) SACR 68 (SCA).
[137] *F v Minister of Safety and Security [2011] ZACC 37; 2012 (1) SA 536 (CC) ("F v Minister of Safety and Security").*
[138] *F v Minister of Safety and Security [2011] ZACC 37; 2012 (1) SA 536 (CC)* at 45.

3.2 **The doctrine of vicarious liability under the common law**

The doctrine of vicarious liability was first recognised in *Feldman (Pty) Ltd v Mall*[139] where the court held:

> *'... a master who does his work by the hand of a servant creates a risk of harm to others if the servant should prove to be negligent or inefficient or untrustworthy; that, because he has created this risk for his own ends he is under a duty to ensure that no one is injured by the servant's improper conduct or negligence in carrying on his work and that the mere giving by him of directions or orders to his servant is not a sufficient performance of that duty. It follows that if the servant's acts in doing his master's work or his activities incidental to or connected with it are carried out in a negligent or improper manner so as to cause harm to a third party the master is responsible for that harm.'*[140]

The doctrine of vicarious liability is a form of strict liability, which consists of liability in the absence of fault.[141] This is due to the fact that an employer will be held liable for the negligent acts or omissions by its employees irrespective of the fact that the employer was not the person that committed the wrongful act and was *'entirely removed from the event.'*[142]

In *Booysen v Minister of Safety and Security*[143] Plasket J held:

> *'In the normal course, a person is not liable in delict to another unless he or she has caused harm to that other person by a wrongful and unlawful act or omission. The imposition of vicarious liability is an exception to this norm: an employer who has committed no wrong is held liable for the consequences of his or her employee's wrongful and unlawful conduct.'*[144]

---

[139] *Feldman (Pty) Ltd v Mall* 1945 AD 733 at 741.
[140] *Feldman (Pty) Ltd v Mall* 1945 AD at 741.
[141] T.J. Scott 'Some reflections on vicarious liability and dishonest employees' 2000 *Acta Juridica* 266.
[142] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 16.
[143] *Booysen v Minister of Safety and Security* [2015] ZAECGHC 56 ("*Booysen v Minister of Safety and Security*").
[144] *Booysen v Minister of Safety and Security* [2015] ZAECGHC 56 at paragraph 9.

3.2.1 **Requirements for vicarious liability**

The common law requirements[145] for vicarious liability are as follows: -

a) an employment relationship must exist;

b) the employee's conduct must have been unlawful;

c) the act of the employee must have led to a third person suffering damages; and

d) the act must have taken place within the scope of his or her employment.[146]

The contract of employment can be defined as:

> *'The contract of employment is the foundation of the relationship between an employee and his employer. The contract links the employer and the employee in an employment relationship. The existence of an employment relationship is the starting point for the application of all labour law rules: if there is no employment relationship between the parties, the rules of labour law do not apply to that relationship.'*[147]

The existence of an employment relationship, that is a contract of employment,[148] at the time of the commission of the wrongful act by the employee is the primary requirement for the employer to be held vicariously liable to a third party.[149] For an employer to be held liable to a third party it must be established in which capacity the employee was acting at the commission of the delict due to the fact that an

[145] See *Mkize v Martens* 1914 AD 382 at 390.
[146] B Loots 'Sexual harassment and vicarious liability: a warning to political parties' (2008) 19 *SLR* 149.
[147] A Basson … et al *Essential Labour Law* 4 ed (2005) 19.
[148] In South African labour legislation there is no legal requirement that an employer and employee must enter into a written contract of employment in order for an employment relationship to exist. However, s 29 of the Basic Conditions of Employment Act 75 of 1998 stipulates that an employer must supply an employee, when the employee commences employment, with certain particulars in writing. This is generally done in the form of a contract of employment.
[149] B Loots 'Sexual harassment and vicarious liability: a warning to political parties' (2008) 19 *SLR* 149.

employer cannot be held liable on account of a wrongful act by an agent or independent contractor.[150]

In order for an employment relationship to be established the basic elements of the contract of employment need to be present, namely:

(a) a contract;

(b) in terms of which services are rendered;

(b) under the authority of the employer;

(d) for remuneration; and

(e) for a fixed term.[151]

Section 213 of the Labour Relations Act 66 of 1995 defines an employee as: -

'(a) Any person, excluding an independent contractor, who works for another person or for the state and who receives, or is entitled to receive, any remuneration; and

(b) Any person who in any manner assists in carrying on or conducting the business of the employer.'

The definition of an employee as provided for in the Labour Relations Act 66 of 1995 is replicated in s 1 of the Basic Conditions of Employment Act 75 of 1998.

An employer of an independent contractor is not vicariously liable for the wrongful acts of the independent contractor due to the fact that the independent contractor

[150] *Stein v Rising Tide Productions CC* 2002 2 All SA 22 (C) at 26 – 27.
[151] Section 83 of the Basic Conditions of Employment Act 75 of 1998 and s 200A of the Labour Relations Act 66 of 1995.

carries out certain specified work[152] and is not subject to the control or directions of the employer concerning the performance of such work.

In *SA Broadcasting Corporation v McKenzie*[153] the court formulated six important characteristics of employment and a contract of work in respect of independent contractors. These characteristics include:

> *'1. The object of the contract of service is the rendering of personal services by the employee to the employer. The services are the object of the contract. The object of the contract of work is the performance of a certain specified work or the production of a certain specified result.*
>
> *2. According to a contract of service the employee will typically be at the beck and call of the employer to render his personal services at the behest of the employer. The independent contractor, by way of contrast, is not obliged to perform the work himself or to produce the result himself, unless otherwise agreed upon. He may avail himself of the labour of others as assistants or employees to perform the work or to assist him in the performance of the work.*
>
> *3. Services to be rendered in terms of a contract of service are at the disposal of the employer who may in his own discretion subject of course to questions of repudiation decide whether or not he wants to have them rendered. The independent contractor is bound to perform a certain specified work or produce a certain specified result within a time fixed by the contract of work or within a reasonable time where no time has been specified.*
>
> *4. The employee is subordinate to the will of the employer. He is obliged to obey the lawful commands, orders or instructions of the employer who has the right of supervising and controlling him by prescribing to him what work he has to do as well as the manner in which it has to be done. The independent contractor, however, is notionally on a footing of equality with the employer. He is bound to produce in terms of his contract of work, not by the orders of the employer. He is not under the supervision or control of the employer. Nor is he*

[152] *SA Broadcasting Corporation v McKenzie* 1999 20 ILJ 1936 (LAC).
[153] *SA Broadcasting Corporation v McKenzie* 1999 20 ILJ 1936 (LAC).

under any obligation to obey any orders of the employer in regard to the manner in which the work is to be performed. The independent contractor is his own master.

5. *A contract of service is terminated by the death of the employee whereas the death of the parties to a contract of work does not necessarily terminate it.*

6. *A contract of service terminates on expiration of the period of service entered into while a contract of work terminates on completion of the specified work or on production of the specified result."*[154]

In terms of the second requirement for vicarious liability an employer is only liable for the conduct of an employee if the conduct satisfies the essential requirements for the commission of a wrongful act or delict, these being:

a) an act or omission by the employee;

b) which was wrongful;

c) actual damage or personal injury must have been suffered by the third party;

d) which act or omission caused the damage or personal injury to the third party; and

e) was committed in a wilful or negligent manner.[155]

A delict can be described as the wrongful and culpable act of a person that causes harm to another. The purpose of the law of delict is to compensate an individual for loss suffered therefore a prerequisite for liability is that the individual must have suffered harm. As held in the case of *Jowell v Bramwell-Jones and others:*[156]

[154] *SA Broadcasting Corporation v McKenzie* 1999 20 ILJ 1936 (LAC) at paragraph 9.
[155] *Crown Chickens v Rieck* 2007 *ILJ* 307 (SCA)
[156] *Jowell v Bramwell-Jones and others* 2000 3 SA 274 (SCA).

'The element of damage or loss is fundamental to the Aquilian action and the right of action is incomplete until damage is caused to the plaintiff by reason of the defendant's wrongful conduct.'[157]

It follows that the wrongful act is incomplete until the harm arises.

In respect of the third requirement for vicarious liability, the employee's act must have led to a third person suffering damages in order for the employer to be held liable. An employer will be held vicariously liable for the actions of its employees where the third party is able to show that the damage was caused by the employee, either intentionally or negligently, in the course of his or her employment duties.[158]

As accurately held by Judge Watermeyer:

'...It follows that if the servant's acts in doing his master's work or his activities incidental to or connected with it are carried out in a negligent or improper manner so as to cause harm to a third party the master is responsible for that harm.'[159]

The Constitutional Court in the case of *Country Cloud Trading CC*[160] held:

'So the element of wrongfulness provides the necessary check on liability in these circumstances. It functions in this context to curb liability and, in doing so, to ensure that unmanageably wide or indeterminate liability does not eventuate and that liability is not inappropriately allocated.'[161]

In *H v Fetal Assessment Centre*[162] the Constitutional Court held:

'From this it is apparent that "harm-causing conduct" is a prerequisite for the further

[157] *Jowell v Bramwell-Jones and others* 2000 3 SA 274 (SCA) at paragraph 22.
[158] *Minister of Safety and Security v Jordaan* 2000 (4) SA 21 (SCA) at paragraph 5.
[159] *Feldman (Pty) Ltd v Mall* 1945 AD at 741.
[160] *Country Cloud Trading CC v MEC, Department of Infrastructure Development, Gauteng* [2014] ZACC 28.
[161] *Country Cloud Trading CC v MEC, Department of Infrastructure Development, Gauteng* [2014] ZACC 28 at paragraph 25.
[162] *H v Fetal Assessment Centre* 2015 (2) BCLR 127 (CC).

enquiry into the other elements of delict, namely wrongfulness and fault. Without harm-causing conduct there is no conduct which can be found to be wrongful or committed with the requisite degree of fault.'[163]

The fourth requirement, being whether or not the employee acted within the scope and course of his or her employment, is the most controversial of the requirements and has proved to be the most difficult to determine.[164] It is accepted that employees act within the scope and course of their employment when they carry out instructions authorised by their employer, even when they perform the instructions in an unlawful manner.[165]

In *Minister of Safety and Security v Jordaan,*[166], Scott JA stated:

'The standard test for vicarious liability of a master for the delict of a servant is whether the delict was committed by the employee while acting in the course and scope of his employment. The enquiry is frequently said to be whether at the relevant time the employee was about the affairs, or business, or doing the work of the employer.... '[167]

The accepted common law test for vicarious liability was first applied in *Minister of Police v Rabie*[168] wherein the court held: -

'It seems clear that an act done by a servant solely for his own interests and purposes, although occasioned by his employment, may fall outside the course or scope of his employment, and that in deciding whether an act by the servant does so fall, some reference is to be made to the servant's intention . . . The test is in this regard subjective. On the other hand, if there is nevertheless a sufficiently close link

[163] *H v Fetal Assessment Centre* 2015 (2) BCLR 127 (CC) at paragraph 54.
[164] S Murray *The extent of an employer's vicarious liability when an employee act within the scope of employment* (LLB, North West University, 2012) 1.
[165] *Costa Da Oura Restaurant (Proprietary) Limited T/A Umdloti Bush Tavern v Anthony Reddy* 2003 24 ILJ 1337 (SCA).
[166] *Minister of Safety and Security v Jordaan* 2000 (4) SA 21 (SCA).
[167] *Minister of Safety and Security v Jordaan* 2000 (4) SA 21 (SCA) at paragraph 5.
[168] *Minister of Police v Rabie* 1986 (1) SA 117 (A) ("*Minister of Police v Rabie")*.

between the servant's acts for his own interests and purposes and the business of his master, the master may yet be liable. This is an objective test.'[169]

As established in *Minster of Police v Rabie*,[170] the accepted common law test for vicarious liability therefore contains two questions, these being:

a) whether the employee committed the wrongful acts solely for his or her own interests or those of the employer; and

b) if the employee was acting for his or her own interests, whether there was nevertheless a *'sufficiently close link'* between the employee's conduct and the business of his or her employment.

