# THE RIGHT TO PRIVACY AND IDENTITY ON SOCIAL NETWORK SITES: A COMPARATIVE LEGAL PERSPECTIVE

by

MILTON THEMBA SKOSANA

submitted in accordance
with the requirements for the degree of

MASTERS OF LAWS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR

PROFESSOR ANNELIESE ROOS

2016

DECLARATION

Student number: 35612053

I, **MILTON THEMBA SKOSANA** declare that **THE RIGHT TO PRIVACY AND IDENTITY ON SOCIAL NETWORK SITES: A COMPARATIVE LEGAL PERSPECTIVE** is my own work and that all the sources I have used or quoted have been indicated and acknowledged by means of complete references.

_____ _____

Signature Date

# PREFACE

I should like to thank my Heavenly Father for the strength not to give up during the writing of this dissertation. I thank, too, my earthly fathers Flommy and Raynond, for believing in me. My late mother, Dorcas Sisi, you left me at the beginning of this journey, I know how proud you are of me. And to my partner Sonto, I know studies may bring distance in a relationship, but thank you for pushing me to finish. My two lovely sons Ndumiso and Musa, I dedicate this dissertation to your success in your own career paths.

And last but not least thank you to Prof Anneliese Roos for her guidance and patience.

**TABLE OF CONTENT**

## SUMMARY

This study focuses on the use of Social Network Sites (SNSs) and certain personality rights (specifically the right to privacy and the right to identity) that may be infringed by this use. The study also discusses data protection law as the protection of the rights to privacy and identity are interlinked with data protection in that data protection assumes importance when there is processing of personal information on SNSs.

The study seeks to determine whether South African law provides adequate protection for the interests that form the object of these personality rights, and highlights certain shortcomings, particularly in the context of SNSs. It also suggests solutions where there are shortcomings by learning from other jurisdictions. Related issues investigated are: who should be held responsible for the user-generated content uploaded on SNSs; the role of the Internet Service Provider (ISP); and how to deal with anonymous defendants.

KEYWORDS

Anonymous user; discovery; data law; protection of personal information; Social Network Sites; social media; right to privacy; right to identity; Internet Service Provider liability

## List of Abbreviations

| | |
|---|---|
| ACHPR | African Charter on Human and People's Rights |
| ACRWC | African Charter on the Rights and Welfare of the Child |
| AC | Law Report Appeal Cases |
| AD | Appellate Division |
| AJA | Acting Judge of Appeal |
| AJP | Acting Judge President |
| ALBA | Constitutional and Administrative Law Bar Association |
| All ER | All England Law Reports |
| All SA | All South African Law Reports (LexisNexis) |
| AIP | Association of Independent Publishers |
| APEC | Asia-Pacific Economic Cooperation |
| Apps | Applications |
| art | article |
| ASEAN | Association of Southeast Asian Nations |
| AU | African Union |
| Cal | California |
| CC | Constitutional Court |
| CCMA | Commission for Conciliation, Mediation and Arbitration |
| CDA | Communication Decency Act |
| CILSA | Comparative and International Law Journal of Southern Africa |
| CJ | Chief Justice |
| CJEU | Court of Justice of the European Union |
| DPA | Data Protection Authority |
| DC | District of Columbia |
| D Kan | District of Kansas |

| | |
|---|---|
| DPR | District of Puerto Rico |
| DSRMR | Digital Security and Risk Management Recommendation |
| EC | European Council |
| ECHR | European Convention on Human Right |
| ECtHR | European Court of Human Rights |
| ED Pa | Eastern District of Pennsylvania |
| EHRR | European Human Rights Reports |
| EU | European Union |
| EWHC | England & Wales High Court |
| FCJ | Forum of Community Journalists CPD |
| Fn | footnote |
| Ga | Georgia |
| GNP | North Gauteng High Court, Pretoria |
| GSJ | South Gauteng High Court, Johannesburg |
| ICJ | International Court of Justice |
| ICCPR | International Covenant on Civil and Political Rights |
| ICESCR | International Covenant on Economic, Social and Cultural Rights |
| ILJ | Industrial Law Journal |
| Ill App | Illinois Appellate Court |
| *BYU Int'l L & Mgmt Rev* | *Brigham Young University International Law & Management Review* |
| ISP(s) | Internet Service Provider(s) |
| J | Judge |
| JA | Judge of Appeal |
| KZD | KwaZulu-Natal High Court, Durban |
| KZP | KwaZulu-Natal High Court, Pietermaritzburg |
| LAWSA | Law of South Africa |
| Minn | Minnesota |
| MPASA | Magazine Publishers Association of South Africa |
| NASA | Newspaper Association of South Africa |
| ND Cal | Northern District of California |

| | |
|---|---|
| ND Ga | Northern District of Georgia |
| OAU | Organization of African Unity |
| OECD | Organization for Economic Cooperation and Development |
| PCSA | Press Council of South Africa |
| PER | Potchefstroom Electronic Law Journal |
| POPI | Protection of Personal Information Act |
| QB | Law Reports Queen's Bench |
| s | section |
| SALR | South African Law Reports |
| SALJ | South African Law Journal |
| SALRC | South African Law Reform Commission |
| SA Merc LJ | South African Mercantile Law Journal |
| SANEF | South African National Editors' Forum |
| SCA | Supreme Court of Appeal |
| SCA Act | Stored Communications Act |
| SDNY | Southern District of New York |
| SNS(s) | Social Network Sites |
| TSAR | Tydskrif vir die Suid-Afrikaanse Reg |
| UDHR | Universal Declaration of Human Rights |
| UKHL | United Kingdom House of Lords |
| UN | United Nations |
| URL | Uniform Resource Locater |
| US | United States Supreme Court |
| USC | United States code |
| Va | Virginia |
| WLR | Weekly Law Reports |

# Chapter 1

# Introduction

## 1.1 BACKGROUND

In this study I focus on the use of Social Network Sites (SNSs)[1] and certain personality rights (specifically the right to privacy and the right to identity) that may be infringed through the use of SNSs.

SNSs are easy to use and enable one to meet old and new friends online. They are often free. Williams[2] highlights the following reasons why people use SNSs: for social interaction; for information seeking and sharing; to pass the time; for entertainment and relaxation; as a convenient and easy means of communication; for the expression of opinion; for surveillance of others; or to or obtain knowledge about others. SNSs are arguably the cheapest[3] and most widely used of the electronic forms of communication.[4] Since their inception, SNSs have narrowed the distance between people – it has become possible to communicate with friends, family, and even strangers from around the world as frequently as one wishes.

Technological innovation often brings convenience or improvement to life; on the other hand, that very convenience and improvement may herald a minefield of legal consequences. Therefore, if it is adequate to protect society's needs, the law needs to adapt to technological developments.[5] The South African courts, like other courts worldwide, have already pronounced on SNSs in a number of cases.[6]

---

1 Social Network Sites are defined in para 2.3 below. The concept of SNSs, their development and their functionality are explained in ch 2.

2 Williams 2013 *Qualitative Market Research: An International Journal* 364-5.

3 Ibid 363.

4 The Protection of Personal Information Act 4 of 2013, s 1 defines 'electronic communication' to mean any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

5 Roos (2012) *SALJ* 375.

6 *Dutch Reformed Church Vergesig Johannesburg Congregation and Another v Rayan Soknunan t/a GloryDivinee World Ministries* 2012 (6) SA 201 (GSJ); [2012] 3 All SA 322

My study is based on the following assumptions: that the Internet is an important medium of communication; that people retain their personality rights when using the Internet (and specifically SNSs); and that the law must protect the right of those using the Internet and SNSs. If this is the case, it follows that where the personality rights of users or non-users have been infringed on an SNS, liability should follow.

I have limited the study to the protection of the right to privacy and the right to identity in the context of SNSs. The delictual perspective is the focal point of this discussion. I focus on delicts that cause injury to personality (*iniuria)* on SNSs.[7] An *iniuria* to personality occurs where there is an intentional and wrongful infringement of a personality right. These personality rights are protected under the *actio iniuriarum*. Therefore, a person may sue for personality-right infringement relying on the *actio iniuriarum.* The *actio iniuriarum* protects injury to the *corpus* (bodily integrity), *fama* (good name or reputation), and *dignitas* (all personality interests apart from the *corpus* or *fama*). The rights to privacy and identity are therefore part of the wider concept of *dignitas*. Both natural and juristic persons have personality rights.[8] I have, however, limited my study to the personality rights of natural persons and refer only briefly to the position of juristic persons.

Protection of the rights to privacy and identity may be interlinked with data protection.[9] Data protection enters the picture when there is processing of personal information on SNSs. Both the user of an SNS and the Internet Service Provider (ISP) which provides the platform on which the SNS operates, may process personal information. I therefore also refer to data protection in the context of SNSs where it is relevant to do so.

As the study focusses on the private-law protection of the two mentioned personality rights, identity theft will not be investigated. Identity theft falls outside the scope of private law and it is dealt with under public law (specifically criminal law).

---

(GSJ); *Heroldt v Wills* 2013 (2) SA 530; 2013 (5) BCLR 554 (GSJ); [2013] 2 All SA 218 (GSJ); *Isparta v Richter and Another* 2013 (6) SA 529 (GNP); *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* 2012 (5) SA 604 (KZD); *M v B* 2015 (1) SA 270 (KZP); *Harvey v Niland and Others* 2016 (2) SA 436 (ECG).

7 Neethling, Potgieter & Visser *Law of Delict* 5.

8 See para 3.4 below.

9 See Neethling, Potgieter & Visser *Law of Personality* 270-1.

## 1.2 RESEARCH PROBLEM AND PURPOSE OF STUDY

The rights to privacy and identity are affected when users communicate or share personal information on SNSs. Often users post large amounts of information about themselves or others on SNSs;[10] this may lead to the infringement of person's right to privacy or to identity. The right to a good name (*fama*) is often also involved but will, for purposes of this dissertation, not be considered in detail. My research is limited to actions for infringement of the rights to privacy and the right to identity.

In this study I seek to establish whether South African law provides adequate protection for the interests that form the object of the rights to privacy and identity, and to highlight shortcomings, particularly in the context of SNSs. I also aim to suggest solutions for the shortcomings identified by drawing on the experience of other jurisdictions. Other related questions that I investigate are: who should be held responsible for the user-generated content uploaded on SNSs? the role of the ISP; and how to deal with anonymous defendants.

## 1.3 RESEARCH METHOD

This dissertation takes the form of a literature study, based largely on legislation, books, journal articles, case law, and Internet sources. I also consider the historical background, development, and current issues relating to SNSs to provide a basis for the study.

I adopted comparative approach as comparative law is helpful in gaining a better understanding of our own national (South African) law and may provide pointers to improve it.[11] Furthermore, the goals of legal comparison as a science are to identify the differences between legal models and to contribute to the knowledge of these models.[12] The Internet is intrinsically international in nature. One cannot analyse the

---

10 Kosta, Kalloniatis & Gritzalis 2010 *Transforming Government: People, Process and Policy* 194.

11 David & Brierley *Major Legal Systems* 6.

12 Samuel *Comparative Law Theory and Method* 45.

position in South Africa without taking note of the international situation – especially the position in the USA where SNSs originated and where many of their headquarters are located. When dealing with data protection, one cannot ignore the position in the European Union (EU).[13] With this in mind, I have elected to consider the following legal systems: the United States of America (United States); the European Union; and the UK as an example of a European country subject to the EU data protection regime. I also consider various international instruments.

## 1.4 PRELIMINARY DEFINITIONS OF KEY TERMS

In this section I provide preliminary definitions of certain of the key terms frequently used in the dissertation. Certain of these terms are addressed in greater detail in the body of the dissertation.

**Social Network Sites:** According to Boyed, these are "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site." [14]

**Social Media:** "Includes the various online technology tools and forms of electronic communication via the Internet, which include websites for social networking and micro blogging through which users create online communities to share information, ideas, personal messages, and other content".[15]

**Internet Service Provider:** "A company that provides subscribers with access to the Internet".[16]

**Personal information:** "Information relating to an identifiable, living, natural person, and, where applicable, an identifiable, existing juristic person, including, but not limited to: information relating to the race, gender, sex, pregnancy, marital status,

13 Abdulrauf *Data Privacy in Nigeria*12.
14 Boyd & Ellison 2007 *J Comput-Mediat Comm* 11.
15 Films and Publications Amendment Bill [B 37- 2015] s 1.
16 https://www.oxforddictionaries.com/ (date of use: 28 September 2016).

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; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; 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; the views or opinions of another individual about the person; and 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".[17]

**Processing:** "Any operation or activity, or any set of operations, whether by automatic means or not, which concerns personal information, including: the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure or destruction of information". [18]

**Data controller:** Means "any person who by electronic means requests, collects, collates, processes, or stores personal information from or in respect of a data subject".[19] (Also referred to as the responsible party.)[20]

**Data subject:** Means "any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored".[21] (Data subjects include both users and non-users of SNSs if their personal information is processed by the data controller.)

**Internet:** Means "the interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof". [22]

---

17 Protection of Personal Information Act 4 of 2013 s 1.
18 Act 4 of 2013 s 1.
19 Electronic Communications and Transactions Act 25 of 2002 s 1.
20 Act 4 of 2013 s 1.
21 Ibid.
22 Act 25 of 2002 s 1.

**Third party:** In relation to a service provider, a third party means "a subscriber to the service provider's services, any other user of the service provider's services, or a user of information systems". [23]

**Web page:** Means "a single, usually hypertext, document on the World Wide Web that can incorporate text, graphics, sounds, etc".[24]

**Web site:** Means "any location on the Internet containing a home page or web page".[25]

## 1.5 OUTLINE OF CHAPTERS

In Chapter 2 I discuss SNSs as a concept and explain their functionality. I also provide a brief historical background to the development of SNSs and describe a few of them. I also highlight that not only users of SNSs are affected by the challenges and threats they pose, but that non-users too may fall prey to the negative aspects of SNSs.

Chapter 3 focuses on South African law regarding the personality rights to privacy and identity. In the chapter I consider the historical backgrounds of these two personality rights, and examine how they are recognised and protected under South African law. Common law, constitutional law, and legislation are also discussed. I further examine the possible grounds of justification which exclude the wrongfulness of infringing conduct, and explore the infringement of these personality rights in the context of SNSs and possible grounds of justification applicable in this regard. The procedural challenges where either privacy or identity has been infringed in the context of SNSs are also addressed. Finally, I consider the possible remedies available to the plaintiff whose personality rights have been infringed on an SNS.

In Chapter 4 I offer a comparative analysis by discussing the legal system of the United States of America. My focus is on the recognition, protection, and regulation of rights to privacy and identity in the United States. I examine various sources at

23 Ibid s 1.
24 http://www.dictionary.com/browse/web--page?s=t (date of use: 28 September 2016).
25 Ibid s 1.

both Federal and State levels – specifically, constitutional law, legislation, common law, and case law.

In Chapter 5 I discuss some of the important documents relating to the protection of the rights to privacy and identity in the context of SNSs issued by international organisations and the European Union (EU). The chapter is presented in three parts. The first deals with documents issued by international organisations which have contributed to the development and protection of the right to privacy and data protection. The second part focuses on EU legal instruments in this area. Lastly, the chapter explores the legal position in the United Kingdom (UK) as an example of the application of EU law in a particular EU member state. Some of these documents are human rights documents which treat the right to privacy and the right to dignity (encompassing the right to identity) as fundamental human rights. However the majority of the legal instruments that I discuss deal with data protection. Data protection law regulates the protection of personal information when that information is processed and, therefore, in essence protects a person's right to privacy and to identity.

In Chapter 6 I present my conclusions and offer recommendations.

# Chapter 2

# Social Network Sites (SNSs)

## 2.1 INTRODUCTION

In this chapter I discuss the concept of Social Network Sites (SNSs) and explain what they are and how they function. The following framework is used: a brief historical background to the development of SNSs; the nature of SNSs is explained and a description is given of SNSs in general; the use of SNSs is examined; finally, a description of the functionality and usage of specific SNSs is given.