In deviation cases an employee commits unlawful conduct whilst straying from the tasks for which the employee was appointed. In traditional vicarious liability cases the wrongful acts or omission of an employee are committed within the course and scope of the employee's employment, in deviation or detour cases, the wrongful acts or omissions are committed by an employee outside the course and scope of the employee's employment.

In *NK v Minister of Safety and Security*[171] the court applied the common law test as established in *Minster of Police v Rabie* and held that the common law doctrine of vicarious liability should be developed to reflect the spirit, purport and objects of the Constitution.

In this case a woman ("the complainant") was raped by three policemen that were on duty at the time, in uniform and in a marked police vehicle. The three policemen were convicted of rape and the complainant thereafter sued the Minister of Safety and Security for damages based on vicarious liability. The court a quo dismissed the complainant's claim against the Minister and the complainant subsequently appealed to the Supreme Court of Appeal.

[169] *Minister of Police v Rabie* 1986 (1) SA 117 (A) at 134 C-E.
[170] *Minister of Police v Rabie* 1986 (1) SA 117 (A) at 134 C-E.
[171] *NK v Minister of Safety and Security* [2005] ZACC 8; 2005 (6) SA 419 (CC); 2005 (9) BCLR 835 (CC) ("*NK v Minister of Safety and Security*").

The Supreme Court of Appeal[172] dismissed the appeal and held that the acts of the policemen could not be regarded as having been done within the course and scope of their employment and further held that it is:

> *'... unnecessary to consider the question of the development of the law which in any event would best be dealt with by the legislature should a change in law be considered necessary.'*[173]

The complainant thereafter appealed to the Constitutional Court which had to determine whether the Minister was vicariously liable. The Constitutional Court applied the two-stage common law test for liability as established in *Minister of Police v Rabie.* O'Regan J found that the three policemen committed the wrongful act (the rape of the complainant) solely for their own interests. In respect of the second part of the two-stage test the court held:

> *'The next question that arises is whether, albeit that the policemen were pursuing their own purposes when they raped the applicant, their conduct was sufficiently close to their employer's business to render the respondent liable. In this regard, there are several important facts which point to the closeness of that connection. First, the policemen all bore a statutory and constitutional duty to prevent crime and protect the members of the public. That duty is a duty which also rests on their employer and they were employed by their employer to perform that obligation. Secondly, in addition to the general duty to protect the public, the police here had offered to assist the applicant and she had accepted their offer. In so doing, she placed her trust in the policemen although she did not know them personally. One of the purposes of wearing uniforms is to make police officers more identifiable to members of the public who find themselves in need of assistance.'*[174]

Furthermore O'Regan J held:

> *'Thirdly, the conduct of the policemen which caused harm constituted a simultaneous*

[172] *NK v Minister of Safety and Security* [2005] ZACC 8; 2005 (6) SA 419 (CC); 2005 (9) BCLR 835 (CC).
[173] *NK v Minister of Safety and Security* [2005] ZACC 8; 2005 (6) SA 419 (CC); 2005 (9) BCLR 835 (CC) at 8.
[174] *NK v Minister of Safety and Security* 2005 26 *ILJ* 1205 (CC) at 51.

commission and omission. The commission lay in their brutal rape of the applicant. Their simultaneous omission lay in their failing while on duty to protect her from harm, something which they bore a general duty to do, and a special duty on the facts of this case. In my view, these three inter-related factors make it plain that viewed against the background of our Constitution, and, in particular, the constitutional rights of the applicant and the constitutional obligations of the respondent, the connection between the conduct of the policemen and their employment was sufficiently close to render the respondent liable.'[175]

This approach by the Constitutional Court should be embraced as it enforces that the protection of fundamental rights is of profound constitutional importance. The Constitutional Court in coming to its decision applied the two stage common law test as developed in *Minster of Police v Rabie* and went further by developing and expanding the test to take into consideration constitutional norms. The Constitutional Court expanded on the second stage of the common law test by stating that in answering the second question[176] of the test the court should promote constitutional values in the assessment of the presence of a sufficient link.[177] Although there was a deviation from the employment duties of the policemen, there was a sufficiently close connection between the policemans employment and the rape to hold the Minister vicariously liable.

The case of *F v Minister of Safety and Security*[178] involved the rape of a 13-year-old girl by a SAPS police officer whilst on standby duty. The accused was in an unmarked police vehicle to enable him to perform any police functions that he might have been required to perform whilst on standby duty. The accused told the girl that he was a private detective and the girl understood this to mean that the accused was a police officer. The girl trusted the accused for this reason.

The girl's claim against the Minister of Safety and Security was successful in the

[175] *NK v Minister of Safety and Security* 2005 26 *ILJ* 1205 (CC) at 53.
[176] The second question as developed in *Minister of Police v Rabie* is if the employee was acting for his or her own interests, whether there was nevertheless a *'sufficiently close link'* between the employee's conduct and the business of his or her employment.
[177] *NK v Minister of Safety and Security* 2005 26 *ILJ* 1205 (CC) at 32.
[178] *F v Minister of Safety and Security* [2011] ZACC 37; 2012 (1) SA 536 (CC); 2012 (3) BCLR 244 (CC) ("*F v Minister of Safety and Security*").

High Court; however, the Supreme Court of Appeal then overturned the High Court's decision. The girl appealed to the Constitutional Court. The Constitutional Court, in determining the relevant interrelated normative factors at play, held:

> *'...the state's constitutional obligations to protect the public; the trust that the public is entitled to place in the police; the significance, if any, of the policeman having been off duty and on standby duty; the role of the simultaneous act of the policeman's commission of rape and omission to protect the applicant; and the existence or otherwise of an intimate link between the policeman's conduct and his employment.'*[179]

The Constitutional Court, in finding that the Minister of Safety and Security was vicariously liable for the damages suffered by the girl as a result of the rape and assault, held that the facts of the case gave rise to a sufficiently close link between the accused's employment and the assault and rape of the girl. The close link was founded on the grounds that, although the accused was not in uniform at the time of the assault, his police vehicle facilitated the commission of the rape; the girl placed her trust in the accused due to the fact that he was a police official; and that the state has a constitutional obligation to protect the public against crime.[180]

The Constitutional Court in *F v Minister of Safety and Security* ultimately expanded the two-stage test for vicarious liability. This is an important judgment as the Constitutional Court clarified the normative basis for holding the state vicariously liable for the criminal acts of police officers. This clarification is of vital importance as it promotes and develops state accountability for the criminal acts of police officers. In its judgment the Constitutional Court expunges the requirement that the employee must be acting *'within the course and scope of his or her employment'* for vicarious liability to be imposed.

In the recent case[181] of *Booysen v Minister of Safety and Security*[182] the

[179] *F v Minister of Safety and Security* [2011] ZACC 37; 2012 (1) SA 536 (CC); 2012 (3) BCLR 244 (CC) at 52.
[180] *F v Minister of Safety and Security* [2011] ZACC 37; 2012 (1) SA 536 (CC); 2012 (3) BCLR 244 (CC) at 53.
[181] Judgment handed down on 27 June 2018.
[182] *Booysen v Minister of Safety and Security* [2018] ZACC 18.

Constitutional Court confirmed that the two-stage test for vicarious liability is an established legal test. The court held:

> *'The two-stage enquiry for the imposition of vicarious liability in deviation cases first set out in Rabie and as developed in K and F is now an established legal test. Vicarious liability matters involve a careful consideration and weighing of the various factors set out in K and F to establish whether a sufficiently close link exists between an employee's conduct and the business of an employer. K and F expressly refer to factors as opposed to requirements and the weight to be accorded to each factor must inevitably be determined on a case by case basis. This flexibility inherent in the test will naturally lead to different factors being accorded different weights by different courts, but it is this very flexibility that has imbued the common law of delict with the values of the Constitution. As the applicant has not put forward an argument that the established test should be developed in order to afford greater weight to any one factor, this matter purely concerns the application of an established test. The threshold requirement of jurisdiction has not been met.'*[183]

As concluded by Kriegler J[184] in determining whether the employee acted within or without the course and scope of employment, the weighing up of the employee's subjective intention against the objective manifestations of his or her carrying out official duties is required. However if the act:

> *'was committed solely for the employee's own interests and purposes may fall outside the ambit of conduct that renders the employer liable, it is in our law established that liability may nevertheless follow if, objectively seen, there is a 'sufficiently close link' between the self-directed conduct and the employer's business.'*[185]

The Constitutional Court has accepted[186] that in order for an employer to be held vicariously liable for the actions or omissions of its employees a careful consideration and weighing of the various factors set out in K[187] and F[188] is required

[183] *Booysen v Minister of Safety and Security* [2018] ZACC 18 at paragraph 62.
[184] *Minister van Veiligheid en Sekuriteit v Japmoco* 2002 5 SA 649 (SCA) at paragraph 7.
[185] *Minister of Finance v Gore* 2007 1 SA 111 (SCA) at paragraph 28.
[186] See *Booysen v Minister of Safety and Security* [2018] ZACC 18.
[187] *NK v Minister of Safety and Security* 2005 26 *ILJ* 1205 (CC).
[188] *F v Minister of Safety and Security* [2011] ZACC 37; 2012 (1) SA 536 (CC); 2012 (3) BCLR 244 (CC).

in order to establish whether a sufficiently close link exists between an employee's conduct and the business of an employer.

3.2.2 Common-law defences to vicarious liability

The court in *Minister of Police v Rabie*[189] stated:

> *'An employer cannot be held liable if his employee performed an independent act, or acted for a purpose personal to the employee, or was motivated entirely by personal reasons such as spite or malice.'*

The following common-law defences are available to an employer in order to defend a claim founded on vicarious liability:

(a) the employee acts in defiance of an employer's express instruction and acted outside the course and scope of his or her duties;[190] or

(b) the employee deliberately committed a dishonest act solely for his or her own interests and purposes and such dishonest act is not sufficiently linked to the employer's business, thus falling outside the ambit of conduct that renders the employer liable;[191] or

(c) the employee abandoned his or her work and engaged in a frolic of his or her own.[192]

When an employee departs from an employer's express instruction, the employee acts outside the course and scope of his or her duties.[193] The court in *Bezuidenhout v Eskom*[194] held that that an employer will not liable where the employee's negligence in completing tasks within the course and scope of his duties caused damage to a third party because the employee ignored the employer's express instructions.

[189] *Minister of Police v Rabie* 1986 1 SA 117 (AD).
[190] *Bezuidenhout v Eskom* 2003 3 SA 83 (SCA).
[191] *Minister of Finance v Gore* 2007 1 SA 111 (SCA).
[192] *Ess Kay Electronics (Pty) Ltd v First National Bank of Southern Africa Ltd* 2001 1 SA 1214 (SCA).
[193] *Bezuidenhout v Eskom* 2003 3 SA 83 (SCA).
[194] *Bezuidenhout v Eskom* 2003 3 SA 83 (SCA).

In *SA Railways & Harbours v Marais*[195] the court held that where an employee performs an act expressly prohibited by the employer, such act constitutes a prohibition, which limits the sphere of employment.

The court in *Mkize v Martens*[196] held:

> *'A master is answerable for the torts of his servant committed in the course of his employment, bearing in mind that an act done by a servant solely for his own interests and purposes, and outside his authority, is not done in the course of his employment, even though it may have been done during his employment.'*

Accordingly, if an employee does something which he or she was prohibited from doing for the purposes of employment, but which he or she may have been permitted to do for his or her own personal purposes, the employer will not be liable unless the act was incidental to the employment.

The two-stage common law test for liability test as established in *Minster of Police v Rabie* confirms that an employer will only evade liability if his employee, viewed subjectively, has not only exclusively promoted his own interests, but viewed objectively, has also completely disengaged himself from the duties of his contract of employment. This approach adopted in *Minster of Police v Rabie* has been subsequently confirmed by the Constitutional Court in *NK v Minister of Safety and Security* and *F v Minister of Safety and Security.*[197]

3.3 The concept of statutory vicarious liability in terms of POPIA

Section 2(c) of POPIA provides that one of the purposes of POPIA is to provide data subjects with rights and remedies to protect their personal information from processing that is not in accordance with POPIA.

[195] *SA Railways & Harbours v Marais* 1950 4 SA 610 (A).
[196] *Mkize v Martens* 1914 AD 382 at paragraph 390.
[197] In these cases the courts used and accepted the two-stage common-law test for liability as developed in *Minister of Police v Rabie*. This test had both a subjective stage (evaluating the state of mind of the employee) and an objective stage (considering the link between the delict and the employer's enterprise).

A *'data subject'* in terms of POPIA is described as a person to whom personal information relates whereas a *'responsible party'* is a private or public body or person who determines the purpose of and means for processing personal information.

Millard and Bascerano[198] state that s 99 of POPIA essentially provides a form of statutory vicarious liability and imposes significant obligations on an employer.[199] They state that:

> *'the responsible party to whom POPI refers will be an employer, since it is usually the employer who determines the reason for the processing of personal information.'*[200]

Accordingly, Millard and Bascerano conclude that an employer will be held liable for any contraventions of POPIA or any unlawful infringement upon a data subject's right to privacy by its employees due to the fact that an employer is regarded as a responsible party.[201]

POPIA, when applied in the workplace has far-reaching consequences for responsible parties, being employers, as it creates strict liability on the part of the employer and holds the employer accountable for the wrongful acts of its employees.

According to Neethling:

> *'This principle is really self-evident and in line with the common law position that the person processing personal data can be prohibitorily or mandatorily interdicted, or will be liable - and thus accountable - for the wrongful infringement of privacy or identity. However, whereas intent or negligence is a requirement for liability at common law, according to the Bill liability is strict.'*[202]

---

[198] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 19.
[199] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 1 ("Millard and Bascerano").
[200] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 9.
[201] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 3.
[202] J Neethling 'Features of the Protection of Personal Information Bill, 2009 and the law of delict' (2012) *THRHR* 247.

Section 99(1) of POPIA provides as follows: -

> *'99 Civil remedies*
>
> *(1) a data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act as referred to in section 73, whether or not there is intent or negligence on the part of the responsible party.'*

In terms of this section, a civil action for damages may be instituted against the responsible party whether or not there is intent or negligence on the part of the responsible party. The employer must ensure that its employees comply with POPIA and failure by its employees to comply will render the employer accountable.[203]

Section 73 provides: -

> *'73 Interference with protection of personal information of data subject*
>
> *For the purposes of this Chapter, interference with the protection of the personal information of a data subject consists, in relation to that data subject, of –*
>
> *(a) any breach of the conditions for the lawful processing of personal information as referred to in Chapter 3;*
>
> *(b) non-compliance with section 22, 54, 69, 70, 71 or 72; or*
>
> *(c) a breach of the provisions of a code of conduct issued in terms of section 60.'*

Accordingly, in terms of s 99(1) an employer can be held vicariously liable in circumstances where an employee breaches the provisions of POPIA and infringes a data subject's privacy, despite the employers attempt to provide measures to regulate the lawful processing of personal information. Ultimately s 99(1) provides that any breach of POPIA or any unlawful infringement upon a data subject's right to privacy by

[203] Section 99(1) of POPIA.

an employee will result in the employer being held accountable.

Millard and Bascerano undertake a comparative analysis between the common law defences that may be raised by an employer attempting to escape vicarious liability and the statutory defences available to an employer in terms of POPIA. The authors argue that:

> '*… the statutory vicarious liability created by POPI is too harsh.*'[204]

They submit that the reason for this is due to that fact that s 99(2) is not in harmony with the defences available to an employer in terms of s 60(4) of the Employment Equity Act.

The defences that are available to an employer in the event of a breach of POPIA by its employees is contained in s 99(2) which reads as follows: -

> *'(2) In the event of a breach the responsible party may raise any of the following defences against an action for damages:*
>
> *(a) Vis major;*
>
> *(b) consent of the plaintiff;*
>
> *(c) fault on the part of the plaintiff;*
>
> *(d) compliance was not reasonably practicable in the circumstances of the particular case; or*
>
> *(e) the Regulator has granted an exemption in terms of section 37.'*

Section 37 reads as follows: -

[204] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 1.

'Regulator may exempt processing of personal information

37. (1) The Regulator may, by notice in the Gazette, grant an exemption to a responsible party to process personal information, even if that processing is in breach of a condition for the processing of such information, or any measure that gives effect to such condition, if the Regulator is satisfied that, in the circumstances of the case. –

(a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or

(b) the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing…'

Giles[205] identifies the issue concerning the lack of clarity in determining the import of s 99(2)(d) of POPIA. Giles, in dealing with the uncertainty in the interpretation of clause 99(2)(d) goes on to suggest that compliance with POPIA is not absolute and a responsible party only has to do what is *'reasonably practicable'* in order to comply with POPIA. This imprecise terminology will surely lead to uncertainty on the basis of what can be considered as *'reasonably practicable.'*

Giles goes on to state that *'reasonably practicable is a balance between the damages suffered and the steps taken in avoiding the risks.'*[206]

Section 60(4) of the Employment Equity Act states:

'(4) Despite subsection (3), an employer is not liable for the conduct of an employee if that employer is able to prove that it did all that was reasonably practicable to ensure

[205] J Giles 'Only do what is reasonably practicable to comply with POPI' (23 May 2014 available at https://www.michalsons.com/blog/reasonably-practicable-to-comply-with-popi/13296, accessed on 21 April 2018).
[206] J Giles 'Only do what is reasonably practicable to comply with POPI' (23 May 2014 available at https://www.michalsons.com/blog/reasonably-practicable-to-comply-with-popi/13296, accessed on 21 April 2018).

that the employee would not act in contravention of this Act.'

Therefore, in terms of the Employment Equity Act if the employer is able to prove that it did all that was reasonably practicable to ensure that the employee would not act in contravention of the Employment Equity Act, the employer will be able to avoid being held vicariously liable for the contraventions by its employees. The Employment Equity Act therefore provides for the ability of the employer to escape liability in circumstances where the employer has taken all precautionary actions to prevent unlawful conduct of its employees.

Section 60(4) of the Employment Equity Act is therefore an exemption clause that stipulates that the employer is limited or excluded from liability if it *'did all that was reasonably practicable to ensure that the employee would not act in contravention of*[207] the Employment Equity Act.

POPIA, contrary to the Employment Equity Act, does not provide such an exemption clause to employers and employers, in terms of POPIA, can be held vicariously liable for breach of any provision of POPIA whether or not there is intent or negligence on the part of the employer, even in circumstances where the employer has promoted compliance with POPIA and diligently strived to avoid contraventions of POPIA on the part of its employees.[208]

The Employment Equity Act states in s 60(1) that the employees contravention of the Employment Equity Act must occur *'while at work.'*[209] This section resembles the common law requirement for vicarious liability that the employees wrongful act must have taken place within the scope of his or her employment.[210] POPIA does not expressly provide this requirement. Consequently POPIA makes it difficult, if not impossible, for an employer to evade liability in circumstances where an employee

[207] Section 60(4) of the Employment Equity Act.
[208] Sections 99(1) and 99(2) of POPIA.
[209] Section 60(1) of the Employment Equity Act states:
'60. (1) If it is alleged that an employee, while at work, contravened a provision of this Act, or engaged in any conduct that, if engaged in by that employee's employer, would constitute a contravention of a provision of this Act, the alleged conduct must immediately be brought to the attention of the employer.'
[210] As discussed in paragraph 3.2.1 above.

contravenes the provisions of POPIA for personal gain and is completely removed from his or her employment duties.

Similarly, s 37 of the Occupational Health and Safety Act No. 85 of 1993, as amended ("Occupational Health and Safety Act"), reads as follows: -

> *'37. Acts or omissions by employees or mandataries. - (1) Whenever an employee does or omits to do any act which it would be an offence in terms of this Act for the employer of such employee or a user to do or omit to do, then, unless it is proved that –*
>
> *...*
>
> *(c) all reasonable steps were taken by the employer or any such user to prevent any act or omission of the kind in question, the employer or any such user himself shall be presumed to have done or omitted to do that act, and shall be liable to be convicted and sentenced in respect thereof; and the fact that he issued instructions forbidding any act or omission of the kind in question shall not, in itself, be accepted as sufficient proof that he took all reasonable steps to prevent the act or omission.'*

Therefore, in terms of the Occupational Health and Safety Act, the employer will be able to escape liability if it is able to prove that *'all reasonable steps were taken to prevent a contravention'* of[211] the Occupational Health and Safety Act.

The limited defences available to employers in terms of s 99(2) of POPIA will not enable the employer to avoid liability. As accurately summarised by Millard and Bascerano:

> *'Unfortunately, POPI makes no distinction between the liability of a prudent employer and one who adopts a nonchalant approach to the duty to respect the privacy of data subjects. Both the virtuous and the indifferent employer are treated alike in respect of contraventions by their employees. Consequently, the good deeds of the virtuous employer seem to be of no significance. Undeniably, the law-abiding employer's good*

[211] Section 37(1)(c).

deeds will not constitute an acceptable defence against retribution in terms of POPI.'[212]

As it is currently phrased s 99(1) provides that any breach of POPIA or any unlawful infringement upon a data subject's right to privacy by an employee will result in the employer being held accountable, whether or not there is intent or negligence on the part of the employer and the few defences available to employers in terms of s 99(2) of POPIA will not enable the employer to avoid liability.

3.4 Concluding remarks and recommendations

POPIA defences to a claim based on vicarious liability in s 99(2) are not in harmony with the statutory defences provided for in other legislation, such as the Employment Equity Act. Due to the fact that POPIA is not fully operational as yet the effects of the lack of sufficient defences to a claim based on vicarious liability cannot be practically assessed at this stage.

As stated by Millard and Bascerano, the only defence available to an employer would be to ensure that it has comprehensive liability insurance to reduce the risk of contraventions of POPIA by its employees.[213] This will no doubt be a costly exercise.