## 2.2 A BRIEF HISTORICAL BACKGROUND TO THE DEVELOPMENT OF SNSs

The first SNS to be developed was SixDegrees.com which was launched in 1997. It was located in New York and was based on the current Web 2.0 format.[1] It was named after the concept known as 'six degrees of separation'[2] and allowed users to list friends, family members, and acquaintances both on the site and externally. In addition, it invited external contacts to join the site. Its main purpose was to create a charitable social network and inspire participants to donate to charities online. The popularity of SNSs increased dramatically with the launch of Friendster.com in 2002.[3] Friendster was used for dating and discovering new events, bands, and hobbies. This website was created to compete with Match.com and other dating sites.[4]

1 Boyd & Ellison 2007 *J Comput-Mediat Comm* 214. For an explanation of the concept Web 2.0 see para 2.3 below.

2 Ibid.

3 Grimmelmann 2009 *Lowa Law Review* 1144.

4 Boyd "Friendster and Publicly Articulated Social Networking" 2004 (Vienna, Austria) available at http://delivery.acm.org/10.1145/990000/986043/p1279-boyd (date of use: 20 September 2016).

Today there are many recognised SNSs, both nationally and internationally. Amongst the leading SNS are Facebook, WhatsApp, QQ, Facebook Messenger, Q Zone, We Chat, Instagram, Twitter, Google+, Linkedin, Pinterest, BBM, Skype, and many more.[5] Facebook is predominantly referred to in this study as an example. According to the 'Digital in 2016' report,[6] WhatsApp, a rapidly expanding cross-platform mobile messaging company, was the top active social platform in South Africa, followed by Facebook. In 2014 Facebook announced that it had reached a definitive agreement to acquire WhatsApp for approximately $16 billion, including $4 billion in cash and approximately $12 billion in Facebook shares.[7]

Facebook was launched in 2004 by Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, and Chris Hughes. It was originally termed 'The Facebook.com'.[8] Membership was initially restricted to students at Harvard College, but was later extended to include anybody with a valid e-mail address.[9] The website is free of charge to users and generates revenue from advertising, such as banner advertisements (banner ads).[10] Facebook created public search listings on Google and Bing in 2007 to enable users to find other friends or users using public search engines.[11]

---

5 Kemp "Digital in 2016" available at http://wearesocial.com/uk/special-reports/digital-in-2016 (date of use: 6 August 2016).

6 Ibid.

7 "Facebook to acquire WhatsApp" available at //newsroom.fb.com/news/2014/02/facebook-to-acquire-whatsapp/ (date of use: 10 August 2016).

8 Colleges and Universities in the United States often publish official and unofficial books listing their students, faculty, or staff, together with pictures and limited biographical data. Mark Zuckerberg, while a sophomore at Harvard University, created an unofficial online face book on the website 'thefacebook.com', this used photos taken from Harvard house-based face books, using the photos [student faces] in a system to rate the attractiveness of students. See http://en.wikipedia.org/wiki/Face_book (date of use: 6 August 2016).

9 Boyd & Hargittai 2010 *First Monday* available at http://firstmonday.org/ (date of use: 8 August 2016).

10 Banner ads refer to a form of advertising on the World Wide Web (WWW). They function in the same way as traditional advertisements: notifying consumers of a product or service; and presenting reasons why the consumer should choose the product in question. Web banners differ from regular advertisements in that the results of advertisement campaigns may be monitored in real-time and may be targeted to the viewer's interests. See http://en.wikipedia.org/wiki/Web (date of use: 06 August 2016). Facebook generates most of its income through targeted advertising.

11 Sullivan "Facebook Opens Profiles To Tap Into Google Traffic, While Google Grabs Facebook's News Feed Idea" available at http://searchengineland.com/facebook-opens-profiles-to-tap-into-google-traffic-while-google-grabs-facebooks-news-feed-idea-12096 (date of use: 08 September 2016).

Facebook had 1,71 billion monthly active users as of June 2016.[12] It is estimated that somet 84,5 per cent of Facebook users are outside the United States and Canada.[13] There are 1,03 billion people accessing Facebook through their mobile devices.[14]

In 2016 there were close on thirteen million active Facebook users in South Africa.[15] In this context 'active registered user' means a user who has logged into Facebook at least once in the previous 30 days (the so-called 'monthly active user').[16] An analysis of the demographics of South Africa reflects that 20 to 29 year olds form the largest group of users on Facebook, namely 41 per cent; followed by 30 to 39 year olds who make up 21 per cent of all SA users on Facebook.[17] According to the executive summaries in the South African 'Social Media Landscape' reports, the number of active users in South Africa has risen to thirteen million, up from twelve million active users in 2015.[18]

MySpace became the most popular social networking site in the United States, a position that it held throughout 2007 and for part of 2008. In April 2008, according to comScore,[19] MySpace was overtaken internationally by its main competitor, Facebook.[20] Amongst the first users of MySpace included musicians and bands, who may have heard about it in the first place from the website's founders, who were active in the Los Angeles area.[21] Musicians used it to establish a free online

12 See http://newsroom.fb.com/company-info/ (date of use: 20 September 2016).

13 Ibid.

14 Ibid.

15 "South African Social Media Landscape 2016: Executive summary" available at

16 www.facebook.com/editaccount (date of use: 08 September 2016). People who access or use Facebook on their mobile devices are reported to be twice as active on Facebook than non-mobile users.

17 Kemp "Digital in 2016" available at http://wearesocial.com/uk/special-reports/digital-in-2016 (date of use: 21 December 2016).

18 "South African Social Media Landscape 2015 & 2016: Executive summary" available at

19 http://www.comscore.com/About_comScore (date of use: 10 September 2016). comScore is a global leader in measuring the digital world and the preferred source of digital marketing information.

20 This is based on the monthly number of unique visitors. See http://en.wikipedia.org/wiki/Myspace (date of use: 10 September 2016).

21 Weaver & Morrison *Social Networking* 98. The authors note that the idea of 'sharing media' is at the core of MySpace, which later extended to the sharing of music.

presence, to post performance dates, and to communicate with their fans.[22] MySpace was created by Tom Anderson and Chris De Wolfe.[23]

In South Africa, Mxit (pronounced as *'mix it'*) was the leading SNS. It has been overtaken by 2Go which boasted 10,5 million active users in August 2013.[24] Mxit is a free instant messaging[25] application developed by the South African based Mxit Lifestyle (Pty) Limited. Mxit runs on devices including feature phones, Android, BlackBerry, IPhone, iPad, Windows phone, and tablets.[26] Launched in 2006, it operates through Internet protocol to exchange messages.[27] MXit is primarily a Java-based[28] mobile application which gives users the functionality to exchange instant messages; it is thus light of data.[29] In March 2012, Mxit had almost 45 million registered users and an average of ten million active users. This made Mxit the largest SNS in South Africa at that time.[30] In 2014, it was reported that Mxit had 7,4 million monthly active users of which 6,3 million were in South Africa.[31] Although it was launched in South Africa, Mxit also has an international following. The international demographics show that the site has 5,5 million registered users internationally, with an average of 633 373 active international users.[32] It operates in many African and international markets. African markets include Kenya, Lesotho, Namibia, Nigeria and Swaziland. International markets in which Mxit operates include Malaysia, India, Indonesia, the United Kingdom, the United States, Brazil, France, Germany, Italy, Portugal and Spain.[33]

---

22 See http://en.wikipedia.org/wiki/Myspace (date of use: 10/09/2016).

23 Chatfield *Myspace.com Handbook* 39.

24 "South African Social Media Landscape 2014: Executive summary" available at www.worldwideworx.com (date of use: 20 December 2016).

25 Wikipedia defines 'instant messaging' as a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared clients. See http://en.wikipedia.org/wiki/Instant_messaging (date of use: 10 September 16).

26 See www.wikipedia.org/wiki/MXit (date of use: 12 September 2016).

27 Chicona & Chicana 2008 *Southern African Journal of Information and Communication* 43.

28 Java is a programming language and computing platform first released by Sun Microsystems in 1995. There are many applications and websites that will not work unless Java has been installed, and more are created every day. Java is fast, secure, and reliable. See https://java.com/en/download/faq/whatis_java.xml (date of use: 16 September 16).

29 See http://get.mxit.com/about/ (date of use: 16 September 2016).

30 Ibid.

31 "South Africa Social Media Landscape 2014: Executive summary" available at www.worldwideworx.com (date of use: 20 December 2016).

32 Ibid.

33 Ibid.

## 2.3 DEFINING, ANALYSING AND DESCRIBING SNSs

The internet is a fast-growing industry and has provided ample opportunities for subsidiary industries linked to Internet usage or development.[34] The development of the Internet started from the so-called Web 1.0[35] technology, and currently uses Web 2.0[36] technology. With regard to Web 1.0 technology, users played a passive role, in that it allowed them only to view and retrieve information. The current Web 2.0 is more interactive and also allows users to become contributors to the user-generated content.[37]

The focus of this study is on the current Web 2.0 technology. The term Web 2.0 is an umbrella term for web-based software such as blogs, wikis, social networking, and media-sharing sites.[38] Tim O'Reilly was the first to coin the term 'Web 2.0'. Web 2.0 laid a foundation for the development of Social Network Services (SNSs).[39]

The evolution of the Internet has changed the way people communicate and socialise. Advances in technology during the past decade have made it possible to use electronic communication tools to create social network applications.[40] Socialising is, and has always been, part of most people's lives. Therefore, social networking existed long before the dawn of computers and the Internet. It has always

---

34 Brown *Success Secrets* 14 gives an account of the impact of social media on the Internet industry and other related fields. See www.books.google.co.za (date of use: 16 September 2016).

35 Web 1.0 refers to the first stage of the World Wide Web (WWW) linking web pages with hyperlinks. See http://en.wikipedia.org/wiki/Web_1.0 (date of use: 16 September 2016).

36 Davies & Merchant *Learning and Social Participation* 3. The term Web 2.0 does not refer to anything as specific as new hardware or a reconfiguration of the Internet, it is a term that attempts to highlight a new wave and the increased volume of users who have developed new ways of using digital technology to interact with others.

37 Graham & Balachander 2008 *First Monday* available at http://firstmonday.org/article/view/2125/1972 (date of use: 20 September 2016).

38 Seppa "The future of social networking" available at www.cse.tkk.fi/en (date of use: 20 September 2016); Wellman 2001 *Computer and Science* 2031, notes that this concept is not entirely foreign as computer networks in their nature are inherently social networks. Available at http://www.sciencemag.org (date of use: 20 September 2016).

39 Anderson "What is Web 2.0? Ideas, technologies and implications for education" available at http://www.jisc.ac.uk/whatwedo/topics/web2.aspx (date of use: 20 September 2016).

40 Miltiadis & Patricia *Social Web Evolution* 57.

been a term used in a social, political, or business context. Weaver and Morrison express this idea as follows:

> Social networking is a concept that has been around much longer than the Internet or even mass communication. People have always been social creatures; our ability to work together in groups, creating value that is greater than the sum of its parts, is one of our greatest assets.[41]

Papadopoulos[42] defines 'online social networking' sites as websites the main purpose of which is to act as a link between users through the use of computer software to build online social networks. Boyd and Ellison[43] define social network sites as "web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system". This definition is widely accepted by scholars.[44]

It is trite that the nature and purpose of each SNS may vary from site to site. Grimmelmann points out that Boyd and Ellison's definition highlights three important aspects of SNSs: the creation of identity; of relationships; and of community.[45] Morrison and Weaver highlight the following characteristics of MySpace and Facebook:

> MySpace is a peer and media-based SNS where members can create their own mini websites containing pictures and profile information such as age and interests.

---

41 Weaver & Morrison *Social Networking* 97; also see Seppa "The future of social networking" Seminar on Internetworking 2008 available at cse.tkk.fi/en/publications/B/1/papers (date of use: 21 December 2016).

42 Papadopoulos 2009 *Obiter* 32.

43 Boyd & Ellison 2008 *J Comput-Mediat Comm* 211; Roos 2012 *SALJ* 383-5.

44 Roos 2012 *SALJ* 383; Papadopoulos 2009 *Obiter* 33; Beer 2008 *J Comput-Mediat Comm* 518.

45 Grimmelmann 2009 *Iowa Law Review* 1143. He further notes the links between these aspects: the first prong, 'profiles' emphasises *identity* – users create profiles that represent them. The second prong, 'contacts' emphasises *relationships* – users establish one-to-one connections with others. The third prong, 'traversing lists of contacts' emphasises *community* – users occupy a specific place among their peers. Beer 2008 *J Comput-Mediat Comm* 518, 520, disagrees with the proposal by Boyd and Ellison that researchers should use the term 'social network sites' rather than 'social networking sites'. He argues, first of all, that the former is too broad and means too many things and would lose the fine distinction that separates sites like YouTube from Facebook. Second, he argues against what he sees as Boyd and Ellison's artificial segregation of online and offline life, especially with respect to social interactions and friends. With SNS in the cultural mainstream, this distinction is, according to him, unrealistic.

> Facebook is a peer-relationship-based SNS that allows users to create personal profiles describing their real-world selves and then establish connections with other users.[46]

Boyd and Ellison hold that while most SNSs may differ in their culture, they evidence a common element, namely, consistency in their technological features.[47] Roos[48] deduces three characteristics from Boyd and Ellison's definition of SNSs. The user is able to do the following three things: create a profile; add friends or build relationships; and visit other users' sites and leave private or public messages. In other words, it enables a user to create an online identity, to form relationships with other users, to be part of a community, and to interact with other users. It may consequently be accepted that most SNSs have the same basic features. The technical features of SNSs can be categorised as: basic features; and additional features.[49]

The basic features include the creation of a personal profile (also known as digital *persona* or virtual identity) by the user where his or her personal information is stored; an inbox; and a public communication forum. The personal information includes the user's name, e-mail address, gender, and date of birth.[50] It is not compulsory for a user to provide a real name, although Facebook does recommend that users use their real names and users can more easily connect with old acquaintances when they provide their real names. The Applications (Apps) of SNSs allow users to interact with other users. The possibility of sharing photographs is another basic feature. SNSs have privacy settings which allow users to control their visibility to the general public. The role and function of privacy settings is dealt with in greater detail below.

---

46 Weaver & Morrison 2008 *Computer* 98-9.

47 Boyd & Ellison 2008 *J Comput-Mediat Commu* 210; Beer 2008 *J Comput-Mediat Commu* 519. Beer first disagrees with Boyd and Ellison's proposal that researchers use the term 'social network sites' in preference to 'social networking sites', arguing that the former is too broad and means too many things, and would lose the nuance that separates sites like YouTube from Facebook. Secondly, he argues against what he sees as Boyd and Ellison's artificial segregation of online and offline life, especially with respect to social interactions and friends. With SNS in the mainstream, this distinction is unrealistic.

48 Beer 2008 *J Comput-Mediat Comm* 519; Roos 2012 *SALJ* 383-5.

49 Individual features are discussed later in the chapter.

50 A profile is generated by completing a series of questions and filling in relevant information.

## 2.4 USES OF SOCIAL NETWORK SITES

SNSs play an important role in all social strata. The 2014 South African 'Social Media Landscape' report notes that the use of SNSs has crossed the age barrier, the urban and rural divide, and even the relationship gap.[51] The use of SNSs varies in nature, it is therefore not certain that these sites are merely used for entertainment.[52] The South African 'Social Media Landscape' highlights the intensified use of SNSs by South African corporations; the report indicates that 93 per cent of major brands use Facebook, while 79 per cent use Twitter, 58 per cent use YouTube, 46 per cent use LinkedIn, and 28 per cent Pinterest.[53]

SNSs forge a communicative relationship between the users, third parties,[54] the public, and the private sector. This was demonstrated, for example, by the South African President's 2011 State of the Nation Address, when the President Zuma quoted from users' comments on the Presidency's Facebook page:

> Bongokuhle Miya wrote on the Presidency's Facebook page that his hometown Umzimkhulu is in an appalling condition, with burst sewerage pipes everywhere, no drainage system and domestic animals roaming around town. He writes: *If the Government, which is doing very well, could just pay much more attention, with a bit of urgency to such areas.*[55]

There are various reasons why people use SNSs, and these may include both personal and commercial purposes. However, according to Boyd and Ellison, there is currently no reliable information on why people use SNSs.[56] Most users view these

---

51 "South Africa Social Media Landscape 2014: Executive summary" available at www.worldwideworx.com (date of use: 20 December 2016).