It can be accurately concluded that due to the *'legislature's short-sightedness'*[214] in not taking into consideration the fact that the employer has promoted compliance with POPIA and actively sought to avoid infringements of POPIA on the part of its employees, POPIA lacks foresight and the civil remedies as contained in sections 99(1) and 99(2) are excessively one sided in favour of the data subject and so adverse to the employer as to be discriminatory. It is difficult to discern how such incoherence between the statutory defences to a claim based on vicarious liability in terms of POPIA and those available to an employer in alternative legislation will be dealt with

[212] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 31.
[213] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 31.
[214] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 31.

once POPIA is fully operational.[215]

In terms of the Constitutional Court decisions in *NK v Minister of Safety and Security* and *F v Minister of Safety and Security* at common law an employer could be held vicariously liable for an employee's wrongful conduct committed outside of the course and scope of the employee's employment in circumstances where the wrongful act is sufficiently related to conduct authorised by the employer. It would appear that the provisions of POPIA are not consistent with this position in that section 99(1) does not stipulate that the contravention of POPIA must occur '*while at work*'[216] and that the employer will be liable *'whether or not there is intent on the part of the responsible party.'*[217]

Where a data subject's privacy has been infringed the data subject will be in a position to base a claim against the employer, in circumstances where the infringement was committed by an employee of the employer, in terms of the common law right to privacy[218] or in terms of the statutory right to privacy provided in POPIA. As correctly stated by Millard and Bascerano the data subject essentially has *'two roads to an employer's vicarious liability (one in terms of the common-law vicarious liability for delicts committed by an employee and the other in terms of section 99 of POPI).'*[219]

Accordingly, the data subject may claim against the employer either in terms of the common law doctrine of vicarious liability or in terms of s 99(1) of POPIA.[220] The data subject may institute civil action against the employer as the responsible party in terms of s 99(1) of POPIA.

The deciding factor for a data subject will be the fact that in terms of POPIA the employer will not be in a position to escape liability due to the limited defences

[215] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 30.
[216] As provided for in s 60 of the Employment Equity Act.
[217] Section 99(1) of POPIA.
[218] In terms of the common law doctrine of vicarious liability both the employee and the employer will be held liable even through no fault of the employers.
[219] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 15.
[220] The data subject may institute civil action against the employer as the responsible party in terms of s 99(1) of POPIA.

available to the employer in terms of s 99(2). Section 99(2) provides very limited defences that an employer may raise against an action brought in terms of s 99(1). POPIA's current position is in contrast to the position adopted by the Employment Equity Act and the Occupational Health Act discussed above and it is suggested that s 99(2) be amended in order to provide for impartiality on the part of the legislature.

Millard and Bascerano submit that s 99(2) should be amended as follows:

> *'Despite subsection (1), an employer is not liable for the conduct of an employee if that employer is able to prove that it did all that was reasonably practicable to ensure that the employee would not act in contravention of this Act.'*[221]

It is suggested that POPIA be extended, in particular a new s 99(2)(A) be inserted, in order to provide for adequate defences that may be raised by an employer against an action for damages. Whilst the recommendation provided by Millard and Bascerano is suitable, the following would provide more adequate given the approach adopted in foreign jurisdictions:[222]

> *(2)(A) Despite subsections (1) and (2), a responsible party will be exempted from liability, in whole or in part, if the responsible party proves that it is not responsible for the event giving rise to the breach and it did all that was reasonably practicable to ensure compliance with this Act.'*

This simple addition will enable an employer to escape liability and avoid being held vicariously liable for contraventions of POPIA by an employee if the employer can prove that it did all that was reasonably practicable to ensure that employees would not contravene the provisions of POPIA.

[221] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 32.
[222] The approach of foreign jurisdictions is analysed in chapter 4.

Chapter 4: Foreign approaches with regard to vicarious liability

4.1 Introduction

The purpose of this chapter is to consider the concept of an employer's statutory vicarious liability in respect of privacy breaches by their employees in two foreign jurisdictions, namely, the United Kingdom and Canada.

This chapter sets out to determine whether the statutory vicarious liability provided for in POPIA requires modification in order to ensure international compliance in so far as data protection is concerned. The data protection frameworks of the United Kingdom and Canada will be compared to that of South Africa in order to draw lessons that may be useful in so far as the concept of statutory vicarious liability in respect of privacy breaches is concerned.

The rationale behind this comparison is due to the fact that like POPIA, the data protection frameworks of the United Kingdom and Canada are based on the OECD[223] Guidelines. The provisions of POPIA are similar to those of the Data Protection Act 2018 – applicable in the United Kingdom - and the United Kingdom data protection framework is similar to that of POPIA. The data protection legislation in the United Kingdom and Canada has furthermore been in place for a longer period of time and it can therefore be analysed from a practical perspective as well as an academic perspective.

4.2 United Kingdom

The General Data Protection Regulation 2016/679 ("GDPR") was approved by the European Union ("EU") Parliament on 14 April 2016 and commenced on 25 May 2018. The GDPR regulates data protection and privacy in the EU[224] and is designed to lay down rules relating to the protection of natural persons with regard to the processing of

[223] The Organisation for Economic Co-operation and Development (OECD) is an intergovernmental economic organisation with thirty six member countries. The OECD was founded in 1961 to stimulate economic progress and world trade.
[224] Article 3 of the GDPR.

personal data and rules relating to the free movement of personal data and protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.[225]

Following the Brexit[226] referendum on 23 June 2016, the United Kingdom updated its data protection regulations to ensure that the standards set out in the GDPR have effect in the United Kingdom by enshrining those standards in United Kingdom law in the form of the Data Protection Act 2018 ("DPA 2018").

The DPA 2018 is a United Kingdom Act of Parliament[227] that received royal assent on 23 May 2018. The DPA 2018 commenced on 25 May 2018, this being at the same time as the GDPR. Following the United Kingdom's exit from the EU[228] the GDPR will no longer directly apply in the United Kingdom.[229]

The DPA 2018 is essentially the United Kingdom's implementation of the GDPR[230] and has three main purposes:

a) it incorporates the GDPR into United Kingdom law;

b) it repeals and replaces the Data Protection Act 1998 ("DPA 1998") as the primary piece of data protection legislation in the United Kingdom; and

c) it ensures that the United Kingdom and EU data protection regimes will continue to be aligned following Brexit which will allow the UK to continue to be able to freely exchange personal data with the EU.[231]

---

[225] Article 1 of the GDPR.
[226] Brexit is an abbreviation for *'British exit'* referring to the UK's decision to leave the EU. On 29 March 2019 the UK is scheduled to leave the EU.
[227] The DPA 2018 is a UK-specific law.
[228] See note 219.
[229] The GDPR applies in the United Kingdom until it leaves the EU.
[230] After Brexit the DPA 2018 will ensure that United Kingdom data protection legislation will be aligned with the GDPR.
[231] K Lamb 'UK: Introducing the Data Protection Act 2018!' (6 June 2018) available at http://www.mondaq.com/uk/x/708140/data+protection/Introducing+The+Data+Protection+Act+2018), accessed on 4 October 2018.

4.2.1 **Important definitions in the Data Protection Act 2018**

Section 3 of the DPA 2018 provides for the following definitions:

'(2) "Personal data" means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)).

(3) "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to –

(a) an identifier such as a name, an identification number, location data or an online identifier, or

(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

(4) "Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as –

(a) collection, recording, organisation, structuring or storage,

(b) adaptation or alteration,

(c) retrieval, consultation or use,

(d) disclosure by transmission, dissemination or otherwise making available,

(d) alignment or combination, or

(f) restriction, erasure or destruction,

(subject to subsection (14)(c) and sections 5(7), 29(2) and 82(3), which make provision about references to processing in the different Parts of this Act).

(5) "Data subject" means the identified or identifiable living individual to whom

personal data relates.'

Section 6 of Chapter 2 of the DPA 2018 defines *'controller'* as

'6 Meaning of "controller"

(1) The definition of "controller" in Article 4(7) of the GDPR has effect subject to -

(a) subsection (2),

(b) section 209, and

(c) section 210.'

In terms of Article 4(7) of the GDPR *'controller'* means:

'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;'

In terms of Article 4(8) of the GDPR *'processor'* means:

'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;'

4.2.2 **Data protection principles**

Chapter 2 of the DPA 2018 sets out the six data protection principles. The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter.[232] The six data protection principles are:

[232] Section 34(3) of the DPA 2018.

1) the processing of personal data for any of the law enforcement purposes must be lawful and fair;[233]

2) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected;[234]

3) personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed;[235]

4) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay;[236]

5) personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed;[237] and

6) personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, *'appropriate security'* includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).[238]

[233] Section 35 of the DPA 2018.
[234] Section 36 of the DPA 2018.
[235] Section 37 of the DPA 2018.
[236] Section 38 of the DPA 2018.
[237] Section 39 of the DPA 2018.
[238] Section 40 of the DPA 2018.

The six data protection principles provided for in Chapter 2 of the DPA 2018 are aligned with the six data protection principles contained in Article 5 of Chapter 2 of the GDPR. In contrast to the DPA 2018 and the GDPR the DPA 1998 contained eight data protection principles. The two additional data protection principles in the DPA 1998 are:

a) principle 6 - personal data shall be processed in accordance with the rights of data subjects;[239] and

b) principle 8 - data may only be transferred out of the European Economic Area if the country to which the data is being transferred has adequate legal protection for individuals and their details.[240]

4.2.3 **Vicarious liability**

Section 13 of the DPA 1998 provides for compensation for failure to comply with certain requirements. Section 13(3) of the DPA 1998 provides:

> *'(3) In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned.'*

Section 55A of the DPA 1998 states:

> *"(1) The Commissioner may serve a person with a monetary penalty if the Commissioner is satisfied that:*
>
> *(a) there has been a serious contravention of the requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2003 by the person, and*

[239] The GDPR and the DPA 2018 do not provide for an equivalent access principle, instead, access rights are provided for separately in s 2 of Chapter 3 of the GDPR and in s 45 of Chapter 3 of the DPA 2018.
[240] The GDPR and the DPA 2018 do not provide for an equivalent overseas transfer principle, instead, overseas transfer is provided for separately in Chapter 5 of the GDPR and Chapter 5 of the DPA 2018.

(b) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the person –

(a) knew or ought to have known that there was a risk that the contravention would occur, but

(b) failed to take reasonable steps to prevent the contravention.'

Article 23[241] of the EU Directive 95/46/EC[242] states that:

'1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.'

Similarly s 169 of the DPA 2018 provides:

'169 Compensation for contravention of other data protection legislation

(1) A person who suffers damage by reason of a contravention of a requirement of the data protection legislation, other than the GDPR, is entitled to compensation for that damage from the controller or the processor, subject to subsections (2) and (3).

(2) Under subsection (1) –

[241] Chapter III Judicial Remedies, Liability and Sanctions.
[242] European Union (EU) Directive No. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

(a) a controller involved in processing of personal data is liable for any damage caused by the processing, and

(b) a processor involved in processing of personal data is liable for damage caused by the processing only if the processor –

(i) has not complied with an obligation under the data protection legislation specifically directed at processors, or

(ii) has acted outside, or contrary to, the controller's lawful instructions.

(3) A controller or processor is not liable as described in subsection (2) if the controller or processor proves that the controller or processor is not in any way responsible for the event giving rise to the damage.

...'

The exemption provided to employers in s 169(3) of the DPA 2018 is narrower than the exemption provided in Article 23(2) of the EU Directive 95/46/EC.

Recital 55 of the EU Directive 95/46/EC states:

'Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;'

It is evident in s 13(3) of the DPA 1998, s 55A of the DPA 1998, Article 23 of the EU Directive 95/46/EC, s 169(3) of the DPA 2018 and Recital 55 of the EU Directive 95/46/EC that an employer is exempt from liability in circumstances where the employer is able to show that it took reasonable measures to prevent any

the contravention of the legislation.

As previously alluded to, POPIA contains no such mechanism for an employer to escape liability even in circumstances where an employer is able to show that it reasonable steps to prevent the contravention of POPIA.

4.2.4 **Case law**

Due to the fact that the DPA 2018 is a relatively new piece of legislation it is yet to be practically assessed before British courts. However, a landmark ruling was handed down in the Queen's Bench Division of the High Court of Justice on 1 December 2017 in the case of *Various Claimants v WM Morrisons Supermarket Plc.*[243] In this group action 5 518 employees ("claimants") of Morrisons Supermarket PLC ("Morrisons") sued Morrisons and claimed compensation for breach of statutory duty in terms of s 4(4) of the DPA 1998 and at common law for the misuse of private information and breach of confidence.

This case concerned the disclosure of personal data of a large number of employees of Morrisons by a rogue employee ("Skelton"), being a senior IT internal auditor of Morrisons. Skelton posted a file containing the personal information of the employees on a file sharing website. The personal information posted by Skelton contained information such as names, addresses, gender, dates of birth, phone numbers, national insurance numbers, bank codes and account numbers as well as salaries.

[243] *Various Claimants v WM Morrisons Supermarket Plc* (Rev 1) [2017] EWHC 3113 (QB) ("*Various Claimants v WM Morrisons*").

The claimants claimed that Morrisons had primary liability for its own acts or omissions, and vicarious liability for the actions of one of its employees. The claimants claimed a breach of the principles of the DPA 1998, in particular data protection principle 1 which requires the consent of a data subject[244] to the processing[245] of its personal data.[246] The claimants did not consent to the processing of their personal data by Skelton.

The claimants further claimed a breach of the data protection principles referred to in s 4 of the DPA 1998 and contained in Part 1 of Schedule 1 of the DPA 1998. The claimants stated that in terms of s 4(4) of the DPA, which reads as follows: -

> *'(4) Subject to section 27(1), it shall be the duty of the data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller.'*

Morrisons was at all relevant times the data controller[247] in respect of the payroll data abstracted and transferred to Skelton and that it failed to comply with data protection principles 1,[248] 2,[249] 3,[250] 5[251] and 7.[252]

---

[244] In terms of s 1 of the DPA, 1998 *'data subject'* means an individual who is the subject of personal data.
[245] In terms of s 1 of the DPA 1998 *'processing'* in relation to information or data, means:
'obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—
(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data;
[246] In terms of s 1 of the DPA 1998 *'personal data'* means *'data which relate to a living individual who can be identified -*
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.'
[247] In terms of s 1 of the DPA 1998 *'data controller'* means, *'subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.'*
[248] In terms of data protection principle 1 personal data must be processed fairly and lawfully.
[249] In terms of data protection principle 2 personal data must be processed for specified lawful purposes.
[250] In terms of data protection principle 3 personal data must be adequate, relevant and not excessive.
[251] Data protection principle 5 requires that personal data is not to be kept for longer than is necessary.
[252] Data protection principle 7 requires that personal data must be kept secure.

The court held that Morrisons could not be held directly liable for the breach of the DPA 1998 data protection principles due to the fact that it was not the data controller at the time when the first, second, third and fifth data protection principles were breached. The misuse and processing of the data were those of Skelton, and not Morrisons.[253] It was Skelton, acting without authority as an independent data controller that disclosed the personal data of the claimants. The only duty Morrisons owed the claimants was in terms of the seventh data protection principle which requires the data controller to take appropriate measures to protect personal data against unlawful processing.

The court identified at paragraph [73] six respects in which the claimants alleged that Morrisons fell short of its obligations under data protection principle 7 while it was the data controller. These are summarised by Langstaff J as follows:

> *'These contentions became six issues: whether Morrisons fell short of their obligations under DPP7 by: -*
>
> *a) failing to manage/mentor Skelton "to prevent a grudge developing";*
>
> *b) failing to monitor the email "quarantine" area so as to identify that the data was being transferred to Skelton;*
>
> *c) failing to identify that Skelton was researching the "TOR" network;*
>
> *d) failing to deny Skelton access to the data;*
>
> *e) providing the data to Skelton via USB stick which it was alleged was not encrypted; and*
>
> *f) failing to ensure that Skelton deleted the payroll data (in the particulars of claim, the Claimants asserted it ought to have been effective on or about 21st November).'*

[253] *Various Claimants v Wm Morrisons Supermarket PLC* [2017] EWHC 3113 (QB) 2017 at paragraph 47.

The court held that Morrisons had taken the appropriate measures to protect the claimants' data against misuse. Morrisons had put in place security systems which were generally considered by the court to be adequate and appropriate. Surprisingly, Langstaff J went on to hold as follows:

> *'I cannot, however, construe either the Directive or the Act as requiring a data controller to be responsible even without fault for the subsequent disclosure by a third party of some of the information given to it.'*[254]

The court held that *'there was an unbroken thread that linked his work to the disclosure: what happened was a seamless and continuous sequence of events.'*[255]

Langstaff J held as follows:

> *'... it is notable that Lord Toulson explained those cases in which liability had been upheld as being those where the employee misused his position in a way which injured the claimant, and that it was just that the employer who selected him and put him in that position should be held responsible .... I would add to his exposition only that the employer, too, had at least the theoretical right to control. Though employers can hardly tell highly skilled workers the detail of how to do their jobs, it remains a necessary element in every contract of employment that the employer has "...lawful authority to command so far as there is scope for it. and there must always be some room for it, if only in incidental or collateral matters" (Zuijs v. Wirth Brothers Proprietary, Ltd (1955) 93 C.L.R. 561, 571, cited by McKenna J. in Ready-Mixed Concrete v Minister of Pensions and National Insurance [1968] 2 QB 497): nowadays perhaps best rendered as a directory power.'*[256]

The court relied on the judgment in the case of *Catholic Child Welfare Society*[257] wherein Lord Phillips held: -

> *'The relationship that gives rise to vicarious liability is in the vast majority of cases*

[254] *Various Claimants v Wm Morrisons Supermarket PLC* [2017] EWHC 3113 (QB) 2017 at paragraph 57.
[255] *Various Claimants v Wm Morrisons Supermarket PLC* [2017] EWHC 3113 (QB) 2017 at paragraph 183.
[256] *Various Claimants v Wm Morrisons Supermarket PLC* [2017] EWHC 3113 (QB) 2017 at paragraph 192.
[257] *The Catholic Child Welfare Society and others (Appellants) v Various Claimants and The Institute of the Brothers of the Christian Schools (Respondents*) [2012] UKSC 56.

that of employer and employee under a contract of employment. The employer will be vicariously liable when the employee commits a tort in the course of his employment. There is no difficulty in identifying a number of policy reasons that usually make it fair, just and reasonable to impose vicarious liability on the employer when these criteria are satisfied: i) The employer is more likely to have the means to compensate the victim than the employee and can be expected to have insured against that liability; ii) The tort will have been committed as a result of activity being taken by the employee on behalf of the employer; iii) The employee's activity is likely to be part of the business activity of the employer; iv) The employer, by employing the employee to carry on the activity will have created the risk of the tort committed by the employee; v) The employee will, to a greater or lesser degree, have been under the control of the employer.' [258]

In response to the factors set out by Lord Phillips above the court held as follows:

'The factors identified in Catholic Child Welfare Society are typically true of relationships of employee and employer, which was what was addressed in paragraph 35 of the judgment of Lord Phillips. They are true here too, where the context is not relationship but course of employment: Morrisons are more likely to have the means to compensate the victim than Skelton and can be expected to have insured against that liability, even if breaches of data security may not historically have been a mainstream risk; it follows from my finding above (ii) that the tort was committed as a result of activity being taken by the employee on behalf of the employer – in the sense of his being chosen to handle the data, with a view to the employer's interests in completing an audit, such that Skelton's employee activity – viewed broadly – can be seen as part of the business activity of the employee, even though he chose to abuse his position. As to (iv), the employer, by employing the employee to carry on the activity, created the risk of the tort committed by the employee; and v) Skelton was, to a greater or lesser degree, under the control of the employer, at least in the sense described in the last paragraph above.'[259]

Langstaff J held that the principles of vicarious liability apply to the DPA 1998. The aim of the DPA 1998 is the protection of data subjects and accordingly if an

[258] *The Catholic Child Welfare Society and others (Appellants) v Various Claimants and The Institute of the Brothers of the Christian Schools (Respondents*) [2012] UKSC 56 at paragraph 35.
[259] *Various Claimants v Wm Morrisons Supermarket PLC* [2017] EWHC 3113 (QB) 2017 at paragraph 193.

employer can escape liability the moment an employee decides to misuse data to which his employer has given him access, this would defeat the purpose of the DPA 1998.[260]

The *'course of employment'* test for vicarious liability should be applied broadly. The court found that there was a sufficient connection between Skelton's employment and his wrongful conduct for vicarious liability to be established. This was despite the disconnect in time, place and nature from Skelton's employment when he posted the data.

The High Court held that Morrisons was vicariously liable for the actions of Skelton on the basis of vicarious liability. This case is the first successful class action for a data breach in the United Kingdom.

In concluding, Langstaff J stated:

> *'The point which most troubled me in reaching these conclusions was the submission that the wrongful acts of Skelton were deliberately aimed at the party whom the claimants seek to hold responsible, such that to reach the conclusion I have may seem to render the court an accessory in furthering his criminal aims. I grant leave to Morrisons to appeal my conclusion as to vicarious liability, should they wish to do so, so that a higher court may consider it: but would not, without further persuasion, grant permission to cross-appeal my conclusions as to primary liability.'*[261]

Morrisons subsequently appealed the order of Langstaff J dated 1 November 2017 and the appeal was heard in the Court of Appeal (Civil Division) before Lord Justice Bean and Lord Justice Flaux on 9 and 10 October 2018.[262] Judgment was handed down on 22 October 2018.

[260] *Various Claimants v Wm Morrisons Supermarket PLC* [2017] EWHC 3113 (QB) 2017 at paragraph 154.
[261] *Various Claimants v Wm Morrisons Supermarket PLC* [2017] EWHC 3113 (QB) 2017 at paragraph 198.
[262] *Various Claimants v Wm Morrison Supermarkets PLC* [2018] EWCA Civ 2239.

The appeal concerned whether Langstaff J was correct in deciding that Morrisons is vicariously liable to the claimants for the actions of Mr Skelton. The appeal court held:

> *'The common law principle of vicarious liability is not confined to common law wrongs. It holds good for a wrong comprising a breach of statutory duty provided the statute does not expressly or impliedly indicate otherwise: Majrowski v Guy's and St Thomas's NHS Trust [2006] UKHL 34, [2007] 1 AC 224 at [10] Lord Nicholls). The DPA does indicate the contrary. Pursuant to the Directive, the DPA seeks to achieve a balance between the right to privacy and the free flow of personal data from one member state to another in the interests of economic and social progress. It imposes express obligations on the data controller, primarily the obligation under section 4(4) to comply with the DPP. In accordance with ordinary principles of EU jurisprudence, those obligations are to be interpreted as proportionate ones. They are in any event expressly qualified in important respects by reference to what is appropriate or reasonable. So, DPP 7 requires that "appropriate" technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*[263]
>
> *What is "appropriate" is related to the state of technological development and the cost of implementing any measures as well as the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage, and the nature of the data to be protected: Schedule 1 Part II para. 9. Importantly, under DPP 7 the data controller must take "reasonable steps" to ensure the reliability of any employees of his who have access to the personal data: Schedule 1 Part II para. 10. The DPA, therefore, expressly recognises the potential liability of a data controller for the wrongful processing of data by his employees. Instead, however, of imposing a vicarious liability, which is a strict liability irrespective of the employer's fault, it imposes a primary liability on the employer restricted to taking "reasonable steps" to ensure the reliability of the relevant employees. Further, section 13(3) provides that it is a defence to an action by an individual for compensation from the data controller for breach of any of the requirements of the DPA that the data controller has taken such care as in all the circumstances was reasonably required to comply with the requirement concerned. In effect, so far as concerns civil liability, the*

[263] *Various Claimants v Wm Morrison Supermarkets PLC* [2018] EWCA Civ 2239 at paragraph 40.

liability is based on fault or culpability: cf. criminal liability under section 55 of the DPA.'[264]

The appeal court did not accept that *'there is an exception to the irrelevance of motive where the motive is, by causing harm to a third party, to cause financial or reputational damage to the employer.'*[265]

The appeal court agreed with Langstaff J and held that Morrisons was vicariously liable for the wrongful act committed by Mr Skelton against the claimants. The appeal was dismissed. In its concluding remarks the appeal court held:

'There have been many instances reported in the media in recent years of data breaches on a massive scale caused by either corporate system failures or negligence by individuals acting in the course of their employment. These might, depending on the facts, lead to a large number of claims against the relevant company for potentially ruinous amounts. The solution is to insure against such catastrophes; and employers can likewise insure against losses caused by dishonest or malicious employees.'[266]

The Court of Appeal refused Morrisons leave to appeal but it is understood that Morrisons will seek leave to appeal from the Supreme Court.