52 Also see Williams 2013 *Qualitative Market Research: An International Journal* 364-5.

53 "South Africa Social Media Landscape 2014: Executive summary".

54 Act 25 of 2002. Section 1 defines 'third party' in relation to a service provider, as meaning "a subscriber to the service provider's services or any other user of the service provider's services or a user of information systems"

55 See "The State of the Nation 2011" available at www.thepresidency.gov.za/pebble (date of use: 23 February 2011); also see Bozo & Mfeketha *Skawara News* (local newspaper in Confimvaba in the rural Transkei in the Eastern Cape) which has adopted Facebook as a strategy to increase readership and to encourage public participation. This is also a platform for diverse voices and to communicate the citizens' needs and concerns to government.

56 Boyd & Ellison 2008 *J Comput-Mediat Comm* 219.

sites as an informal space, where they can vent their feeling and share thoughts. In most cases users prefer to communicate anonymously.[57]

Companies use SNSs to reach out to current and potential customers through advertising.[58] SNSs also assist companies in analysing recent trends in their target markets. SNSs are used for 'targeted advertising' (also known as behavioural advertising), a very effective form of advertising.[59] Since users provide information that also relates to their interests, through SNSs companies are able to direct their advertising to relevant persons.[60]

Social networking sites allow users to share ideas, activities, events, and interests within their individual networks. Users generally share a common interest, but in some cases their desire is simply to meet new people. For this reason we find different classifications of social media (used as a general, overarching term) in accordance with different interests, purposes, or usage. SNSs may focus only on professionals or business users, for example LinkedIn, Visible Path Classroom 2.0, Nurse Connect, SQL Monster, and Xing. Multimedia sharing interests include YouTube, Flickr, Picasa, Twitter and others. Social connections include Facebook, MySpace, Twitter, Google+ and Mxit, to mention but a few. The majority of people use these SNSs to communicate real-life activities such as sharing personal news, sharing forthcoming events that may be of interest to other users, sharing names of books or movies they have enjoyed, or making arrangements to meet up for business or socially.

On the other hand, SNSs may be used by employers to spy on current and prospective employees who are users of SNSs. Others who may benefit from the

---

57 Rosenblum 2007 *IEEE Security & Privacy* 40. The author mentions that users post their opinions and live their daily lives online, but warns of the complacency which can prove embarrassing or even dangerous in future. This is further highlighted below in the section dealing with the challenges of SNS's.

58 See para 2.5.1.3 below.

59 "Online behavioural advertising … describes a broad set of activities companies engage in to collect information about your online activity (like webpages you visit) and use it to show you ads or content they believe to be more relevant to you." See "TRUSTe *What is online behavioral advertising?*" available at http://www.truste.com/consumer-privacy/about-oba/ (date of use: 28 August 2014).

60 Roos 2012 *SALJ* 383.

use of SNSs include recruitment consultants, insurance companies, and the police who they may use SNSs for background checks or for any law-enforcement-related activities.

SNSs have also played a role in recent political unrest. Protesters in countries such as the People's Republic of China, Vietnam, Iran, Uzbekistan, Pakistan, Syria, and Bangladesh, used SNSs to mobilise marches or for other political reasons.[61] As a result, the governments of these countries have on occasion blocked user access to Facebook. In early 2011 access was also blocked in Egypt as the security forces attempted to suppress the anti-government activists who used both Facebook and Twitter to mobilise and plan mass strike action.[62] In this context SNSs have become useful platforms for citizens to assemble, demonstrate, picket, and petition,[63] whilst they can also be used to promote freedom of association.[64] These actions are protected as fundamental rights, for example, in the Constitution of the Republic of South Africa, 1996, (the Constitution). Blocking citizens' access to SNSs can be seen as a curtailment of fundamental rights.

In a democratic society SNSs can promote public participation by citizens[65] and support freedom of expression, which is protected under section 16 of the Constitution.[66] On the negative side, SNSs may be used as a conduit to promote hate speech.[67]

61 See www.wikipedia.org/wiki/Facebook (date of use: 10 September 2016).

62 See http://mashable.com/2011/01/26/facebook-blocked-in-egypt (date of use: 30 August 2016).

63 Constitution of the Republic of South Africa, 1996, s 17.

64 Ibid s 18.

65 See para 2.4 above.

66 Constitution s 16.

67 Marx 2011 *Obiter* 322-3.

## 2.5 THE FEATURES OF A SPECIFIC SNS: FACEBOOK

### 2.5.1 General features

In order for users to register or acquire an account on Facebook, they are required to have an active e-mail address. Users must agree to the SNS's 'terms of service' and 'privacy policies'. Only once they have agreed to these terms, may they use the SNS and create a profile.[68]

Once registered on Facebook, users are required to create a profile by supplying certain of their personal information. On most Facebook profiles, it is a common trend for users to provide their real names and information. Facebook also encourages their users to use real names in order to assist in providing account security. Whilst there is no explicit requirement to provide a facial image, the majority of users do provide a photo of themselves. A photo makes it easier for others searching the site to find a particular user; if there is more than one user with the same name it may be difficult to distinguish between users. Facebook allows people who are not yet registered to search for a user's profile. A user's privacy settings will determine how much personal information can be accessed by other users on the same SNS.[69] Users can update their profiles regularly. Automatic notifications are sent to other friends when users update their profiles. This updates are reflected in a user's 'Newsfeed' feature.

After creating a profile, the next step is to create a network of friends by accepting or adding certain persons or contacts as 'friends'. Facebook offers multiple tools for users to search out and add potential contacts. Depending on the user's privacy settings, these friends may have access to information about that user which is not generally accessible to non-friends.

A user is able to send messages to friends, either in a private message space or by posting a message on a message board accessible to all friends. On Facebook this used to be called a user's 'Wall'. The Wall feature is currently called 'Timeline' and is

---

68 Hodge 2006 *Southern Illinois University Law Journal* 98; also see Roos 2012 *SALJ* 383-4.

69 Privacy settings are discussed below.

discussed in detail below. A private message may also be sent to other users without it being displayed publicly on the Timeline.

Facebook also allows users to post pictures, songs, web links, and other content on their Timeline for invited friends to comment on. Users may join groups that share a particular characteristic, for example, the same interests or hobbies.[70] The 'News Feed' feature of Facebook shows all the information posted by friends or groups to which a user's profile is connected. The News Feed feature is a user's homepage and is displayed first when a user logs on to Facebook.

A user who registers on Facebook makes certain commitments relating to registering and maintaining the security of his or her account.[71] Facebook encourages its users to provide only accurate personal information and to create an account for themselves only.[72]

On Facebook a user is not permitted to create more than one personal profile. If Facebook disables a user's account, the user cannot create another one without Facebook's permission. Facebook also has certain restrictions on who may register as a user. It prohibits people under the age of thirteen and convicted sexual offenders from registering or using the site. It is not clear how Facebook verifies the information provided by users. The terms of use clearly list content and conduct that are not permitted together with the consequences of engagement in prohibited behaviour.[73]

### 2.5.2 Privacy policy and privacy settings on Facebook

Facebook allows a user to determine who may view the profile or other information posted by the user by changing privacy settings provided by Facebook. Facebook's privacy settings have evolved over the years. Initially, when Facebook was restricted to university students with the same e-mail domain, the user's profile was visible to all other students on the same network or e-mail domain.[74] Today, a user can limit who may see his or her profile, and when posting information on his or her Timeline the

70 See www.wikipedia.org/wiki/Facebook (date of use: 30 August 2016).
71 www.facebook.com/terms (date of use: 10 June 2016)
72 Ibid.
73 Ibid.

user may further limit the visibility of the information to only certain of his or her friends.

On Facebook a user must accept the data protection policy when creating a profile.[75] The terms of use and the data protection policy are on hand on the SNSs homepage; however, there is no guarantee that users read or understand these policies.[76]

Facebook's default settings allow for users' profiles to be viewed only by registered users of the same network.[77] Facebook allows its users to block their profile information from other users and third parties.[78] Users are also able to prevent certain friends from seeing updates about particular types of activity, including profile changes, Timeline posts, and newly added friends.[79] Once a user blocks someone completely (as opposed to only blocking them from certain information), that person can no longer be the user's friend on the network or interact with the user.[80]

It is, therefore, imperative that users review the SNSs' privacy policy regularly to ensure they are informed of any changes. Users should also make the necessary changes to their individual privacy settings. With regard to data protection practices, Facebook states that it shall notify users before it make changes to its data protection policy and allow the user an opportunity to review and comment on the revised policy before continuing to use Facebook services.[81]

---

74 Roos 2012 *SALJ* 386-7 where the author notes that on Facebook there are three privacy settings for users to choose from, this allows a user to make information available to 'everyone', or to 'friends of friends', or to 'friends only'.

75 See www.facebook.com/policy.php (date of use: 16 September 2016); also see Hodge 2006 *Southern Illinois University Law Journal* 97.

76 See http://www.facebook.com/ (date of use: 16 September 2016).

77 Hodge 2006 *Southern Illinois University Law Journal* 98; also see Zheleva & Getoor "To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles" 531 available at //linqs.cs.umd.edu/basilic/web/Publications/2009/zheleva:www09/ (date of use: 21 September 2016).

78 See www.facebook.com/help/?page=419#!/settings/?tab=privacy (date of use: 10 September 2016); Rosenblum 2007 *IEEE Security & Privacy* 40, opines that with the Internet as a preferred mode of communication, users' private lives will increasingly be lived out in the public domain with the loss of a reasonable expectation of privacy protection for personal information.

79 See para 2.5.1.3 (a) below.

80 See https://www.facebook.com/settings?tab=timeline (date of use: 10 September 2016).

81 See https://www.facebook.com/about/privacy (date of use: 22 September 2016).

### 2.5.3 Noteworthy features on Facebook

*2.5.3.1 Timeline and News Feed*

The Timeline feature was introduced in 2011[82] to replace the Wall feature. The Timeline gives a user space for all the stories they wish to share. Users may post updates or share content with their friends on their Timeline. This is then displayed on the Timeline, but also in their friends' News Feeds. In the *CMC Woodworking* case,[83] Steyn J opined that "wall postings are basically public conversations".

Users may, however, restrict access to their Timelines to some extent. They may classify their contacts by using their privacy settings to determine who may see messages or content that appears on the Timeline.[84] It is also possible for a user to allow access to messages or content on the Timeline only to family, or close friends (who will include family), or all friends (who will include the previous two groupings), or friends but not acquaintances, or acquaintances, or specific groups, or the public.

A notification will automatically be sent to the user's friends if he or she updates information on the Timeline. This notification message is sent through the News Feed feature. Facebook introduced the News Feed feature in 2006; it appears on every user's homepage and highlights activities and other information on a user's profile, for example, any profile changes made, upcoming events that are listed, and birthdays of the user's friends.[85] Unless a user has changed the default privacy settings, the News Feed feature on Facebook displays every action a user makes on his or her site to their friends – for example, it will inform them of who the user has accepted as a new friend, or if a user has updated his or her status. This normally prompts other users to view that user's profile and possibly to add comments on their status. The introduction of the News Feed feature generated an uproar over its privacy implications,[86] as this feature notifies the users' friends of all recent activities.

---

82 Ibid.

83 2012 (5) SA 604 (KZD); [2012] 4 All SA 195 (KZD).

84 Roos 2012 *SALJ* 386-7 notes that the privacy settings, including the visibility of the 'Wall' feature have evolved over the years; also see Grimmelmann *Saving Facebook* 1150.

85 Mann 2008 *International Journal of Law and Information Technology* 4; also see Rosenblum 2007 *IEEE Security & Privacy* 44.

86 Grimmelmann 2009 *Iowa Law Review* 1146.

Users are able to control who can see their News Feed, however, by clicking on the relevant tabs on the privacy settings.

The Timeline and News Feed features allow a user to be kept informed of what is happening in the lives of his or her friends. It is no longer necessary to phone or talk to a friend in person to remain up to date on his or her life.

#### *2.5.3.2 'Social plugins' on Facebook*

Another Facebook feature is 'social plugins'.[87] Social plugins result in the integration of other websites with Facebook. The main social plugins are: the 'Like' button (once clicked a user publicly shares and connects with content from within Facebook or other Websites that a user finds interesting); the 'Send' button (this may be used to share a link and an optional note as a private Facebook message, Facebook group post, or e-mail); the 'Comment' box (this may be used to comment publicly on Facebook or another Website using a Facebook account); and 'Recommendations' (which informs a user of the most liked content among their friends on a site).[88]

87 'Social plugins' are tools that other websites can use to provide people with personalised and social experiences. See https://www.facebook.com/help/103828869708800 (date of use: 10 August 2016).

88 Ibid.

#### *2.5.3.3 'Tagging' on Facebook*

Facebook has an application or feature that allows a user to 'tag' a photograph of another user or non-user.[89] Tagging implies that the user associates a name of another person with someone in the photograph. If a user uploads and tags a photograph, it documents what a particular user or non-user looks like, and may also document the place where the person has been. Grimmelmann points out that the tagging application also reveals certain personal information about the tagger, such as that the tagger knows the person being tagged on the photograph, which might be a user or non-user, and a reasonable inference can be drawn that the tagger was the photographer.[90]

Facebook allows users to choose tagging settings. They may choose to review tags people have added to their post before the tags appear on Facebook. The tagging feature is not without limits. Users have control over their tagged photographs, for example, on Facebook a user who has been tagged against his or her will has two options. Firstly, he or she may choose to 'untag' the tagged image. Secondly, a user may send a request to Facebook that the photographs be removed. A user can also control who may see the photographs and videos tagged on his or her profile by means of the privacy settings.[91] A non-user is not able to send such a request to Facebook.

When Facebook users add photographs to their pages, facial-recognition software is used by Facebook to suggest names for the people in the photographs (this is referred to as the 'tag-suggestion' feature). This software compares the photographs with other photographs previously uploaded in which the same people have already been identified.

---

89 Grimmelmann 2009 *Iowa Law Review* 1146, the tags can be place on a particular area of the photograph; the tag creates a hyperlink to the profile of the user tagged. If the person in a photograph is not a Facebook user, the tag will not create a hyperlink but show plain text with the person's name.

90 Ibid 1146, 1150.

91 See www.facebook.com/about/privacy (date of use: 22 September 2016), a user may put settings to receive any notifications regarding the tagging of a user's photograph either tagged by anyone or only photographs tagged by close acquaintances.

## 2.6 SUMMARY

In this chapter I have provided an historical background of the development of SNSs. The concept Web 2.0 is explained and it is shown how Web 2.0 contributed to the development of SNSs. I have also provided some definitions of SNSs and explained how academics have analysed the elements of SNSs. I further described selected SNSs and the different types of SNS. Thereafter I considered some of the features of SNSs; these may differ depending on particular SNSs and may also be determined by the target group of the SNSs.

# Chapter 3

# Privacy and identity: A South African perspective

## 3.1 INTRODUCTION

The previous chapter gave an overview of the development, nature, and use of SNSs. In this chapter I focus on specific personality rights that may be infringed through the use of SNSs.

Personality rights are, first of all, protected under the law of delict. The intentional, wrongful infringement of a personality right results in an *iniuria*. A person[1] may sue for infringement of a personality right using a delictual remedy – the *actio iniuriarum* – which protects injury to the *corpus* (bodily integrity), *fama* (good name or reputation), and *dignitas* (all personality interests apart from the *corpus* or *fama*).

This discussion focuses specifically on the right to privacy and identity, since it is argued that it is these two rights which are affected when users share or communicate information, either about themselves or others, on SNSs.[2] These two rights form part of the wider concept of *dignitas*. In this chapter I seek to determine whether South African law provides adequate protection to the interests that form the object of these personality rights and to highlight certain shortcomings – particularly in the context of SNSs.

Privacy is also protected by section 14 of the Bill of Rights in the Constitution, and identity is indirectly protected by section 10 of the Bill of Rights as part of the right to human dignity.[3] Although the focus of this dissertation is on private law, the influence of the Constitution on these concepts cannot be ignored, and I therefore briefly consider their meaning under the Constitution. Sections 10 and 14, however, do not

1 This includes a natural person and juristic person, see par 3.4 for a discussion of juristic persons and personality rights.