4.3 **Canada**

In Canada there are currently 38 separate statutes[267] regulating the collection and use of personal information. Statutory causes of action are provided by way of the following statutes:

1) Personal Information Protection and Electronic Documents Act, S.C. 2000, ch. 5

[264] *Various Claimants v Wm Morrison Supermarkets PLC* [2018] EWCA Civ 2239 at paragraph 41.
[265] *Various Claimants v Wm Morrison Supermarkets PLC* [2018] EWCA Civ 2239 at paragraph 76.
[266] *Various Claimants v Wm Morrison Supermarkets PLC* [2018] EWCA Civ 2239 at paragraph 78.
[267] E Dolden … et al. 'Current landscape of personal information and privacy liability in Canada' (February 2016) *Dolden Wallace Folick LLP* available at *http://www.dolden.com/wp-content/uploads/2016/06/166-Current-Landscape-of-Personal-Information-and-Privacy-in-Canada-February-2016.pdf,* accessed on 4 October 2018.

("PIPEDA") or the equivalent substantially similar provincial acts;

2) Privacy Act right of action for breach of privacy available in four provinces;[268] or

3) Canada's Anti-Spam Law.[269]

PIPEDA is the Canadian federal legislation regulating the private sector organisations in certain provinces. PIPEDA adopted the CSA International Privacy Code, being a national standard developed in conjunction with the private sector and based on the OECD principles, into law for the private sector. PIPEDA defines personal information as *'information about an identifiable individual.'*[270]

In Canada every province and territory has its own laws that apply to provincial and territorial government agencies and their handling of personal information. Some provinces have private-sector privacy laws that have been deemed *'substantially similar'* to PIPEDA. This means that those substantially similar laws apply to the particular province instead of PIPEDA. These provinces are Alberta, British Columbia and Quebec.

Section 3 of the PIPEDA states that the purpose of the PIPEDA is:

> *'The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.'*

For the purposes of this study the British Columbia Privacy Act [RSBC 1996] Chapter 373, will be analysed and discussed. Section 1 of the Privacy Act [RSBC 1996] Chapter

[268] These four provinces are British Columbia, Manitoba, Newfoundland and Labrador and Saskatchewan.
[269] E Dolden … et al. 'Current landscape of personal information and privacy liability in Canada' (February 2016) available at *http://www.dolden.com/wp-content/uploads/2016/06/166-Current-Landscape-of-Personal-Information-and-Privacy-in-Canada-February-2016.pdf,* accessed on 4 October 2018.
[270] Section 2(1) of PIPEDA.

373, creates the statutory tort of violation of privacy.[271] It reads:

> *'Violation of privacy actionable*
>
> *1 (1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.*
>
> *(2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.*
>
> *(3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.'*

Ultimately s 1 of the Privacy Act [RSBC 1996] Chapter 373, requires that the act leading to the breach of privacy be intentional, and proof of economic loss or other specific harm is not a pre-requisite for liability or damages.[272] Therefore a person whose privacy is breached in British Columbia has a right to sue only if the breach meets the elements of the statutory tort set out in the Act. While persons will not have to prove that they have suffered harm as a result of the breach, they will have to prove that the breach was wilful, without claim or right, and violated their reasonable privacy expectations.

In *Ari v Insurance Corporation of British Columbia* 2015 BCCA 468 ("*Ari*") the Court of Appeal for British Columbia was tasked with deciding whether certain portions of a proposed class action ought to have been struck. The plaintiff in this matter alleged, *inter alia*, that an employee of the defendant breached common law and statutory rights to privacy by improperly accessing the personal information held by the Insurance Corporation of British Columbia. The plaintiff sought to hold the Insurance Corporation of British Columbia vicariously liable for its employee's misconduct and

[271] E Dolden … et al. 'Current landscape of personal information and privacy liability in Canada' (February 2016) available at *http://www.dolden.com/wp-content/uploads/2016/06/166-Current-Landscape-of-Personal-Information-and-Privacy-in-Canada-February-2016.pdf,* accessed on 4 October 2018.
[272] Section 1 of the Privacy Act [RSBC 1996] Chapter 373.

alleged breach of the Privacy Act [RSBC 1996] Chapter 373.

The Insurance Corporation of British Columbia contended that s 1 of the Privacy Act [RSBC 1996] Chapter 373 does not permit it to be held liable for its employees wrongdoing. The Court of Appeal held that the Privacy Act [RSBC 1996] Chapter 373, did not exclude the imposition of vicarious liability on the employer and suggested that the principles of vicarious liability may be applied in the context of a breach of privacy by an employee just as they would to any other wrongful act of an employee.

The Court of Appeal did not evaluate the matter on its merits and the dispute essentially revolved around considering the test for striking out of pleadings. The matter therefore did not definitively answer the question of whether and when an employer is vicariously liable for the privacy breaches of its employees and the court stated that it was necessary for it to receive evidence in order to fairly address whether Insurance Corporation of British Columbia could be held vicariously liable.

The Court of Appeal provided the following reasons for its decision:

> *'[25] It is not clear that s. 1 of the Privacy Act should be interpreted as limited in the same fashion as the relevant provisions in Nelson. Section 1(1) states that "[i]t is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another". There is no language (as there was in Nelson) that clearly limits a plaintiff to recovery of damages from the person identified in s. 1(1). While, as the chambers judge observed, vicarious liability for acts of intentional and deliberate wrongdoing has generally been rejected, it is not unheard of (see: Lewis Klar, Tort Law, 5th ed. (Toronto: Carswell, 2012) at 682). To the extent that s. 1(1) of the Privacy Act requires deliberate wrongdoing, it is not per se incompatible with vicarious liability.*
>
> *[26] Although Nelson may provide, by analogy, a basis for denying the availability of vicarious liability, I cannot conclude that the chambers judge erred in finding the appellant's claim is on this basis, not bound to fail.*
>
> *[27] Alternatively, ICBC says that there is a policy argument which supports its*

position that there is no cause of action in vicarious liability. For policy reasons ICBC says, employers should not be held vicariously liable for wilful breaches of privacy under the Privacy Act.

[28] ICBC also contends that the question before the chambers judge was whether vicarious liability should be imposed due to policy considerations. It says that the appropriate question to ask is: should liability lie against a public body for the wrongful conduct of its employee, in these circumstances? The question necessarily demands some exploration of the evidence about the connection between ICBC's security procedures and the security lapse that occurred, as well as a weighing of the policy considerations involved. It is reasonable to conclude that a factual matrix is necessary in order to fairly address whether ICBC's conduct materially enhanced the possibility of committing the breach of privacy, and to determine the connection between the impugned conduct and ICBC's conduct. In other words, to clearly determine how public policy considerations affect the viability of the vicarious liability claim, some evidence is required.'[273]

This is the only Canadian decision which has considered whether an employer can be vicariously liable for a breach of the Privacy Act [RSBC 1996] Chapter 373[274] and due to the fact that the matter is still pending it can be submitted that Canadian courts have not directly decided whether vicarious liability may be extended to employers in respect of the privacy breaches of their employees.[275]

It would however seem that the decision in the *Ari* case is consistent with the recent decision in the United Kingdom in *Various Claimants v WM Morrisons* which holds that the test for vicarious liability of an employer for the wrongful acts of its employees is the same as it is for any other wrongful act of an employee.

[273] *Ari v Insurance Corporation of British Columbia* 2015 BCCA 468 paragraphs 25 to 28.
[274] K Zimmer 'Canada: Privacy Breach By Your Rogue Employee: Are You Liable?' (26 September 2018) available at http://www.mondaq.com/canada/x/739684/Data+Protection+Privacy/Privacy+breach+by+your+rogue+employee+Are+you+liable, accessed on 4 October 2018.
[275] K Zimmer 'Canada: Privacy Breach By Your Rogue Employee: Are You Liable?' (26 September 2018) available at http://www.mondaq.com/canada/x/739684/Data+Protection+Privacy/Privacy+breach+by+your+rogue+employee+Are+you+liable, accessed on 4 October 2018.

4.4 **Concluding remarks**

The ultimate decision of the High Court and the Court of Appeal in *Various Claimants v WM Morrisons* effectively achieved Mr Skelton's motive of punishing Morrisons by making it liable to its employees through no fault of its own.[276] This seems harsh in the circumstances especially given the fact that Langstaff J held that Morrisons had taken the appropriate measures to protect the claimants' data against misuse.[277]

Although British and Canadian legislation provides for a mechanism for employers to escape vicarious liability in circumstances where its employees breaches the provisions of the relevant legislation, when practically implemented it would seem that the courts have been inclined to hold the employers vicariously liable for such unlawful conducts on the part of its employees notwithstanding that they have taken appropriate steps to mitigate the risk of unlawful conduct occurring.

This is set to have far reaching consequences as employers are exposed to potential claims arising from the misuse of personal data by employees, even in circumstances where the employee has deliberately set out to harm the employer.

If the case of *Various Claimants v WM Morrisons* is to be followed an employer cannot evade liability by demonstrating that it implemented appropriate measures in accordance with data protection legislation. It would follow that the only option available to employers is to provide appropriate liability insurance against the risk of contraventions of data protection legislation by its employees.[278]

[276] *Various Claimants v Wm Morrisons Supermarket PLC* [2017] EWHC 3113 (QB) 2017 at paragraph 198.
[277] *Various Claimants v Wm Morrisons Supermarket PLC* [2017] EWHC 3113 (QB) 2017 at paragraph 82.
[278] See *Various Claimants v Wm Morrison Supermarkets PLC* [2018] EWCA Civ 2239 at paragraph 78 and D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 31.

Chapter 5: Conclusion and recommendations

5.1 Overview

> *'Worldwide, the ever-increasing surge of technology has brought with it a myriad of legal problems. South Africa is not immune to these.'*[279]

The motivation behind the analysis of POPIA is due to the fact that 2018 has marked a landmark year for data protection globally.[280] Rapid technological advancement has drastically increased the necessity for adequate data protection legislation in order to regulate the processing and dissemination of personal information.

The ultimate purpose of this chapter is to draw a conclusion as to the effect that statutory vicarious liability as created in terms of POPIA will have on employers, and to provide recommendations for the way forward by drawing and deriving measures from those adopted by foreign jurisdictions.

As precisely encapsulated by Britz:

> *'We are currently living in the so-called information age which can be described as an era were economic activities are mainly information based (an age of informationalization). This is due to the development and use of technology.'*[281]

The adoption of the GDPR and the DPA 2018 on 25 May 2018 provides a clear indication of how data legislation is continually responding to shifts in the technological landscape and is symbolic of how the technological world has fundamentally changed. In South Africa, POPIA delivers an essential framework in how responsible parties are to handle personal data and it clearly establishes data protection conditions that set out the minimum requirements for the processing of

[279] D van der Merwe 'Introduction' in D P van der Merwe… et al (2ed) *Information and Communications Technology Law* (2016) 1.
[280] See for example the enactment of the EU GDPR and the United Kingdom DPA 2018.
[281] J.J Britz 'Technology as a threat to privacy: ethical challenges to the information profession' (1996) 13(3) *Microcomputers for Information Management: Global Internetworking for Libraries* available at *http://web.simmons.edu/~chen/nit/NIT%2796/96-025-Britz.html,* accessed on 4 September 2018.

personal information. As technology has evolved the potential risk to privacy has grown. It is therefore essential that POPIA fulfils its mandate to safeguard the fundamental right to privacy as enshrined in the Constitution.

Various Claimants v WM Morrisons has increased public awareness of data protection issues worldwide as it highlights the wide reach of data protection. As it currently stands an employer can be liable for data breaches on the part of their employees even if the employer has taken appropriate measures to comply with the data protection legislation. Due to the fact that s 99(2) does not provide adequate defences[282] for an employer to evade liability for breaches of POPIA on the part of their employees, it would follow that POPIA will be faced with similar difficulties once fully operational.

5.2 **Observation**

The doctrine of vicarious liability provides an incentive to employers to exercise care in the selection, hiring, training and supervision of employees in order to prevent unlawful conduct on the part of their employees.[283] It is therefore comprehensible that an employer should evade liability in circumstances where the employer has eagerly exercised reasonable care and encouraged compliance with POPIA. O'Regan J corroborates this view by stating:

> *'There is a countervailing principle too, which is that damages should not be borne by employers in all circumstances, but only in those circumstances in which it is fair to require them to do so.'*[284]

The provisions of the Employment Equity Act and the Occupational Health and Safety Act expressly provide alleviation to employers that can prove that they did all that was

[282] Section 99(2) of POPIA does not provide an exemption to employers, being responsible parties that have taken reasonable measures to comply with POPIA.
[283] See O'Regan J in *NK v Minister of Safety and Security* [2005] ZACC 8; 2005 (6) SA 419 (CC); 2005 (9) BCLR 835 (CC) at 21:
'The rationale for vicarious liability is to be found in a range of underlying principles. An important one is the desirability of affording claimants efficacious remedies for harm suffered. Another is the need to use legal remedies to incite employers to take active steps to prevent their employees from harming members of the broader community.'
[284] *NK v Minister of Safety and Security* [2005] ZACC 8; 2005 (6) SA 419 (CC); 2005 (9) BCLR 835 (CC) at 21.

reasonably practicable to ensure that the employee would not act in contravention of the relevant legislation.[285] This relief is mirrored in the provisions of the GDPR, the DPA 1998, the DPA 2018 and the British Columbia Privacy Act [RSBC 1996] Chapter 373.[286]

It would appear that the South African courts have expressed the view[287] that employers that take all reasonable steps to prevent any unlawful act or omission on the part of their employees should not be held liable for any unlawful act or omission caused by their employees, however, the legislature seem to have overlooked this important provision when drafting POPIA, in particular s 99.

In terms of POPIA where an employee infringes a data subjects right to privacy and thereby breaches the provisions of POPIA, the employer will be held liable, whether or not there is negligence on the part of the employer.[288] The employer's liability extends to circumstances where the employee has purposely and maliciously sets out to harm the employer, has acted for their own gain, and has acted outside the course and scope of their employment.[289] Section 99(2) of POPIA does not enable an employer to escape being held vicariously liable even in circumstances where the employer is able to prove that it proactively took all reasonable and practicable steps to prevent a contravention of POPIA.

Although *Various Claimants v WM Morrisons* concerned data breaches that occurred prior to the application of the GDPR and the DPA 2018, the GDPR and the DPA 2018 expressly provide[290] that any person who has suffered material or non-material damage as a result of an infringement of the relevant legislation shall have the right to receive compensation for the damage suffered. Similarly, s 99(3)(a) of POPIA empowers the court to award payment of damages as compensation for patrimonial and non-

[285] Section 60(4) of the Employment Equity Act and s 37 of the Occupational Health and Safety Act.
[286] As analysed in chapter 4 of this study.
[287] See O'Regan J in *NK v Minister of Safety and Security* [2005] ZACC 8; 2005 (6) SA 419 (CC); 2005 (9) BCLR 835 (CC) at 21:
'There is a countervailing principle too, which is that damages should not be borne by employers in all circumstances, but only in those circumstances in which it is fair to require them to do so.'
[288] Section 99(1) of POPIA.
[289] See POPIA s 99(2) defences against an action for damages.
[290] Article 82 of the GDPR and s 169 of the DPA 2018.

patrimonial loss suffered by a data subject as a result of breach of the provisions of POPIA. These provisions will make it even easier for individuals to succeed with claims based on vicarious liability.

With numerous high profile data breaches having taken place in 2018, it will be interesting to see how the South African judiciary will deal with claims based on statutory vicarious liability in terms of POPIA once it is fully operational and whether or not the legislature will be inclined to amend s 99 of POPIA to bring it in line with the Employment Equity Act, the Occupational Health and Safety Act and foreign legislation in order to *'alleviate the plight of the employer without compromising any of the all-important objectives.'*[291]

5.3 Conclusion and recommendation

As accurately expressed by Roos:

> *'All in all the Act is an excellent piece of legislation and it is hoped that it will become fully operative soon.'*[292]

In light of the above it can be concluded that POPIA is a comprehensive and effective piece of legislation that aligns South African data protection to international standards and gives effect to the constitutional right to privacy by safeguarding personal information.

Section 99 of POPIA does however require some further consideration by the legislature as once POPIA is fully operational s 99 could be problematic and be deemed to be excessively one sided in favour of data subjects. The full impact of s 99 can only be thoroughly analysed once practically implemented and therefore the effective date for full promulgation of POPIA is eagerly anticipated.

---

[291] D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 32.

[292] A Roos 'Data Privacy Law' in D P van der Merwe… et al (2ed) *Information and Communications Technology Law* (2016) 478.

As submitted earlier in this study a new subsection, s 99(2)(A), should be inserted to include the following, namely:

> *(2)(A) Despite subsections (1) and (2), a responsible party will be exempted from liability, in whole or in part, if the responsible party proves that it is not responsible for the event giving rise to the breach and it did all that was reasonably practicable to ensure compliance with this Act.*

This insertion will provide adequate relief to employers that have done all that was reasonably practicable to ensure compliance with POPIA. This clause extends and goes further than that suggested by Millard and Bascerano in that it provides exemption from liability in circumstances where the employer was not responsible for the relevant breach of the provisions of POPIA. This straightforward addition will eliminate uncertainty that may arise in circumstances such as those presented in *Various Claimants v WM Morrisons* whereby an employee deliberately and maliciously sets out to harm the employer by breaching the provisions of POPIA

Bibliography

6.1 Primary sources

6.1.1 Cases

Absa Bank Ltd v Bond Equipment Pretoria (Pty) Ltd 2001 1 SA 372 (SCA).

Barkhuizen v Napier 2007 5 SA 323 (CC).

Bernstein and Others v Bester NO and Others 1996 (4) BCLR 449 (CC).

Bezuidenhout v Eskom 2003 3 SA 83 (SCA).

Booysen v Minister of Safety and Security [2018] ZACC 18.

Carmichele v Minister of Safety and Security and Another [2001] ZACC 22; 2001 (10) BCLR 995 (CC); 2001 (4) SA 938 (CC).

Carter & Co (Pty) Ltd v McDonald 1955 1 SA 202 (A).

Costa da Oura Restaurant (Pty) Ltd t/a Umdloti Bush Tavern v Reddy 2003 24 ILJ 1337 (SCA).

Country Cloud Trading CC v MEC, Department of Infrastructure Development, Gauteng [2014] ZACC 28.

Crown Chickens v Rieck 2007 *ILJ* 307 (SCA).

Ess Kay Electronics (Pty) Ltd v First National Bank of Southern Africa Ltd 2001 1 SA 1214 (SCA).

F v Minister of Safety and Security [2011] ZACC 37; 2012 (1) SA 536 (CC); 2012 (3) BCLR 244 (CC).

Feldman (Pty) Ltd v Mall 1945 AD 733.

Grobler v Naspers 2004 2 All SA 160 (C).

H v W [2013] 2 All SA 218 (GSJ).

Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and others: In re Hyundai Motor Distributors (Pty) Ltd and others v Smit NO and others 2001 (1) SA 545 (CC).

Jansen van Vuuren and another NNO v Kruger 1993 (4) SA 842 (A).

Jowell v Bramwell-Jones and others 2000 3 SA 274 (SCA).

NK v Minister of Safety and Security [2005] ZACC 8; 2005 (6) SA 419 (CC); 2005 (9) BCLR 835 (CC).

Messina Associated Carriers v Kleinhaus 2001 (3) SA 868 (SCA).

Minister of Finance v Gore 2007 1 SA 111 (SCA).

Minister of Justice and Constitutional Development and Others v Prince (Clarke and Others Intervening); National Director of Public Prosecutions and Others v Rubin; National Director of Public Prosecutions and Others v Acton (CCT108/17) [2018] ZACC 30.

Minister of Police v Rabie 1986 1 SA 117 (A).

Minister of Safety and Security v Jordaan 2000 (4) SA 21 (SCA).

Minister of Safety and Security v Morudu and Others 2016 (1) SACR 68 (SCA).

Minister van Veiligheid en Sekuriteit v Japmoco 2002 5 SA 649 (SCA).

Mistry v Interim National Medical and Dental Council and Others [1998] ZACC 10.

Mkize v Martens 1914 AD 382.

National Media Ltd v Jooste 1996 (3) SA 262 (SCA).

NK v Minister of Safety and Security 2005 26 *ILJ* 1205 (CC).

Ntsabo v Real Security CC 2003 24 ILJ 2341 (LC)

O'Keeffe v Argus Printing and Publishing Co Ltd [1954] 3 All SA 159 (C).

Pharmaceutical Manufacturers Association of SA and Another: In re ex parte President of the Republic of South Africa and Others 2000 (2) SA 674 (CC).

Piliso v Old Mutual Life Assurance Co (SA) Ltd and Others (2007) 28 ILJ 897 (LC).

R v Umfaan 1908 TS 62.

Rhodesian Printing and Publishing Co Ltd v Duggan and Another [1975] 2 All SA 125 (RA).

S v Bailey [1981] 1 All SA 338.

SA Broadcasting Corporation v McKenzie 1999 20 ILJ 1936 (LAC).

SA Railways & Harbours v Marais 1950 4 SA 610 (A).

Stein v Rising Tide Productions CC 2002 2 All SA 22 (C).

6.1.2 **Statutes**

Basic Conditions of Employment Act 75 of 1998.

Constitution of the Republic of South Africa, 1996.

Employment Equity Act 55 of 1998 (as amended).

Labour Relations Act 66 of 1995.

Occupational Health and Safety Act 85 of 1993 (as amended).

Protection of Personal Information Act 4 of 2013.