2 The right to a good name (*fama*) is also often implicated, but will is not a focus in this dissertation.

3 Constitution of the Republic of South Africa, 1996, (the Constitution) s 10; Neethling, Potgieter & Visser *Law of Personality* 76; Burchell *Delict* 14.

aim to provide litigants a basis on which to litigate for compensation. Case law involving the constitutional right to privacy, for example, has focussed primarily on the validity of laws.[4] In *NM v Smith (Freedom of Expression Institute as* Amicus Curiae*)*,[5] the plaintiffs approached the Constitutional Court "with a view to vindicate their constitutional rights to privacy, dignity and psychological integrity" which, they alleged, had been violated by the respondents. The plaintiffs' claim was based on the *actio iniuriarum*, but the Constitutional Court decided that the dispute was worthy of constitutional adjudication in that it involved "a nuanced and sensitive approach to balancing the interests of the media, in advocating freedom of expression, privacy and dignity of the applicants irrespective of whether it is based on the constitutional law or the common law".[6] Although the plaintiffs claim was to be dealt with under the *actio iniuriarum,* "the precepts of the Constitution must inform the application of the common law." [7]

In this chapter I also explore the recognition and protection of these personality rights in case law. I approach an analysis of the case law irrespective of whether or not the *actio iniuriarum* and other applicable remedies are capable of fully protecting a person's *dignitas* on SNSs. Further, I focus on the procedural aspects which dictate who may institute an action and who may be held liable for the infringement of personality rights on SNSs. Privacy is also recognised and protected in several pieces of legislation, and these are considered briefly in so far as they are relevant to SNSs.[8]

---

4 Loubser et al *Law of Delict* 322. The right to identity has as yet not been considered from a constitutional perspective.

5 *NM v Smith (Freedom of Expression Institute as* Amicus Curiae*)* 2007 (5) SA 250 (CC) paras 98 - 99, 182.

6 Ibid para 31.

7 Ibid para 28.

8 Examples of laws in which a person's right to privacy is recognised and protected are: the Promotion of Access to Information Act 2 of 2000; the Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002; the Electronic Communications and Transactions Act 25 of 2002 the National Health Act 61 of 2003; the National Credit Act 34 of 2005; the Children's Act 38 of 200; the Protected Disclosures Act 26 of 2000; Protection from Harassment Act 17 of 2011; and the Protection of Personal Information Act 4 of 2013.

## 3.2 THE RIGHT TO PRIVACY

### 3.2.1 Development and recognition

*3.2.1.1 Common law*

The origin of the right to privacy in South African law can be traced back to Roman law, Roman-Dutch law, and case law. In Roman law, the homeowner was granted the *actio iniuriarum* if his peace was disturbed, or if someone came into his house without permission.[9] Publication of confidential information, for example, the reading of the will of a testator by the *depositarius*, could also result in an action under the *actio inuriarium*.[10] Roman-Dutch law took over the *iniuira* concept from Roman law and also protected the privacy of a person under the *dignitas* concept.[11] As I have indicated, *dignitas* is a collective term for all personality rights, apart from the right to a good name (*fama*) and the right to bodily integrity (*corpus*).[12]

Initially, South African law protected the right to privacy under the wider concept of *dignitas*.[13] However, case law later recognised that the common-law right to privacy is an independent personality right within the wider concept of *dignitas.*[14] Privacy, being a personality interest, is of a non-patrimonial nature. It has already been mentioned that an infringement of the right to privacy is considered a delict in the form of an *iniuria* and is actionable in terms of the *actio iniuriarum*.

The recognition of the right to privacy in South African law can be traced back to the 1950s and the case of *O'Keeffe v Argus Printing and Publishing Co Ltd.*[15] According

---

9 Van der Merwe & Olivier *Die Onregmatige Daad* 448-9.

10 Ibid.

11 Ibid.

12 Neethling, Potgieter & Visser *Law of Personality* 50.

13 Ibid. See also *R v Holliday* 1927 CPD 395; *S v A* 1971 (2) SA 293 (T).

14 *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T); *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1979 (1) SA 441 (A) 455H-456H; *National Media v Jooste* 1996 (3) SA 262 (A); *Bernstein v Bester* 1996 (2) SA para 68. Neethling "Personality infringement" in Joubert & Faris 1999 *LAWSA* para 431; Neethling, Potgieter & Visser *Law of Personality* 217; Burchell 2009 *EJ Comp L* 3, who holds that the argument in favour of recognising privacy as an independent right really only acquires significance when the concept of impairment of dignity is given a narrow focus linked to insulting behaviour.

15 1954 (3) SA 224 (C). The decision demonstrates the influence of US legal jurisprudence with regard to the concept of privacy in SA law. A proper analysis of the case reveals that the personality right infringed as actually the right to identity (particularly the appropriation of a person's identity) and not privacy, as was decided with reference to US legal jurisprudence.

to Neethling, *O'Keeffe* is the *locus classicus* for the recognition of an independent right to privacy in South African case law.[16] In this case, the *Cape Argus* newspaper (the defendant) published an advertisement for guns that contained a photograph of the plaintiff. The photograph was published without the plaintiff's consent.[17] The plaintiff alleged that such a publication constituted an intentional infringement of her right to personal privacy, that it was an unjustified aggression upon her dignity, and that she was, in fact, much aggrieved and humiliated as a result.[18] The court held that the unauthorised publication of a person's photograph and name for advertising purposes is capable of "constituting an aggression upon that person's *dignitas"*.[19]

*3.2.1.2 Constitutional law*

As I have pointed out, the Constitution of the Republic of South Africa[20] also recognises the right to privacy in the Bill of Rights. Section 14 provides as follows:

> 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 constitutional right to privacy is seen as "part of a web of mutually supporting rights" promoting human dignity and social transformation.[21]

---

Watermeyer AJ (245), with reference to the American Restatement of Law, Torts s 867, stated that in the US legal system, the principle of privacy was well established and actionable. See Neethling "Personality infringement" in Joubert & Faris 1999 *LAWSA* para 339; see also Roos 2012 *SALJ* 376; *Kumalo v Cycle Lab (Pty) Ltd* [2011] ZAGPJHC 56 (June 2011).

16 Neethling, Potgieter & Visser *Law of Personality* 217. See also *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T); *National Media Ltd v Jooste* 1996 (3) SA 262 (A); 1996 (2) SA 751 (CC).

17 1954 (3) SA 224 (C) 246D-247B. The photograph had been taken by the first defendant's employee with the plaintiff's consent, but only for the purpose of illustrating an article to be printed in the news column of the first defendant's newspaper.

18 Ibid. Watermeyer AJ (246, 248) correctly rejected the idea that *contumelia* or insult is the essence of an *iniuria*.

19 Ibid.

20 Constitution s 14.

21 *Case v Minister of Safety and Security* 1996 (3) SA 617 (CC) para 27; *Jordan v State* 2002 (6) SA 642 (CC) para 81.

### 3.2.2 Definition and content of the right to privacy

*3.2.2.1 Common law*

Privacy is not a stagnant concept which means that its definition may change over time. Its meaning and content are also influenced by the particular jurisdiction and cultural background involved. Therefore, the concept of privacy is not an easy one to define.[22] In South African common law, Neethling's definition of privacy has been accepted by the courts.[23] Neethling[24] defines privacy as

> an individual condition of life characterised 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.

In other words, "privacy consists of the sum total of information or facts that relate to the individual in his or her state of withdrawal from publicity, which facts are excluded from the knowledge of outsiders." [25] It is important to take note of the fact that a person's privacy only encompasses personal information that is truthful.[26]

In *National Media Ltd v Jooste,*[27] Harms J interpreted Neethling's concept of privacy. He held that this definition should not be interpreted to mean that the boundary of the individual's right to privacy is determined solely by that individual's wishes or will, because that is not what Neethling intended.[28] He pointed out that the boundary of a right or its infringement remains an objective question. All that this means is that "absent a will to keep a fact private, absent an interest (or a right) that can be protected".[29] The right to privacy encompasses, according to Harms J, "the

---

22 *Bernstein v Bester* 1996 (2) SA 751 (CC) paras 65, 73; Neethling, Potgieter & Visser *Law of Personality* 30.

23 *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T) 384; *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 271; *Bernstein v Bester* 1996 (2) SA 751 (CC) 789; *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 4 SA 549 (T) 533; *Greeff v Protection 4U h/a Protect International* 2012 (6) SA 393 (GNP) para 406.

24 Neethling, Potgieter & Visser *Law of Personality* 32. See also Rautenbach 2001 *TSAR* 116. .

25 Roos *Data (Privacy) Protection* 555-6.

26 Neethling, Potgieter & Visser *Law of Personality* 37; De Antrade "The right to privacy" 34.

27 *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 271.

28 Ibid.

29 Ibid. Roos *Data (Privacy) Protection* 556 agrees that "the individual himself or herself determines which information is private, couples with the will or desire to keep the particular

competence to determine the destiny of private facts."[30] It also means that "the individual concerned is entitled to dictate the ambit of disclosure, for example a circle of friends, a professional adviser or the public."[31] The individual may also prescribe the purpose and method of the disclosure, and may decide when and under what conditions private facts may be made public. [32]

In a similar vein, Roos [33] emphasises that 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. She argues that a person's right to privacy entails that he or she should have control over his or her personal information.[34]

Although a person may determine the scope of the information that should be excluded from others, the boundary of the right to privacy, and whether or not it has been infringed, remains an objective one, as pointed out by Harms J in *National Media Ltd v Jooste.*[35] In other words, in terms of South African delictual principles, a right to privacy exists where a person's subjective determination of the extent of his or her privacy is recognised by the *boni mores* (legal convictions of the community) as reasonable.[36]

*3.2.2.2 Constitutional law*

The constitutional right to privacy has a broader content than that of the common law.[37] It protects the right of individuals to decide who may enter their homes, and

---

facts private. If the will to keep facts private (*privaathoudingswil*) is lacking, the individual's interest in privacy is also lacking".

30 Ibid.

31 Ibid.

32 Ibid.

33 Roos 2007 *SALJ* 400.

34 Ibid.

35 *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 271.

36 Ibid. See also Neethling, Potgieter & Visser *Law of Personality* 31 n 328, who point out that in other instances "the individual's right of privacy cannot (always) be fixed with reference to [an individual's] own determination" for example, "when the privacy of an insane or unconscious person or a young child has to be considered"; see also Roos *Data (Privacy) Protection* 575-79.

37 Neethling, Potgieter & Visser *Law of Personality* 220.

protects them against unauthorised intrusions;[38] it also protects personal autonomy to make decisions about family relationships and private life;[39] and limits the ability of the state and other persons to gain access to personal information of others and to use and disclose such information (so-called 'informational privacy').[40] Section 14 of the Constitution also places an obligation upon the state to enact legislation which directly protects the privacy of personal information.[41] The interpretation given to (constitutional) informational privacy can inform the discussion on the protection of privacy of individuals when using SNSs.

In *NM v Smith (Freedom of Expression Institute as* Amicus Curiae*)*,[42] the Constitutional Court defined 'private facts' as "those matters the disclosure of which will cause mental distress and injury to anyone possessed of ordinary feelings and intelligence in the same circumstances and in respect of which there is a will to keep them private".[43] The court held that the disclosure of a patient's HIV status in the biography of a well-known politician breached the patient's right to privacy. The fact that this information had previously been published in an official document (the Strauss Report) did not mean that the sensitive medical information should become part of the public domain. The court said the following[44]

> [t]the assumption that others are allowed access to private medical information once it has left the hands of authorised physicians and other personnel involved in the facilitation of medical care is fundamentally flawed. It fails to take into account an individual's desire to control information about him or herself and to keep it confidential from others.

In terms of the constitutional right to privacy, a person also has the ability to decide what information he or she wishes to disclose to the public, provided that the

---

38 *S v Madiba* 1988 (1) SA BCLR 38 (D); Loubser et al *Law of Delict* 334.

39 *Case v Minister of Safety and Security* 1996 (3) SA 617 (CC); *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1998 (12) BCLR (CC).

40 *Bernstein v Bester* 1996 (2) SA 751 (CC); *C v Minister of Correctional Services* 1996 (4) SA 292 (T); *Mistry v Interim National Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC).

41 Neethling, Potgieter & Visser *Law of Personality* 272.

42 *NM v Smith (Freedom of Expression Institute as* Amicus Curiae*)* 2007 (5) SA 250 (CC).

43 Ibid para 34.

44 Ibid para 44.

person's expectation that such a decision will be respected, is reasonable.[45] In other words, the right extends to those aspects of a person's life with regard to which he or she has "a legitimate expectation of privacy".[46]

In *Bernstein v Bester*[47] Ackermann J explained the scope of the constitutional right to privacy as follows:

> The truism that no right is to be considered absolute implies that from the outset of interpretation each right is always already limited by every other right accruing to another citizen. In the context of privacy this would mean that it is only the inner sanctum of a person, such as his or her family life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community. This implies that community rights and the rights of fellow members place a corresponding obligation on a citizen, thereby shaping the abstract notion of individualism towards identifying a concrete member of civil society. Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly.

In *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd,*[48] Langa DP indicated that one should not interpret Ackermann J's statement to mean that a person does not have a right to privacy when he or she interacts in a social capacity with others. People retain a right to privacy even when they are in their offices or on mobile telephones. According to the court:

> Wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable, the right to privacy will come into play.[49]

Privacy should be seen as existing in a continuum where the 'inner sanctum' of a person's life is more rigorously protected than when he or she is moving outside the inner core of privacy to the outer fringes of the right, [50] for example, when he or she is interacting with other people in a social setting.

---

45 *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 (1) SA 545 (CC) 557.

46 *Bernstein v Bester* 1996 (2) SA 751 (CC) 789.

47 Ibid para 67.

48 2001 (1) SA 545 (CC) 557.

49 Ibid.

50 De Vos & Freedman *Constitutional Law* 463.

A number of factors are considered in distinguishing the core of privacy from its penumbra, such as the nature of the relationship that is invaded, [51] or whether it is a natural or a juristic person whose right to privacy is involved. [52]

The applicability of personality rights in the context of SNSs is discussed below.[53]

### 3.2.3 Infringement of privacy

*3.2.3.1 Common law*

(a) Introduction

As previously stated, the right to privacy will be protected when a person has a subjective expectation of privacy which society considers objectively reasonable. The plaintiff, who alleges that his or her personality has been infringed, bears the onus of proving the infringement.[54] In order to succeed with the *actio iniuriarum,* there must have been a factual infringement of privacy which is considered to be wrongful by the *boni mores*, and there must have been fault in the form of intention (*animus iniuriandi*).

A person's privacy may be infringed in different ways or through different acts. Privacy is factually infringed when outsiders become aware of true personal facts about the individual against his or her will.[55] An infringement can take place in one of two ways: either by an act of intrusion; or by an act of disclosure.[56] While intrusion

---

51 If the relationship that is invaded is one between parent and child or intimate partners, it is a strong indication that the inner sanctum of privacy has been violated - De Vos & Freedman *Constitutional Law* 463.

52 Although juristic persons also have a right to privacy, their privacy rights are considered to be less intense than those of individuals - *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 (1) SA 545 (CC) para 18; De Vos & Freedman *Constitutional Law* 463.

53 See para 3.4 below.

54 *Case v Minister of Safety and Security* 1996 (3) SA 617 (CC).

55 Neethling, Potgieter & Visser *Law of Personality* 37. See also Loubser et al *Law of Delict* 326.

56 Neethling, Potgieter & Visser *Law of Personality* 221. See also *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another* 1993 (2) SA 451 (A); *Bernstein v Bester* 1996 (2) SA 751 (CC) para 68.

denotes that the third party obtained this knowledge him- or herself, an act of disclosure occurs when somebody else reveals the information to the third party. [57]

Examples of privacy infringement by means of intrusion are: gaining entry to a private residence; [58] reading private documents; listening to private conversations; shadowing a person;[59] searching a person or his or her possessions; and conducting unauthorised medical examinations.[60] More relevant examples for this study, include reading someone's private e-mail, or hacking into another person's social network profile.[61]

Examples of privacy infringement through disclosure are the disclosure of private facts which have been acquired by a wrongful act of intrusion,[62] and the disclosure of private facts in violation of a confidential relationship.[63] One example of this is when a user (wrongdoer) gains unauthorised access to another's (plaintiff) social network profile and obtains private facts which have already been shared with a limited number of people (friends of the user on the SNS), and thereafter makes such facts publicly available. Another example of the disclosure of private facts contrary to a confidential relationship, would be if a doctor, having diagnosed a patient, were to post details on an SNS or send a private message to a third party regarding the diagnosis.

---

57 *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A).

58 *S v A* 1971 (2) SA 293 (T).

59 *Bernstein v Bester* 1996 (2) SA 751 (CC) para 65.

60 Neethling, Potgieter & Visser *Law of Personality* 222-4; McQuoid-Mason *Law of Privacy* 67-8. In *Tshabalala-Msimang v Makhanya* 2008 (6) SA 102 (W) para 26, Jajbhay J held that the medical records of a person are private and confidential. Accessing the information in an unauthorised manner therefore amounts to a wrongful act of intrusion which infringes upon the patient's right to privacy.

61 'Hacking into an account' means that a person has gained unauthorised access to the account by exploiting a weakness in the computer system or computer network.

62 This normally happens when the media publishes documents that were acquired in a wrongful, intrusive manner.

63 *Bernstein v Bester* 1996 2 SA 751 (CC) para 68. See also *Jansen van Vuuren v Kruger* 1993 (4) SA 842 (A); *Financial Mail v Sage Holdings Ltd* 1993 (2) SA 451 (A); *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 (4) SA 293 (AD). See further Neethling, Potgieter & Visser *Law of Personality* 226 ff; McQuoid-Mason *Law of Privacy* 129 ff.

(b) Wrongfulness

An act of intrusion or disclosure constitutes a wrongful violation of privacy only if the acquaintance with private facts is both contrary to the *subjective* determination and will of the prejudiced party, and, viewed *objectively*, is unreasonable or contrary to the legal views of the community[64] – that is, if it is *contra bonos mores*. The legal convictions of society (*boni mores*) are determined by what would be deemed reasonable or unreasonable. The legal convictions of the community are influenced by the Constitution and its values.[65] They can also be determined or influenced by legislation.[66] The *boni mores* is an objective test based on the criterion of reasonableness. Currie and De Waal explain that a person's privacy expectations must be reasonable in order to qualify for protection.[67] According to Loubser and Midgley,[68] the invasion of privacy would be wrongful if the court is satisfied that the invasion was such as to attract liability:

> In accordance with general principle, courts used the criterion of reasonableness, or the *boni mores* or legal convictions of the community to determine whether they should

64 Neethling, Potgieter & Visser *Law of Personality* 221.

65 Constitution Ch 1; see also Neethling, Potgieter & Visser *Law of Personality* 76.

66 McQuiod-Mason 2000 *Acta Juridica* 232; see also *Smith v Partners in Sexual Health (Non-profit)* 32 IJL 1470 (CCMA). This was a labour matter, which led to the dismissal of an employee (the Company's Administrator). During the inception of the organisation's operation, the organisation did not have its own Microsoft Outlook domain e-mail account and thus relied on Google's e-mail account (Gmail). They conducted their business communications through a Gmail account, which was frequently managed by the organisation's administrator. However, the management of the organisation still had full access to this Gmail account. The employer accessed the employee's private Gmail account allegedly by accident, since the employee was on leave at the time and had not logged off from her private Gmail account. The company also owned a Gmail account before acquiring its own Microsoft Outlook domain, and the organisation's Gmail was also managed by the employee. Subsequently, the employer discovered confidential information about internal matters in the employer's e-mails. The e-mails were later used as evidence in the employee's dismissal. Bennett C found that the e-mails were discovered in a manner which contravened the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002. Chapter 2 of the Act provides for the prohibition of interception of communications and exceptions. Section 2 provides that "subject to the Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission". The Commissioner concluded that the action of the employer was in contravention of the provisions of Act 70 of 2002 and that the acquisition of the e-mail constituted a wrongful intrusion, and therefore infringed upon the constitutional right to privacy. Although this case has persuasive authority only, the facts are interesting and fit with the privacy threats addressed in this study. This case also demonstrates how other laws may be invoked to protect the constitutional right to privacy.

67 Currie & de Waal *Bill of Rights* 318.

68 Loubser et al *Law of Delict* 328.

> recognise a claim. Factors that courts consider include whether society would protect confidentiality in the situation, for example, a doctor-patient relationship, or boardroom deliberations, whether a public value or constitutional right such as freedom of expression is involved, or whether the information disclosed is of public concern.

Let us consider the following scenario: X, whilst walking in a park, notices Y who has collapsed due to an epileptic seizure. X searches Y's handbag to establish her identity and obtain contact information. During the search, he also discovers an embarrassing detail about Y, which X considers to be a private fact. Although it is certain that there was a factual intrusion into her privacy, such an intrusion will not be wrongful unless X discloses this private fact to a third party. In this scenario, Y has a reasonable expectation of privacy with regard to the contents of her handbag. On the other hand, when X's act of intrusion is tested against the *boni mores*, it is clear that in this instance, X's conduct will be considered reasonable. In the same vein, an American author, Parent, [69] opines that an adequate conception of privacy must not allow for the possibility that a person's privacy should be considered to have been violated when another person has simply observed that person openly engaging in public activities. The case of *De Reuck v Director of Public Prosecutions* further illustrates the fact that an intrusion into the inner sanctum of the home is not *prima facie* wrongful in itself.[70]

In the context of SNSs, in order for users to have a reasonable expectation of privacy with regard to their social network profiles or communications, they must select the necessary privacy settings. A user is able to control the 'visibility' or level of privacy of his or her social network profile and communications.[71] Therefore, selecting the correct privacy settings is indicative of a subjective choice to limit access by outsiders to one's private information and communications. This may also limit the possibility of an intrusion into the user's social network profile, but does not guarantee that there will be no such intrusions.

---

69 Parent 1983 *American Philosophy Quarterly* 344.

70 In *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, and Others* 2004 (1) SA 406 (CC) para 90, the court held that although possession and consumption of child pornography often takes place in the inner sanctum of the home, the fact should not be overlooked that many of the resultant acts of abuse against children take place in private. In other words, where the reasonable risk of harm to children is likely to occur in private, some intrusion by the law into the private domain is justified.

71 Roos 2012 *SALJ* 386-7.

Neethling points out that whether or not an intrusion or a disclosure will, once objectively considered, be wrongful, depends on the particular circumstances. [72] This view is also accepted in South African case law.[73] It should be noted that it is not required that the plaintiff should have felt insulted or humiliated by the infringement before a person can be held liable for the infringement of privacy.[74]

In the case of infringement of privacy by means of an intrusion or knowledge of private facts, Neethling distinguishes between two scenarios. In the first scenario, the private facts that the person accessed were considered confidential and were only available to a limited number of people. On Facebook, this would be the case if the Facebook user has restricted access to his or her profile to a particular group of users by limiting the number of friends accepted, and by ensuring that proper privacy settings have been selected. In such a scenario, an intrusion by a party not included in the close circle of friends will be considered *contra bonos mores* and thus wrongful.[75] Roos[76] argues that the law should recognise that

> people who use SNSs such as Facebook do not give up all expectations of privacy. The mere fact that they reveal personal information on what may be considered a public forum does not mean that they intend to make that information available to all and sundry. Information revealed to "friends only" should be treated as information that has been published to a limited number of persons and any distribution of that information by third parties to a wider audience should be considered an invasion of the right to privacy.

In the second scenario, the personal facts are available to an indeterminate number of persons. In the Facebook context, this will be the case if the user has not used the privacy settings, or has accepted hundreds of people as friends, who then have access to his or her complete profile. In this scenario, an intrusion by an outsider will usually not be considered wrongful.[77] The surrounding circumstances may, however,

---

72 Neethling, Potgieter & Visser *Law of Personality* 221 ff.

73 See *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) 462; *Jansen van Vuuren v Kruger* 1993 (4) SA 842 (A) 850; *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 270; *O'Keffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C) 248.

74 Neethling, Potgieter & Visser *Law of Personality* 33, correctly state that "an infringement of dignity or insult plays no role in deciding whether there has been a violation of privacy".

75 Ibid 222. An interesting decision by the CCMA can be found in *Smith v Partners in Sexual Health (Non-profit)* (2011) 32 IJL 1470 (CCMA). Although this case has persuasive authority only, the facts are interesting and are relevant to the privacy threats addressed in this study, see discussion in n 66 above.

76 Roos 2012 *SALJ* 401.

77 Neethling, Potgieter & Visser *Law of Personality* 225.

in particular cases indicate that the intrusion is wrongful. The electronic shadowing of a person serves as an example in this regard. In the 'real world',[78] constantly following a person and keeping track of his or her movements is considered unlawful.[79] It is suggested that when a person uses Facebook to shadow another person digitally, and so causes that person distress or a feeling of harassment, the conduct should be considered wrongful, even if the Facebook user has not used the privacy settings to limit his or her visibility.[80]

In the case of infringement of privacy by means of disclosure, Neethling[81] distinguishes between three instances in which disclosure or revelation of private facts may occur: disclosure of private facts acquired through wrongful intrusion; disclosure of private facts acquired through a confidential relationship (contrary to the confidential relationship); and mass publication of private facts.

In the first scenario, the private facts disclosed are acquired through a wrongful intrusion. Disclosure of such facts will, as a general rule, be wrongful and constitute an infringement of privacy.[82] In the case of *Tshabalala-Msimang v Makhanya,* it was held that "where a person acquires knowledge of private facts through a wrongful act of intrusion, any disclosure of such facts by such person or by any person, in principle, constitutes an infringement of the right to privacy". [83]

---

78 'Real world' is used because that is how people often refer to the world away from one's keyboard. However, activities in the 'cyberworld' also have real life implications.

79 Neethling, Potgieter & Visser *Law of Personality* 225. The 'shadower' may, of course, have a legitimate reason for following the other person, such as a policeman following a suspect. Such conduct is not unlawful.

80 The Protection from Harassment Act 17 of 2011 affords victims of harassment an effective remedy against stalking (which is included in the broader definition of harassment); Roos 2012 *SALJ* 399; also noteworthy is the Florida Statute, Ch 2003-23, amended by s 784.048, which includes cyberstalking as one of the recognised methods of stalking prohibited by Florida law. The statute defines cyberstalking as "the act of engaging in a course of conduct to communicate or cause to be communicated words, images or language through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose". A law enforcement officer has the power to arrest, without a warrant, any person that he or she has probable cause to believe has committed an act of cyberstalking.

81 Neethling, Potgieter & Visser *Law of Personality* 226-36.

82 *Financial Mail v Sage Holdings Ltd* 1993 (2) SA 451 (A); *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 (4) SA 293 (AD); *Tshabalala-Msimang v Makhanya* 2008 (6) SA 102 (W) para 26.

83 2008 (6) SA 102 (W).

In the second scenario, the private facts are disclosed contrary to a confidential relationship. This often happens in a specific type of relationship, whereby a professional renders a service to a client, for example, a doctor-patient[84] or attorney-client relationship. Many of these relationships are governed by professional rules of conduct and ethical behaviour.[85]

Neethling suggests that if the private facts are disclosed to only a few persons, the conduct is not wrongful, because people tend to gossip and the disclosure is, therefore, part of human nature.[86] This means that trivial cases may not warrant legal recourse. However, should the private facts be published widely, for instance in the media, the publication would be considered unlawful. [87]

In the third scenario, private facts are disclosed through mass publication. Neethling argues that such publication is, as a general rule, always unlawful, provided that the information was intended to be accessible only to specific persons.[88] In the Facebook context, this is the scenario in which a Facebook user limits the number of friends who are allowed to see his or her profile, and utilises the privacy settings to limit their visibility. If the privacy settings are breached and the information is made available to anyone on Facebook, such publication is unlawful and, in the absence of a ground of justification, constitutes an infringement of privacy.[89]

If a person (A) publishes private information about another person (B) on his or her (A's) Facebook page, the privacy of the other person (B) is, of course, also infringed.

---

84 *Jansen Van Vuuren and another NNO v Kruger* 1993 (4) SA 842 (A).

85 General Council of the Bar or South Africa Uniform Rules of Professional Conduct highlight the professional ethics that are expected from a counsel. For instance, Rule 4.18.3 (f) states the following: "It is undesirable for a member to express an opinion in the press, by letter, article, interview or otherwise, on any matter which is still pending in the Courts. Notwithstanding the aforegoing, a member may express an opinion in the media, in general terms, on an issue which is still pending, provided that the member does not thereby purport to pre-judge the result."

86 Neethling, Potgieter & Visser *Law of Personality* 227.

87 *NM v Smith (Freedom of Expression Institute as* Amicus Curiae*)* 2007 (5) SA 250 (CC). The applicants in this matter were three HIV-positive women who claimed that the respondents had violated their rights to privacy and dignity by publishing their names and HIV status in an autobiography; see also *National Media Ltd and Another v Jooste* 1996 (3) SA 262 (A).

88 Neethling, Potgieter & Visser *Law of Personality* 231. *O'Keffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C); *Kidson v SA Associated Newspapers Ltd* 1957 (3) SA 461 (W); *Mhlongo v Bailey* 1958 (1) SA 370 (W); *Rhodesian Printing and Publishing Co Ltd v Duggan* 1975 (1) SA 590 (RA); *Le Grange v Schoeman* 1980 (1) SA 885 (E); *National Media Ltd v Jooste* 1996 (3) SA 262 (A); see also *Jooste v National Media Ltd* 1994 (2) SA 634 (C).

89 Neethling 2014 *LitNet Akademies* 40.

In *Dutch Reformed Church v Rayan Sooknunan*[90] defamatory allegations were published by the defendant about the plaintiff on the defendant's Facebook page. The plaintiff's personal email address was also published on the webpage. Satchwell J[91] considered this

> a gross invasion of privacy to furnish an individual's personal contact details on a public forum such as his Facebook wall. It exposes the recipient to unsolicited and unwanted messages. It interferes with the recipient's normal communications to others. It is private information which only [the plaintiff and his lawyer] have the right to impart or make public.

It may sometimes be uncertain who should be considered responsible for the publication of the information on a Facebook webpage. In *Sooknunan* a Facebook page was created under the name 'Glory Devine World Ministries' (GDWM). Sooknunan was trading as GDWM. He denied, however, that he was the creator of the webpage, although several things pointed to the fact that the website was created to promote the viewpoint of GDWM, and Sooknunan himself also posted information on the site under his own name. The court found that GDWM's denial of responsibility or control over the website was not credible. The court held that Sooknunan was personally the owner of the Facebook page and he was held responsible for the publications made by other anonymous users of the site. Sathcwell J held:[92]

> Sooknunan has created and made available this notice board in a public passage… He has made available the opportunity for such unlawful content and is, in effect, the publisher thereof – much as a newspaper takes responsibility for the content of its pages.

A *prima facie* wrongful infringement of privacy can, of course, be justified by the presence of a ground of justification resulting in the conduct not being considered wrongful. These grounds of justification will be discussed after the discussion of the right to identity, as the grounds of justification for infringements of privacy and identity may overlap.

---

90 2012 (6) SA 201 (GSJ).
91 Ibid para 78.
92 Ibid para 49.

(c) Fault (*animus iniuriandi*)

In order to be held liable for an infringement of privacy, the intruder must have acted with fault, usually in the form of intent.[93] Once wrongfulness has been proved, intention or *animus iniuriandi* (intention to injure) is immediately presumed.[94] The defendant will then bear the onus of rebutting this presumption. The requirement of intention means that the wrongdoer must have directed his or her will to achieving the specific result (infringement of the privacy of the plaintiff), and furthermore, that he or she must have been conscious of the wrongfulness of the intended result (that is, conscious of the wrongfulness of his or her infringement of another's privacy).