6.2 Secondary sources

6.2.1 Books

Basson, A. … et al. *Essential Labour Law* 4 ed Gauteng: Mace Labour Law Publications, (2005).

Burns, Y & Burger-Smidt, A *A Commentary on the Protection of Personal Information Act* Durban: LexisNexis, (2018).

Currie, I & De Waal, J *Bill of Rights Handbook* 6 ed Cape Town: Juta, (2013).

Davey, R & Dahms-Jansen, L *Social Media in the Workplace* Durban: LexisNexis, (2017).

De Stadler, E & Esselaar, P *A Guide to the Protection of Personal Information Act* Cape Town: Juta, (2015).

Neethling J, Potgieter JM & Visser PJ *Neethling's Law of Personality* 2 ed Durban: Butterworths, (2005).

Neethling, J, Potgieter, JM & Visser, PJ*, Neethling Potgieter Visser Law of Delict* 7 ed Durban: LexisNexis, (2015).

Papadopoulos, S & Snail, S *Cyberlaw@SA III: The law of the internet in South Africa* 3 ed Pretoria: Van Schaik, (2012).

Van der Merwe, DP. … et al. *Information and Communications Technology Law* 2 ed Durban: LexisNexis, (2016).

Woolman, S. … et al. *Constitutional Law of South Africa* Cape Town: Juta, (1996).

6.2.2 Journal Articles

Burchell, J 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13(1) *EJCL* 11.

Buys, M 'Protecting personal information: implications of the Protection of Personal Information (POPIA) Act for healthcare professionals' (2017) 107(11) *SAMJ* 954 – 956.

Calitz, K 'The close connection test for vicarious liability' (2007) 18(3) *SLR* 451 – 468.

Calitz, K 'Vicarious liability of employers: Reconsidering risk as the basis for liability' (2005) *TSAR* 215 – 235.

De Bruyn, M 'The Protection of Personal Information Act – Impact on South Africa' (2014) 13(6) *International Business and Economics Research Journal* 1316.

Edwards, JLJ 'Vicarious liability in criminal law' (1951) 14(3) *The Modern Law Review* 334 – 340.

Iyamu, T & Ngqame, Y 'Towards a conceptual framework for protection of personal information from the perspective of activity theory' (2017) 19(1) *South African Journal of Information Management* 1 – 7.

Jangara, BT & Bezuidenhout H ' Addressing emerging risks in transborder cloud computing and the protection of personal information: The role of internal auditors' (2015) 17(1) *SAJAAR* 11 – 24.

Kobrin, L ‘Vicarious liability: Easy to understand, difficult to adjudicate’ (2017) May *De Rebus* 28 - 29.

Le Roux, R 'Vicarious liability: revisiting an old acquaintance' (2003) *ILJ* 1879-1883.

Le Roux, R 'Sexual harassment in the workplace: Reflecting on *Grobler v Naspers'* (2004) *ILJ* 1897 – 1900.

Loots, BE 'Sexual harassment and vicarious liability: a warning to political parties' (2008) 19 *SLR* 143 - 169.

Luck, R ‘POPI- is South Africa keeping up with international trends?’ (2014) May *De Rebus* 44 - 46.

Magolego, N 'Personal data on the internet – can POPIA protect you?' (2014) *De Rebus* 20 – 23.

McQuoid-Mason, David 'Invasion of privacy: common law v constitutional delict – does it make a difference?' (2000) *Acta Juridica* 227 – 261.

Milo, D and Ampofo-Anti, O 'A not so private world' (2014) 14(9) *Without Prejudice* 30 – 32.

Millard, D and Botha, MM 'The past, present and future of vicarious liability in South Africa' (2012) *De Jure* 225 – 253.

Millard, D and Bascerano, EG 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19(1) *PELJ* 1 – 38.

Mischke, C and Beukes, V 'Vicarious liability: When is the employer liable for the wrongful acts of employees? (2002) *CLL* 11 – 17.

Neethling, J 'The concept of privacy in South African Law' (2005) 122(1) *SALJ* 18 – 28.

Neethling, J 'Vicarious liability of the State for rape by a police official' (2011) *TSAR* 186 – 191.

Neethling, J 'Features of the Protection of Personal Information Bill, 2009 and the law of delict' (2012) *THRHR* 241 – 255.

Nyoni, P. & Velempini, M 'Data protection laws and privacy on Facebook' (2015) 17(1) *South African Journal of Information Management* 1 – 10.

Perumall, A 'Problems in protecting personal information' (2013) 13(2) *Without Prejudice* 61 – 62.

Potgieter, J.M. 'Preliminary Thoughts on Whether Vicarious Liability Should be Extended to the Parent-Child Relationship' (2011) 32 *Obiter* 189 – 203.

Rautenbach, I.M. 'The conduct and interests protected by the right to privacy in section 14 of the Constitution (2001) *TSAR* 115 – 123.

Roos A 'Core principles of data protection law' (2006) 39(1) *CILSA* 102 – 130.

Roos A 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 400 - 437.

Roos, A 'Personal data protection in New Zealand: lessons for South Africa?' (2008) *PELJ* 61 – 109.

Scott, TJ 'Some reflections on vicarious liability and dishonest employees' (2000) *Acta Juridica* 265 – 279.

Whitcher, B 'Two roads to an employer's vicarious liability for sexual harassment: *S Grobler v Naspers Bpk en 'n Ander* and *Ntsabo v Real Security CC*' (2004) *ILJ* 1907 – 1924.

6.2.3 Online Sources

'POPI commencement date or POPI effective date starts the clock' *Michalsons*, 10 July 2018 available at *https://www.michalsons.com/blog/popi-commencement-date-popi-effective-date/13109,* accessed on 4 September 2018.

Britz, J.J 'Technology as a threat to privacy: ethical challenges to the information profession' (1996) 13(3) *Microcomputers for Information Management: Global Internetworking for Libraries* available at *http://web.simmons.edu/~chen/nit/NIT%2796/96-025-Britz.html,* accessed on 4 September 2018.

Giles, J 'Only do what is reasonably practicable to comply with POPIA' (23 May 2014) *Michalsons* available at *https://www.michalsons.com/blog/reasonably-practicable-to-comply-with-POPIA/13296*, accessed on 21 April 2018.

Van Wyk, J & Van Heerden, A 'The Protection of Personal Information Bill from an employment perspective' (17 September 2013) *Polity.org.za* available at *http://www.polity.org.za/article/the-protection-of-personal-information-bill-from-an-employment-perspective-2013-09-17,* accessed on 4 September 2018.

6.2.4 Reports and discussion papers

South African Law Reform Commission *Privacy and Data Protection* (Discussion paper 109, Project 124) Pretoria: SALRC, (2009).

6.2.5 Theses

Murray, S *The Extent of an Employer's Vicarious Liability when an Employee Act within the Scope of Employment* (LLB, North West University, 2012).

Naude, A *Data Protection in South Africa: the Impact of the Protection of Personal Information Act and Recent International Developments* (LLM thesis, University of Pretoria, 2014).

Reddy, M *An analysis of the Protection of Personal Information Act 4 of 2013 in the context of unsolicited electronic communications* (LLM thesis, University of KwaZulu-Natal, 2016).

Roos, A *The law of data (privacy) protection: A comparative and theoretical study* (LLD thesis, UNISA, 2009).

Van Eeden, AJ *The constitutionality of vicarious liability in the context of South Africa Labour Law: a comparative study* (LLM thesis, University of South Africa, 2014).

6.3 Foreign law

6.3.1 Cases

Ari v Insurance Corporation of British Columbia 2015 BCCA 468.

The Catholic Child Welfare Society and others (Appellants) v Various Claimants and The Institute of the Brothers of the Christian Schools (Respondents) [2012] UKSC 56.

Various Claimants v Wm Morrisons Supermarket PLC [2017] EWHC 3113 (QB) 2017

Various Claimants v Wm Morrison Supermarkets PLC [2018] EWCA Civ 2239.

6.3.2 Statutes

An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q.

Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data No 108 Strasbourg, 1981.

Data Protection Act 1998.

Data Protection Act 2018.

European Union (EU) Directive No. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

General Data Protection Regulation (EU) 2016/679 ("GDPR").

Organisation for Economic Co-operation and Development "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" Paris, 1981.

Personal Information Protection and Electronic Documents Act, S.C. 2000.

Personal Information Protection Act, S.A. 2003.

Personal Information Protection Act, S.B.C. 2003.

Privacy Act [RSBC 1996] Chapter 373.

6.3.3 Books

Bennett, J '*Regulating Privacy: data protection and public policy in Europe and the United States* Cornell University Press (1992).

Young, JB *Privacy* John Wiley & Sons (1978).

6.3.4 Journal Articles

Gross, H 'The concept of privacy' (1967) *New York University Law Review* 34 – 54.

6.3.5 Online Sources

Dolden, E. … et al. 'Current landscape of personal information and privacy liability in Canada' (February 2016) *Dolden Wallace Folick LLP* available at *http://www.dolden.com/wp-content/uploads/2016/06/166-Current-Landscape-of-Personal-Information-and-Privacy-in-Canada-February-2016.pdf,* accessed on 4 October 2018.

Lamb, K 'UK: Introducing the Data Protection Act 2018!' (6 June 2018) *Mondaq* available at http://www.mondaq.com/uk/x/708140/data+protection/Introducing+The+Data+Protection+Act+2018, accessed on 4 October 2018.

Zimmer, K 'Canada: Privacy Breach By Your Rogue Employee: Are You Liable?' (26 September 2018) *Mondaq* available at http://www.mondaq.com/canada/x/739684/Data+Protection+Privacy/Privacy+breach+by+your+rogue+employee+Are+you+liable, accessed on 4 October 2018.

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

3 September 2018

Ms Cammrynn-Lee Larsen 216076634
School of Law
Howard Campus

Dear Ms Larsen

Protocol reference number: HSS/1402/018M
Project title: Data privacy protection in South Africa: An Examination of the Protection of Personal Information Act no.4 of 2013(POPI) and how it proposes to safeguard the fundamental right to privacy

FULL APPROVAL – No Risk/Exemption Application

In response to your application received 11 January 2018, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol has been granted **FULL APPROVAL.**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment /modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

.....
Professor Shenuka Singh (Chair)
Humanities & Social Sciences Research Ethics Committee

/pm

cc Supervisor: Lee Swales
cc. Academic Leader Research: Dr Shannon Bosch
cc. School Administrator: Ms Robynne Louw/Mr P Ramsewak

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

08 February 2019

Ms Cammrynn-Lea Larsen (216076634)
School of Law
Howard College Campus

Dear Ms Larsen,

Protocol reference number: HSS/1402/018M
New project title: Data privacy protection in South Africa: An analysis of vicarious liability in light of the Protection of Personal Information Act No. 4 of 2013 ("POPIA")

Approval Notification – Amendment Application

This letter serves to notify you that your application and request for an amendment received on 10 October 2018 has now been approved as follows:

- Change in Title

Any alterations to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form; Title of the Project, Location of the Study must be reviewed and approved through an amendment /modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for period of 3 years from the date of original issue. Thereafter Recertification must be applied for on an annual basis.

Best wishes for the successful completion of your research protocol.

Yours faithfully

.....
Dr Shamila Naidoo (Deputy Chair)

/ms

cc Supervisor: Lee Swales
cc Academic Leader Research: Dr Freddy Mnyongani
cc Post Graduate Administrator: Mr Pradeep Ramsewak

Humanities & Social Sciences Research Ethics Committee
Dr Rosemary Sibanda (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za