The absence of consciousness of wrongfulness on the part of the wrongdoer, excludes his or her fault. In *Jansen van Vuuren v Kruger,*[95] the absence of consciousness of wrongfulness was successfully pleaded as a defence. Other factors which may result in the absence of an intention to injure due to the absence of consciousness of wrongfulness, include insanity and intoxication on the part of the defendant.[96]

In the case of defamation, an exception is made for cases involving defamation by the media, in that fault in the form of negligence is sufficient to establish liability on the part of media defendants.[97] Before the decision of *National Media v Bogoshi*,[98] the mass media could be held strictly liable for defamation. In *Bogoshi*, the Supreme Court of Appeal rejected the strict liability of the mass media on the ground that such an approach was incompatible with freedom of expression. The court created a rule based on the objective reasonableness of the publication to replace the rule of strict liability.[99]

According to Loubser and Midgley, there are signs that in future negligence may also suffice in privacy cases involving media defendants. They refer to the minority

---

93 It seems as if there are Constitutional Court justices who are open to the idea of requiring negligence as sufficient for privacy infringement. See the minority judgments of O'Regan J and Langa CJ in *NM v Smith (Freedom of Expression Institute Intervening as* Amicus Curiae*)* 2007 (5)250 (CC).

94 Neethling, Potgieter & Visser *Law of Personality* 166-167, Neethling, Potgieter & Visser *Delict* 339; Loubser et al *Law of Delict* 356; Mcquiod-Mason 2000 *Acta Juricica* 237.

95 1993 4 SA 842 (A).

96 Mcquiod-Mason 2000 *Acta Juridica* 237.

97 Ibid 229.

98 1998 (4) SA 1196 (SCA).

99 Burchell *Personality Rights* 5.

judgment of O'Regan J and Langa CJ in *NM v Smith (Freedom of Expression Institute as* Amicus Curiae*)*,[100] who were of the opinion that the common-law requirements for fault in privacy cases should be similarly modified. O'Regan J stated: [101]

> … I accept that the legal principles developed in *Bogoshi* should apply not only in the law of defamation but also to the infringement of privacy rights by the media. I take this view for the following reasons. First, the reason in *Bogoshi* and other given for distinguishing between the media and other citizens in respect of their liability for defamation lies in the power that the media have to cause harm by publication of defamatory material… Modern electronic, print and broadcast media are immensely, and indeed, increasingly powerful. Publications often reach hundreds of thousands of readers, viewers and listeners. It is accordingly appropriate, given the scale of damage to an individual that can be caused by such widespread publication, to confer special obligations upon the media in respect of publication. In so doing, we recognise that the media are not only bearers of rights under our constitutional order, but also bearers of obligations.
>
> The nature of obligations imposed however is merely a requirement that the media establish that the publication is reasonable in the circumstances or that it is not negligent. Such obligations require the media to consider the constitutional rights at play and be persuaded that publication is nevertheless appropriate. The effect on the media, therefore, is to require them to act in an objectively appropriate fashion. In determining whether they have so acted, a court will bear in mind the particular constraints under which the media operate and will not impose a counsel of perfection in circumstances where it would not be realistic. The effect of such a rule would be to require editors and journalists to act with due care and respect for the right to privacy, prior to publishing material that infringes that right. It will require them to ask the question: is the publication of this information, although it is private information, nevertheless reasonable in the circumstances?
>
> Such an obligation will provide some real protection for important constitutional rights. Accordingly, I conclude that it is appropriate to require the media when publishing private facts without consent to establish either that the publication is reasonable in the circumstances, in which case they will rebut wrongfulness, or that they have not acted negligently in the circumstances in which instance they will need to rebut the requirement of intention.

Although the majority in *NM v Smith (Freedom of Expression Institute as* Amicus Curiae*)*,[102] did not depart from the intention requirement for the *actio iniuriarum*, the

---

100 *NM v Smith (Freedom of Expression Institute as* Amicus Curiae*)* 2007 (5) SA 250 (CC) paras 98 - 99,182.

101 Ibid paras 77-9.

102 *NM v Smith (Freedom of Expression Institute as* Amicus Curiae*)* 2007 (5) SA 250 (CC).

judges did not exclude the possibility that the common law could in future be developed in this regard.[103]

In future it could, therefore, be relevant to determine whether or not SNSs may be equated to the 'mass media', and whether or not a user can be equated to a publisher.[104] Social media such as YouTube, Flickr, Picasa, or Twitter are categorised as multimedia sharing sites. As a result, users of these sites could in future be considered to be part of the 'mass media'. This includes institutions' interactive websites which are used for business marketing, and those used for professional or social purposes as they also have mass audiences. The problem with this approach is that the users of SNS are non-media professionals and do not belong to the media's professional body.[105] The media professional bodies often set out regulations and ethical standards, which media professionals are expected to abide by. The same cannot, however, be expected of users of SNSs.

I turn now to the infringement of privacy within the constitutional framework.

---

103 Ibid para 57.

104 See Ch 2 para 2.4 above for the different categorisations of 'social media'; Stefanone, Lackaff & Rosen 2010 *Journal of Broadcasting and Electronic Media* 511, highlight that "the development of social media platforms enables non-media professionals or 'normal people' to participate in a newly accessible media environment, not just as an audience member, but also as multimedia producers".

105 The Press Council of South Africa (PCSA), which is the mother body of the press in South Africa. It has other affiliated bodies, which include the following: Newspaper Association of South Africa (NASA); The Magazine Publishers Association of South Africa (MPASA); The Association of Independent Publishers (AIP); The Forum of Community Journalists (FCJ); and The South African National Editors' Forum (SANEF).See http://www.presscouncil.org.za/-ContentPage (date of use: 4 October 2016).

*3.2.3.2 Constitutional law*

In order to establish an infringement of the constitutional right to privacy, a two-stage analysis is used.[106] Firstly, the scope of the right must be assessed to determine whether or not the law or conduct has infringed the right to privacy. Secondly, if there has been an infringement, it must be determined whether or not it is justifiable in terms of the limitation clause.[107]

As has been indicated, like other fundamental rights, the right to privacy may be limited in terms of the limitation clause. Although the right to privacy is of utmost importance in any democratic state, it should be balanced against other fundamental rights – such as the right to freedom of expression and the right to access to information.[108] This is because no fundamental right is absolute, and it may be limited if it is justifiable and reasonable to do so in an open and democratic society, as contemplated in section 36 of the Constitution. The importance of other rights in the Bill of Rights should not be overlooked in attempts to protect the right to privacy at all costs. A balance should always be struck between the individual's rights and those of others or competing social interests. [109]

Importantly, it has been held that the *actio iniuriarum* must contain rules to regulate the relationship between the right to privacy and the right to freedom of expression, as the basis of a claim for breach of privacy in our common law is the *actio iniuriarum.* The legal rules forming the basis of the *actio iniuriarum* should be developed in a manner that "recognises both the importance of privacy and the importance of freedom of expression." [110]

---

106 Currie & de Waal *Bill of Rights* 317, *Bernstein v Bester* 1996 (2) SA 751 para 75.

107 Constitution s 36; De Vos & Freedman *Constitutional Law* 354; Currie & de Waal *Bill of Rights* 164 ff. In the case of *Bernstein v Bester* 1996 (2) SA 751 para 75, Ackermann J also noted that the American constitutional interpretative approach poses only a single inquiry, and does not follow the two-stage approach of Canada and SA.

108 Constitution ss 16, 34.

109 De Vos & Freedman *Constitutional Law* 349.

110 *NM v Smith (Freedom of Expression Institute as* Amicus Curiae*)* 2007 (5) SA 250 (CC) para 47.

## 3.3 THE RIGHT TO IDENTITY

### 3.3.1 Introduction

As with the right to privacy, the right to identity is a personality right protected in terms of the common law by the *actio iniuriarum,* as well as by the Constitution. Although the Constitution does not directly refer to the right to identity, it is argued that this right is protected under the right to human dignity.[111]

Neethling defines identity as a person's uniqueness or individuality, which identifies or individualises him or her as a specific person and so distinguishes such person from others.[112] The person's identity comprises all those facets (*indicia*)[113] of his or her personality which make him or her a unique individual.[114]

In the USA, identity is protected by privacy torts known as the 'false-light tort' and the 'appropriation tort'.[115] Initially, South African courts also protected the right to identity under the right to privacy, [116] but more recently identity has been recognised as an independent personality right.[117]

Although privacy and identity are analogous, they should be distinguished since privacy infringement involves acquaintance by a third party with true personal information, whereas identity infringement revolves around falsifying personal information. In identity infringement, the person's identity is falsified or an incorrect image is conveyed. [118] In contrast, privacy is not infringed by the false use of the person's characteristics, but through an acquaintance with (true) personal facts

---

111 Constitution s 10; Neethling, Potgieter & Visser *Law of Personality* 76; Burchell *Delict* 14.

112 Neethling, Potgieter & Visser *Law of Personality* 36; see also *Kumalo v Cycle Lab (Pty) Ltd* [2011] JOL 27372 (GSJ) paras 15-17.

113 *Indicia* includes the facets of a person's personality which are characteristic of or unique to him or her, such as his or her life history, name, creditworthiness, voice, handwriting, appearance etc. See Neethling, Potgieter & Visser *Law of Personality* 37.

114 Ibid 36.

115 Ibid. These torts will be dealt with in Ch 4 below.

116 *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 3 SA 224 (C); *Kidson v SA National Associated Newspapers Ltd* 1957 (3) SA 461 (W).

117 *Grütter v Lombard* 2007 (4) SA 89 (SCA); *Kumalo v Cycle Lab (Pty) Ltd* [2011] ZAGPJHC 56 (17 June 2011).

118 De Antrade "The right to privacy" 32.

regarding that person.[119] In other words, "at the heart of the distinction between the right to privacy and the right to identity we find two important elements: firstly, whether the facts concerning a given person are truthful or not; and secondly, whether such person wants to keep them private or not." [120]

The distinction between the right to privacy and identity may at times seem complex as the two concepts are often intertwined.[121] It can, for example, be said that privacy protects information that is linked to one's identity.[122] Furthermore, both rights are personality rights (rights which are non-patrimonial and which cannot exist independently of a person) and relate to an individual's right to dignity[123] and self-determination.[124] Nevertheless, they are two autonomous personality rights and should not be confused. [125]

It should also be kept in mind that infringement of identity can also constitute the crime of identity theft, which constitutes 'fraud'.[126]

---

119 Neethling, Potgieter & Visser *Law of Personality* 37.

120 De Antrade "The right to privacy" 32.

121 Ibid 19.

122 Ibid 25.

123 Constitution s 10.

124 De Antrade "The right to privacy" 29.

125 In *Bernstein v Bester* 1996 (2) SA 751 (CC) para 65 the court stated the following: "The scope of privacy has been closely related to the concept of identity and it has been stated that 'rights, like the right to privacy, are not based on a notion of the unencumbered self, but on the notion of what is necessary to have one's own autonomous identity'."

126 If a user's profile on a SNS is cloned, the cloned profile is often used to commit a crime, such as the infamous 419 scams. A cloned profile is also sometimes used to solicit money from friends of the original profile holder, or fake profiles are created using the names of charities in order to solicit donations. Snyman *Criminal Law* 520 defines fraud as the unlawful and intentional making of a misrepresentation, which causes actual prejudice or which is potentially prejudicial to another.

### 3.3.2 Infringement of identity: Wrongfulness and fault

In South African case law, the right to identity is recognised as an independent personality right that requires protection under the *actio iniuriarum.*[127] As has been said, the protection of the right to identity in South African law has developed from two independent privacy torts recognised in American law, namely:[128]

- publicity which places the plaintiff in a false light in the eyes of the public; or
- appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[129]

An example of a false-light situation from early case law can be found in *Kidson v SA National Associated Newspapers Ltd*[130] where a newspaper published a false story and photographs of the plaintiffs, depicting them as lonely nurses looking for boyfriends. The nurses had consented to their photographs being taken for the purposes of raising funds to build a recreation hall near their training facility. Some of the nurses were married and some engaged and accordingly felt aggrieved by the story. The court awarded damages for the *iniuria*.

The *O'Keeffe* case, in which the right to privacy was recognised *eo nomine* for the first time in South African case law, actually provides an example of identity infringement involving the appropriation of the plaintiff's image for advertising purposes. [131]

*Grütter v Lombard*[132] is a more recent case which provides a good illustration of the right to identity as an independent personality right. It deals with a case of appropriation of the plaintiff's (appellant's in this case) name or likeness for the

---

127 *Grütter v Lombard* 2007 (4) SA 89 (SCA).

128 Neethling, Potgieter & Visser *Law of Personality* 256.

129 Ibid 257, notes that the mere use of corresponding names cannot be regarded as infringement of identity.

130 1957 (3) SA 461 (W).

131 1954 (3) SA 224 (C). A proper analysis of the case reveals that the personality right infringed was actually the right to identity (particularly the appropriation of a person's identity) and not privacy, as was decided with reference to US legal jurisprudence.

132 2007 (4) SA 89 (SCA).

defendant's advantage.[133] Grütter and Lombard were two attorneys who, at some point had practised in association under the name 'Grütter and Lombard'. Grütter then terminated his association with Lombard, but Lombard, together with another attorney, continued to practise under the name 'Grütter and Lombard'. Grütter requested Lombard to remove his name from the name of the practice, because he (Grütter) was known to be the person named in the description of the practice and he no longer wished to be identified with it after his association with Lombard had come to an end. Lombard declined to do so and Grütter applied to the court for an order prohibiting Lombard from using his name.

The Supreme Court of Appeal held that Lombard had infringed upon Grütter's right to identity when he used his name without authorisation for his own commercial advantage, and ordered Lombard to remove Grütter's name, as requested.[134] Nugent JA stated the following:

> What is conveyed to the outside world by the use of Grütter's name is that he is in some way professionally associated with the respondents, or at least that he is willing to have himself portrayed as being associated with them, which … is a misrepresentation of the true state of affairs for which there can be no justification. [135]

The right to identity was also protected in *Kumalo v Cycle Lab (Pty) Ltd.*[136] Kumalo was a celebrity and public figure (model, television presenter, magazine editor and businesswoman), and Cycle Lab was a retailer of bicycles and cycling products. While Kumalo was shopping in the defendant's store, a man approached her and took her photograph (on instruction of the defendant). The defendant subsequently incorporated the plaintiff's photograph in an advertisement for its store, which was published in a magazine entitled *About Time* and in a brochure called *Cycling News*. Kumalo objected, stating that the defendant had sought to exploit her image for commercial purposes without her knowledge and consent, and had published a low-quality photograph of her in a poorly-designed advertisement for its shop. She felt that she had been abused and her privacy invaded. Kumalo was embarrassed, as

---

133 Neethling, Potgieter & Visser *Law of Personality* 257 note that the mere use of corresponding names cannot be regarded as infringement of identity.

134 2007 (4) SA 89 (SCA) para 13.

135 Ibid.

136 [2011] ZAGPJHC 56 (17 June 2011).

she feared that her friends, professional colleagues, and peers would assume that she had consented to the publication of the photograph, thereby lowering her professional standards and standing. [137]

Boruchowitz J held that the misleading use of the plaintiff's photograph in an advertisement without her permission constituted an infringement of her right to identity. [138] It was also a violation of the plaintiff's privacy, since a personal fact, namely her image, had been publicly exposed, contrary to her determination and will.[139]

Applying these principles to SNSs, it becomes clear that a person's identity will be infringed if he or she is portrayed in a false light on a SNS, or his or her identity is appropriated on a SNS for the wrongdoer's benefit, as illustrated in the scenarios below.

In the first scenario, user X creates or registers a Facebook profile in the name of a prominent politician, Y, and uploads a real photograph of Y. Furthermore, X provides false information to the effect that Y has joined an opposition party, even posting manipulated photographs of Y wearing the opposition's colours. In another scenario, P creates or registers a Twitter profile in the name of Q, a well-known musician, in order to secure followers. This conduct infringes on Q's identity for the benefit of P.

Once a factual violation of the plaintiff's identity has been established – in other words, that there has been a misrepresentation of his or her identity – an inference of wrongfulness and an inference of *animus iniuriandi* arise, which the defendant may rebut.[140] Wrongfulness can be rebutted by grounds of justification, which will be discussed below.[141] What has been said under privacy in regard to liability for negligence should also be kept in mind with regard to identity infringement.

137 Ibid para 5.
138 Ibid.
139 Para 23.
140 Loubser et al *Law of Delict* 335.
141 See para 3.7 below.

## 3.4 JURISTIC PERSONS AND PERSONALITY RIGHTS

Juristic persons may also create profile pages on SNSs. The profile page may be used for various activities, such as marketing, communication, research, and many others that could benefit a juristic person. The question arises of whether juristic persons also have a right to privacy and identity which can be infringed by users of SNS.

Midgley and Loubser highlight that "historically, the *actio iniuriarum* was available to protect the personality rights of natural persons only, based on the traditional acceptance that artificial or juristic persons cannot have rights that are closely associated with human beings". The courts have also long recognised that a trading corporation can sue for defamation where its business reputation has been injured.[142] In *Dhlomo v Natal Newspapers (Pty) Ltd,* the Appellate Division (now the Supreme Court of Appeal) confirmed that a non-trading corporation or juristic person may sue for defamation.[143]

Neethling highlights that a juristic person possesses those personality rights the objects of which may be infringed without the victim's knowledge (that is, without the victim subjectively experiencing injured feelings).[144] This means that a juristic person does possess a legitimate interest in the protection of its reputation, privacy, and identity. Therefore, in the case of a juristic person's right to privacy or identity, the emphasis is placed on the objective aspect, which does not require human consciousness, sensation, feelings, or emotion with regard to the harm suffered.[145]

---

142 *Witwatersrand Native Labour Association Ltd v Robinson* 1907 TS 264 266; *African Life Assurance Society Ltd v Phelan* (1908) 25 SC 743; *GA Fichardt Ltd v The Friend Newspaper Ltd* 1916 AD 1 5-6, 9.

143 1989 1 SA 945 (A) 952-3; *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 2 SA 451 (A) 46*; Motor Industry Fund Administrators (Pty) Ltd v Janit* 1994 3 SA 56 (W) 60-1; *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 4 SA 293 (A) 303-04; also see Neethling, Potgieter & Visser *Law of Personality* 69.

144 Neethling 2005 *CILSA* 244.

145 Neethling, Potgieter & Visser *Law of Personality* 51-2, the objective element refers to the external, generally recognisable and concrete manifestation of personality harm, whilst the subjective element of personality exists in a person's consciousness and is, inter alia, formed by his or her reaction to the factual infringement of his or her interests of personality.

The Constitution also adopts the common-law approach, namely the recognition that juristic persons may have personality rights. In terms of section 8(4) of the Constitution "a juristic person is entitled to the rights in the Bill of Rights to the extent required by the rights and the nature of that juristic person". The Constitutional Court in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd*,[146] confirmed that:

> The right to privacy is applicable, where appropriate, to a juristic person…. Juristic persons are not the bearers of human dignity. Their privacy rights, therefore, can never be as intense as those of human beings. However, this does not mean that juristic persons are not protected by rights to privacy. Exclusion of juristic persons would lead to the possibility of grave violations in our society, with serious implications for the conduct affairs…

This section highlights the fact that the personality rights under discussion in the context of SNSs may be applicable where a juristic person has suffered the infringement of such a personality right on SNSs either as a user or non-user.

## 3.5 GROUNDS OF JUSTIFICATION

### 3.5.1 Introduction

Once the wrongfulness of the infringement of privacy or identity has been factually established, the defendant has an opportunity to show that his or her conduct is not wrongful. The wrongfulness of an infringement of privacy and/or identity may be excluded where a ground of justification can be shown to exist. The onus is on the defendant to prove that although there has been a factual infringement of privacy or identity, the infringement is not wrongful because of the presence of a ground of justification.[147]

The different grounds of justification are situations in which the legal convictions of the community have, over time, determined that the conduct involved is not

146 2001 (1) SA 545 (CC) 557D-G; also see Currie & de Waal *Bill of Rights* 38.
147 Loubser et al *Law of Delict* 163.

wrongful.[148] Consequently, different grounds of justification may emerge with changes in the society's norms. The grounds of justification which are applicable where other types of personality right are factually infringed, such as infringement of a person's reputation (good name), dignity, and feelings, may also be relevant to the rebuttal of wrongfulness where there has been an infringement of privacy or identity.[149]

In the case of privacy, the relevant grounds of justification are: necessity; private defence; consent to injury; and performance in a statutory or official capacity. These are the so-called 'traditional grounds' of justification. More recently the maintenance and furtherance of legitimate interests, including the public interest, has been recognised as a ground justifying knowledge of private facts. This defence is closely connected to the traditional grounds of private defence and necessity.[150] The defences traditionally used in defamation cases, such as fair comment and privilege, could also justify the publication of private facts.

The grounds of justification that may be relevant in the case of identity infringement, are consent (*volenti non fit iniuria*) – the only relevant ground of justification in appropriation cases; and, but only highly exceptionally, in the false-light cases), necessity and private defence.[151] Privilege and media privilege (traditionally used for justification of defamation) may also be relevant; so too, public interest (in information). [152]

### 3.5.2 Consent or *volenti non fit iniuria*

This ground of justification applies to rebutting both an infringement of the right to privacy and the right to identity (in cases of appropriation, consent could be the only

148 Burchell *Principles of Delict* 67

149 McQuoid-Mason 1973 *SALJ* 28; see also Burchell *Principles of Delict* 193.

150 Neethling, Potgieter & Visser *Law of Personality* 240.

151 Ibid 261.

152 Ibid.

possible ground of justification).[153] In Roman and Roman-Dutch law, consent as a ground of justification was expressed in the maxim *volenti non fit iniuria,* which means that no harm is done to someone who voluntarily consents to injury or to the risk of injury.[154] A person who willingly releases private information to the public can, therefore, not complain that his or her privacy has been infringed. Also, where a person consents to his or her image being used to promote a product, that person cannot claim that his right to identity has been infringed.

According to Loubser and Midgley,[155] consent to the intentional causing of harm, which must be for a lawful purpose, involves a willingness to suffer specific harm, for example, consenting to an operation. Consent to the risk of injury, on the other hand, is less specific and involves a willingness to risk suffering some harm during a dangerous activity, such as a sport that involves risk of injury. They also point out that in specific situations, both forms of consent may apply – for example, where one consents to a specific operation, but also consents to the risk of complications as a result of the operation. In order for the consent to be valid, the person consenting must, of course, be fully informed of all the possible risks. The person must also be willing to suffer the risk. [156] In *Waring and Gillow Ltd v Sherborne*[157] the court explained this as follows

> …in order to render the maxim [*volenti non fit iniuria*] applicable, it must be clearly shown that the risk was known, that it was realised, and that it was voluntarily undertaken. Knowledge, appreciation, consent – these are the essential elements; but knowledge does not invariably imply appreciation, and both together are not necessarily equivalent to consent…

Consent may either be given expressly or may be implied. It can be given verbally or tacitly by conduct. It must, however, be indicated in an obvious manner.[158] The consent must also be given before the prejudicial act that infringes upon the privacy or identity of the injured party. The act of giving consent is a unilateral act, which means that it can be retracted unilaterally.[159]

---

153 Ibid.
154 Loubser et al *Law of Delict* 163.
155 Ibid 163-4.
156 Ibid.
157 1904 TS 340 344.
158 Loubser et al *Law of Delict* 163.
159 Neethling, Potgieter & Visser *Delict* 90.

The party whose personality rights have been infringed must have consented him or herself, and must have had the capacity to give such consent.[160] That means that the person must be legally capable of expressing his or her will; the person does not have to be a major, but "they must have the mental ability to appreciate the implications of his or her actions, to distinguish between right and wrong, and to act accordingly".[161]

One cannot consent to the causing of harm that is considered *contra bonos mores*. Consent to harm that offends the *boni mores* will be wrongful and thus invalid. [162]

The subjective element of the right to privacy embraces the idea that a person (or a user in the context of SNSs) dictates which private facts are regarded as private. As soon as a person has disclosed private facts about him- or herself publicly or to a third party, he or she loses the reasonable expectation of keeping those facts private. For instance, in a situation where a user of SNSs publicly discloses private facts about him- or herself, that user loses the reasonable expectation of privacy with regard to those facts. Facebook, for instance, clearly specifies that it will use the information it obtains through the registration of a user profile, and any other information that users share with other users.[163] In a case where a user makes use of privacy settings on his or her SNS profile, it can be argued that such user retains a reasonable expectation of privacy. On the other hand, it could also be argued that he or she tacitly consents to the risk of injury (the Internet is not an absolutely safe environment – any piece of information posted online may go viral within a split second, thereby infringing upon the user's personality rights).

The following examples illustrate situations in which a person consents to injury. In terms of the RICA Act, a party to a conversation may consent to the interception of the conversation.[164] Another example is section 14 of the National Health Act[165]

---

160 *Santam Insurance v Vorster* 1973 (4) SA 764 (A) 779.

161 Loubser et al *Law of Delict* 163, 165.

162 Ibid 167.

163 See https://www.facebook.com/about/privacy/your-info (date of use: 20 December 2016).

164 Act 70 of 2002 s 5 (1): "Any person, other than a law enforcement officer, may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception, unless such communication is intercepted by such person for purposes of committing an offence, where the party is satisfied that there are reasonable grounds to believe that the party has given consent, as contemplated in this section."

which provides that all the information concerning a user (patient), including information relating to his or her health status, treatment, or stay in a health establishment, is confidential, unless the patient consents to its disclosure, which may include publication of the information.

The case of *Jordaan v Delarey*[166] provides a good illustration of when consent can be viewed as a ground of justification. Although this case involves an action for damages for alleged defamation, the conduct complained of also caused an *iniuria* (that is, an infringement of a personality right) and the grounds of justification for infringement of personality rights are similar. The defendant had made grossly insulting remarks to the plaintiff in private. The plaintiff was anxious to get evidence that the defendant had uttered these insulting remarks, and for that reason she telephoned the police, asking them to come to the house where she was living. Two policemen arrived, and, before the plaintiff herself arrived, the defendant already knew of the police's presence and the purpose for which they had been called by the plaintiff. The defendant told them what he had said to the plaintiff. Immediately thereafter, the plaintiff arrived and requested the defendant to repeat his remarks in the presence of the police. He did so.[167] Hiemstra J held that in these circumstances, the *iniuria* took place with the assent (consent) of the plaintiff and dismissed the claim.[168]

Consent is especially relevant in employment relationships. The contract of employment determines the terms and conditions of employment. This often includes a waiver of the right to privacy on the part of the employee. Other policies of the company, for instance its information and communications technology (ICT) policy, may also contain provisions in this regard. Although employees may be asked to waive their right to privacy in an employment contract, such terms are prohibited by law, since they could be considered immoral or contrary to public policy. Such terms are therefore not enforceable.[169]

---

165 Act 61 of 2003.

166 1958 (1) SA 638.

167 Ibid 638.

168 Ibid 639.

169 Hutchison *Law of Contract in South Africa* 240.

### 3.5.3 Necessity

This ground of justification is applicable in cases of an infringement of the right to privacy,[170] and, in exceptional circumstances, to infringement of the right to identity (only in false light cases).[171] Necessity is present where the infringement of privacy or identity of an innocent person is the only reasonable way of protecting one's own interest, or that of another person, against the danger created by natural phenomena (*vis major*) or human conduct.[172] The danger must be present or imminent at the time, and the person relying on necessity must not be legally obliged to endure the consequences of the dangerous situation.[173] Furthermore, there should be proportionality between the protected interest and the infringed interest – since an innocent party's interest is infringed in necessity, the interest protected should not be outweighed by the harm done to the innocent party.[174]

In the context of SNSs, the state of necessity may arise, for instance, when the life of another person is in jeopardy. Neethling[175] provides an example of a father who publishes personal information regarding his missing son, who suffers from amnesia, in the hope that the information will help to locate the son. In this instance the infringement of the son's privacy is reasonable in the circumstances and therefore not wrongful.

A state of necessity may also arise in an employment relationship where the employer has a commercial interest which he or she must protect. In order to protect this commercial interest, the employer may infringe upon the privacy of prospective employees by obtaining or searching for information regarding not only the prospective employee's technical and intellectual abilities, but also his or her personality or character.[176]

---

170 Neethling, Potgieter & Visser *Law of Personality* 241 give the example of a person entering another's private residence to escape violent rioters.

171 Ibid 261 give the example where an attorney gives false information about a client to another party who is threatening to harm the client.

172 Ibid 241; Loubser et al *Law of Delict* 171.

173 Loubser et al *Law of Delict* 174.

174 Ibid 171.

175 Neethling, Potgieter & Visser *Law of Personality* 241.

176 Ibid 241.

### 3.5.4 Private defence

This ground of justification is applicable where the defendant defends himself or herself against another's actual or imminently threatening wrongful act, in order to protect his or her own privacy or identity, or the privacy or identity of some other person.[177] Although it is said that private defence may be invoked against infringement of the right to privacy, acts of private defence justifying an infringement of privacy seldom occur.[178] Neethling provides the example of one spouse appointing a private investigator to spy on the other spouse in order to collect evidence of adultery. He argues that the spouse has a legitimate interest in not being misled.[179] This example could also extend to the SNS environment where a spouse hacks into the other spouse's SNS account in order to determine whether the spouse is cheating on him or her.

Private defence may also justify an infringement of the right to identity, but only in exceptional circumstances and only in false-light cases.[180] A SNS user who posts false information on an SNS about another person, may use this ground of justification if that user posted the false information under duress – for example because he or she is being threatened with violence by a third party who is forcing him or her to make the posting.

The act of private defence must remain within the prescribed limits; it must be relevant to the protection of the defendant's interests; and may not exceed what is reasonably necessary to protect the interests.[181]

### 3.5.5 Public interest in information

The public interest in a true statement of fact can justify an infringement of privacy, similar to justifying an infringement of the reputation in defamation cases.

177 Ibid 242.
178 Ibid.
179 Ibid.
180 Ibid 261.
181 Ibid 160.

The information published must, of course, be true, otherwise privacy will not have been infringed (as noted above, the publication of false information does not infringe on someone's privacy, but on his or her identity.) All that need be proved further is that the publication was in the public interest.[182] The public has a right to be informed which is protected by the right to freedom of expression.[183] Both the right to privacy and the right to be informed are constitutionally protected as fundamental rights.[184] In a case where infringement of privacy is alleged, a balance must be struck between the interest of the public in being informed, and the interest of the individual in having a private life. Although publication of private facts is *prima facie* wrongful, the wrongfulness may be excused by the fact that the person concerned is a public figure, and as such, the publication of facts about his or her private life may be in the public's interest.[185]

McQuiod-Mason correctly opines that whether or not the invasion of privacy is for the public benefit is often a question of policy and has to be decided on a case-by-case basis.[186] The case of *Tshabalala-Msimang v Makhanya*[187] served as an example. The case involved the late Minister for the Department of Health and afforded the court an opportunity to consider the balance to be struck between the right to privacy and the public's right to know about a public figure's private life.

The applicant, the minister, sought an order interdicting and restraining the respondent from making further comments and publishing any comments on unlawfully obtained medical records relating to her.[188] The respondents contested the application on the basis that the allegations of alcohol abuse by the applicant during her stay in hospital (which emerged from her hospital records) were so germane to her fitness for office as a member of the Cabinet, that her hospital records and their disclosure were justified by the greater public interest in this

182 Ibid; see also Burchel *Personality Rights* 272 Loubser et al *Law of Delict* 360.

183 Constitution s 16 (1) which includes the freedom of expression of the press and media, as well as [citizens'] freedom to receive or impart information or ideas.

184 Constitution s 14 and s 34 respectively.

185 McQuoid-Mason *Law of Privacy* 219.

186 Ibid 218.

187 2008 (6) SA 102 (W).

188 Ibid paras 4, 15.

information.[189] The court held that "the overwhelming public interest points in the direction of informing the public about the contents incorporated in the medical records in relation to the first applicant, albeit that the medical records may have been unlawfully obtained."[190]

Neethling[191] points to the following factors that have been identified in case law as relevant to the determination of fairness: the fact that the plaintiff is a public figure; is involved in a newsworthy event; or exposed his or her privacy to the risk of publication (for example, by seeking the limelight). Other factors that should be considered are: whether the public has an interest in the information, or whether they are merely interested (curious) about it; the intensity of the violating conduct; the fact that the information was obtained wrongfully or was published contrary to a court order or in breach of a contract; the status of the person in society; the time span between the occurrence of the newsworthy event and its publication; the degree of identifiability of the plaintiff; and the defendant's motive or purpose in publishing the information.

The public interest in information may also justify an infringement of identity. In this instance the information published is, of course, not correct and creates a false image of the person reported on. Neethling[192] refers to Coetser[193] who argues that the media has to act with speed and efficiency when they distribute news. In the process errors will crop up when a person is portrayed in the press. The press will find itself in an intolerable situation if every false portrayal of personality leads to liability. Provided that the portrayal reflects the truth as far as is reasonably possible, the press should not be held liable. It is easy to imagine that a journalist who is tweeting on a prominent court case, may in his or her haste to stay on track with the reporting as the case progresses, portray a witness or one of the parties to the case in a manner that does not correctly reflect the image of the particular person. In such

189 Ibid para 11; see also *Malema v Rampedi and others* 2011 (5) SA 631 (GSJ) E, where Lamont J held that the public is entitled in general terms to have full disclosure concerning persons who stand in a public position, and who are high-profile personalities who invite comments about themselves.

190 Ibid para 49.

191 Neethling, Potgieter & Visser *Law of Personality* 246-9.

192 Ibid 261-2.

193 Coertser *Reg op Identiteit* 224-6.

an instance the public's interest in receiving the information timeously may arguably be offered as a defence.

### 3.5.6 Public interest in art

According to Neethling,[194] public interest in art (freedom of creativity) may justify the infringement of identity in appropriate cases. The author further asserts that an artwork of exceptional quality will justify the infringement of identity more readily than one of inferior quality.[195] Currie and de Waal[196] note that artists are sometimes responsible for radical criticism of the way society functions and that all the activities associated with and necessary for the artist to be creative should, therefore, be constitutionally protected. The Constitution guarantees and protects freedom of artistic creativity under freedom of expression.[197] In *Laugh it Off Promotions CC* v *South African Breweries International*,[198] Moseneke J notes that:

> It follows clearly that unless an expressive act [an act artistic creativity] is excluded by section 16(2) it is protected expression. Plainly, the right to free expression in our Constitution is neither paramount over other guaranteed rights nor limitless.

It is not clear whether the defence of public interest in art may apply in the context of SNSs, where infringement of identity in an appropriation case is alleged. The defendant arguably will not be liable where his or her act is successfully protected in terms public interest in art.[199] Section 7 of the Protection of Personal Information Act,[200] provides for the public interest in art in the context of the processing of personal information.

---

194 Neethling, Potgieter & Visser *Law of Personality* 262.
195 Ibid.
196 Currie & de Waal *Bill of Rights* 370.
197 Constitution s 16 (1)(c).
198 *Laugh it Off Promotions CC v South African Breweries International (Finance) BV t/a Sabmark International* 2005 (8) BCLR 743 (CC); 2006 (1) SA 144 (CC) para 47.
199 Constitution s 16 (1)(c).
200 Act 4 of 2013. This Act is discussed in para 3.7.3.1 below.

### 3.5.7 Privilege

Privilege as a ground of justification may be applicable to justify the publication of both true and untrue statements. Privilege may therefore be applied to rebut an infringement of both privacy (true facts) and identity (untrue facts).[201] There are two groups of privilege: absolute privilege; and relative privilege. For instance, statements made while participating in parliamentary proceedings (this includes the National Assembly and the National Council of Provinces) enjoy the protection of absolute privilege.[202]

On the other hand, in cases of a qualified privilege, the defendant forfeits the protection of the defence if he or she acted with improper motive (or malice) in publishing the material.[203] In case of infringement of privacy, privilege may justify the defendant's wrongful conduct "where a duty rests on a person to reveal private facts concerning another to outsiders who have a reciprocal duty or justified interest to be informed of such facts".[204] There are a number of recognised categories of qualified privilege. These include statements published in the discharge of a duty, the exercise of a right, or the furtherance of a legitimate interest; and statements published in the course of judicial or quasi-judicial proceedings.[205] It is still uncertain whether privilege will be a successful defence for users' in the context of SNSs.

### 3.5.8 Media privilege

201 Neethling, Potgieter & Visser *Law of Personality* 251, 261.

202 Ibid and145; Loubser et al *Law of Delict* 366; Constitution s 58(1) grants absolute privilege to cabinet members and s 71(1) grants privilege to delegates of the National Council of Provinces.

203 Ibid 286.

204 Neethling, Potgieter & Visser *Law of Personality* 252; also see *Jansen van Vuuren v Kruger* 1993 4 SA 842 (A) 851.

205 Burchell *Personality Rights* 288, this may include statements made by judges, magistrates, witnesses, litigants, advocates, and attorneys. Judges and magistrates enjoy a special form of qualified privilege (there is a rebuttable presumption that their actions are lawful and within the limits of their authority).

Media privilege may be invoked against the reasonable publication of false or untrue defamatory allegations.[206] It may also be applicable to rebut an infringement of both privacy and identity.[207] In the context of SNSs, it is unclear whether a user (defendant) may rely on this ground of justification. If SNSs can be equated to mass media and its users to publishers, then they could possibly rely on this ground of justification.[208]

### 3.5.9 Fair comment

This ground of justification is closely linked to the defence that the publication of a true statement is in the public interest. As I have pointed out, the right to freedom of expression is an important fundamental right in a democratic society, and citizens should be free to comment publicly without fear of prosecution or persecution. It has been said that the defence of fair comment protects "the right of the citizen honestly to express his genuine opinion on a matter of public interest, however wrong, exaggerated or prejudiced that opinion may be". [209]

In order for the defendant to succeed with the defence of fair comment, the defendant's comments must comply with four requirements which have been developed through case law.[210] These requirements are: the allegation in question must amount to comment or opinion; it must be fair; the factual allegations on which the comment is based must be true; and the comment must be related to a matter of public interest. For instance, a user may make a comment on SNSs about the behaviour of a certain politician or a famous cricket player's lifestyle. Neethling[211] holds that in order for such a comment to be fair, it must remain within certain prescribed limits. These limits are determined in terms of the criterion of

206 Neethling, Potgieter & Visser *Law of Personality* 155-6, 261.
207 Ibid 251, 261.
208 See the discussion under para 3.2.3.1 (c) above.
209 *Telnikoff v Matusevitch* [1991] 4 All ER 817 826.
210 *Crawford v Albu* 1917 AD 102; *Marais v Richard* 1981 (1) SA 1157 (A); see also Burchell *Personality Rights* 277.
211 Neethling, Potgieter & Visser *Law of Personality* 157.

reasonableness or the legal convictions of the community.[212] A comment made with malice or improper motive does not qualify for the defence of fair comment.[213]

In the following section I summarise the relevant principles as they apply to SNSs.

## 3.6 CONCLUSION: PRACTICAL APPLICATION TO SNSs

The discussion so far has dealt with privacy and identity as personality rights, and how they may be infringed by users of SNSs, as well as the legal framework which governs or protects these infringements. In this section I provide a summary of the most important principles as they apply in the SNS environment. The delictual perspective is the focal point of this discussion.

SNSs provide a platform for the free flow of information amongst users and third parties. However, every online conversation leaves a digital footprint, in contrast to the physical or offline world where a conversation between two people will only be remembered for a short while by the parties, and no physical trace of it will remain. On the other hand, anything which is posted on SNSs may go viral within a split second. The privacy policies of different SNSs therefore warn users that their privacy cannot be guaranteed.[214]

Roos[215] correctly points out that subscribing to SNSs and registering a profile account can be equated with appearing in a public space. In this space, the scope of privacy will be curtailed. This view is also evident from *Bernstein* v *Bester,*[216] where it was held that as a person moves out of the inner sanctum of privacy into communal relations and activities such as business and social interaction, the scope of personal

---

212 Ibid 157- 8.

213 Loubser et al *Law of Delict* 361; *Crawford v Albu* 1917 AD 102 114; *Jansen van Vuuren v Kruger* 1993 SA 842 850H-I; *Heroldt v Wills* 2013 (2) SA 530 para 28.

214 Roos 2012 *SALJ* 398; see also http://site.mxit.com/pages/policies/privacypolicy (date of use: 2 August 2016). Mxit guarantees users that it will respect their privacy and right to anonymity, but also states that it abides by the law, and sometimes may be required by law to hand over information [relating to the user] to the authorities. It also informs its users of the fact that communication amongst them is not encrypted – consequently, any third party can intercept the communications, for which Mxit will not be liable.

215 Roos 2012 *SALJ* 398.

216 *Bernstein and others v Bester NO* 1996 (2) SA 751 (CC) para 67.

privacy shrinks accordingly. Roos[217] further maintains that the type of privacy setting chosen by the user should determine whether he or she still maintains or has a reasonable expectation of privacy.

As has been pointed out above,[218] if the Facebook user has utilised the privacy settings, for instance, to limit visibility to a particular group of friends (accepted into his or her network), an intrusion by a party not listed as a friend should be considered *contra bonos mores* and thus wrongful. In such circumstances, the user's expectation that his or her privacy will be respected, is reasonable.

However, it has also been pointed out that if the user has not utilised the privacy settings, or has accepted a large number of people as friends, who then have access to the user's complete profile, an acquaintance with the user's personal information by a third party will usually not be considered wrongful. It may be argued that such a user lacks the necessary reasonable expectation of privacy.

As far as the publication of the user's personal information is concerned, it was argued that if the user limits the number of friends that are allowed and utilises the privacy settings, but the privacy settings are breached and the information is made available to anyone on SNSs, such publication is *prima facie* unlawful and constitutes an infringement of privacy.[219] Arguably, if one publishes another person's photographs on SNSs without the person's consent, this amounts to an infringement of the person's right to privacy.

Furthermore, in a case where a defendant (user) uses another persons' photograph as his or her profile picture on a SNS website, the defendant's conduct infringes that persons privacy (publication of the plaintiff's photograph) and identity (false-light situation). Furthermore, this conduct may infringe on a person's identity (in cases of appropriation of name and likeness, for the defendant's advantage), where the defendant uses the SNSs profile page for commercial purposes. Therefore, in such an instance there is an overlap between the rights to privacy and to identity.

217 Roos 2012 *SALJ* 398.
218 Chapter 2 para 2.5.1.2 above.
219 Ibid.

It has been pointed out that an infringement of privacy and identity may be justified by: consent; necessity; private defence; public interest in information; public interest in art; privilege; media privilege; and fair comment.

From the above discussion it is my opinion that the common law adequately protects the infringement of privacy and identity in the context of SNSs. South African courts have already applied common-law principles in the context of SNSs, in the main cases dealing with defamation.[220] None of these cases has, however, dealt directly with the right to privacy or right to identity in the context of SNSs.

In the next section I discuss selected pieces of the legislation which limit the right to privacy.

## 3.7 LEGISLATION REGULATING THE RIGHT TO PRIVACY

This section discusses a few pieces of legislation which may justify the wrongful intrusion into the privacy of a person, or which regulate the processing of personal information. Posting personal information on Facebook, of course, also qualifies as processing personal information.[221] The Promotion of Access to Information Act,[222] the Regulation of Interception of Communications and Provision of Communication Related Information Act,[223] and the Protection of Personal Information Act[224] are the most relevant laws in the context of SNSs.[225]

---

220 *Dutch Reformed Church Vergesig Johannesburg Congregation and Another v Rayan Soknunan t/a GloryDivinee World Ministries* 2012 (6) SA 201 (GSJ); [2012] 3 All SA 322 (GSJ); *Isparta v Richter and Another* 2013 (6) SA 529 (GNP).

221 Paragraph 1.4 above on 'personal information'.

222 Act 2 of 2000.

223 Act 70 of 2002 (commonly referred to as 'RICA').

224 Act 4 of 2013.

225 Other pieces of legislation which may be relevant, albeit to a lesser extent, are the National Credit Act 34 of 2005 and the Consumer Protection Act 68 of 2008.

### 3.7.1 Promotion of Access to Information Act[226] (the PAIA)

*3.7.1.1 The scope and objects of the Act*

Although it may appear self-evident that access to one's personal information by third parties constitutes a wrongful intrusion into one's right to privacy, this intrusion may be justified in terms of section 32 of the Constitution. Section 32 provides for the right of access to information. The Constitution also provides in section 36 that the rights contained in the Bill of Rights may be limited by a law of general application. Furthermore, section 32(2) stipulates that "[n]ational legislation must be enacted to give effect to this right, and may provide for reasonable measure to alleviate the administrative and financial burden on the state".[227] This culminated in the enactment of the Promotion of Access to Information Act (the PAIA). The PAIA therefore gives effect to section 32 of the Constitution. The objects of the PAIA are to: give effect to the constitutional right of access to any information held by the state; and any information that is held by another person and that is required for the exercise or protection of any rights; to give effect to that right subject to justifiable limitations, including, but not limited to, limitations aimed at the reasonable protection of privacy, commercial confidentiality, and effective, efficient good governance; in a manner which balances that right with any other rights, including the rights in the Bill of Rights.[228]

*3.7.1.2 Access to information*

The PAIA creates a legal framework that makes it possible to request access to information held by both public and private bodies. Part 2 of the PAIA makes provision for access to the information held by public bodies, while Part 3 provides for access to information held by private bodies. This discussion focuses on the latter, since SNSs are private bodies. It is noteworthy that the PAIA does not apply to records requested for criminal or civil proceedings after the commencement of such proceedings.[229] In terms of section 50, a requester[230] may make an application for

226 Act 2 of 2000.
227 Constitution s 36.
228 Act 2 of 2000 (PAIA) s 9.
229 Section 7.

access to the records of private bodies in order to protect rights of others. In the context of SNSs, the PAIA applies to private bodies within the Republic, thus it is possible to request access to records of an SNSs within the Republic.[231] This means that access to users' information through a PAIA application is not wrongful if the request falls within the provisions of the Act.

In *Makhanya v Vodacom*[232] the court ordered the respondent (Vodacom Service Provider Company (Pty) Ltd) to supply the applicant with information relating to an unsolicited caller who had harassed the applicant with persistent, unsolicited telephone calls for several months. The infringement of the caller's privacy was justified by the fact that such access is authorised by the PAIA.

Mxit, a South African SNS, states in its privacy policy that the information or communications of its users may be given to authorities if the law requires it to do so.[233] Once a user agrees to these terms set by Mxit, he or she gives implied consent to the terms.

### 3.7.2 Regulation of Interception of Communications and Provision of Communication Related Information Act[234] (the RICA)

*3.7.2.1 The scope and objects of the Act*

Interception of any form of communication is *prima facie* an act of intrusion, which amounts to an infringement of privacy, unless justified by a ground of justification.[235] The right to privacy enshrined in the Constitution specifically recognises the privacy of people's communications.[236] The Regulation of Interception of Communications

---

230 Section 1, "requester in relation to a private body means any person, including, but not limited to, a public body or an official thereof, making a request for access to a record of that private body or a person acting on behalf of the person making such a request".

231 Section 50.

232 *Makhanya v Vodacom* 2010 (3) SA 79 (GNP) paras 5, 18.

233 See http://site.mxit.com/pages/policies/privacypolicy (date of use: 6 August 2016).

234 Act 70 of 2002.

235 Section 1 distinguishes between two types of communication: direct communication and indirect communication.

236 Constitution s 14(d).

and Provision of Communication Related Information Act (the RICA)[237] creates a legal framework for the protection of the arbitrary interception of a communications and the Act now regulates any interception of a communication. The RICA, amongst its provisions, requires that all cell phone owners must register their sim-cards with their respective 'service providers'.[238]

The RICA regulates:

- the interception of certain communications, the monitoring of certain signals and radio frequency spectrums, and the provision of certain communication-related information;
- the making of applications for, and the issuing of directions authorising, the interception of communications and the provision of communication-related information under certain circumstances; and
- the execution of directions and entry warrants by law enforcement officers and the assistance to be given by postal service providers, telecommunication service providers, and decryption key holders in the execution of such directions and entry warrants.

*3.7.2.2 Interception of communications*

The RICA contains a general prohibition on the intentional or attempted interception of any communication in South Africa in the course of its occurrence or transmission.[239] There are exceptions to this general prohibition in the Act.[240] Intentional interception of communication is allowed if the interception is under an

237 Act 70 of 2002. Another notable reason for this Act may be the availability of cheaper cellular phones, which has made the ownership of cellular phones easier and more widespread. In addition, due to the fact that a person may now own multiple sim-cards, it became imperative to introduce legislation which regulates, amongst others, the ownership and registration of sim-cards.

238 Ibid s 1 states that: "Sim-card means the Subscriber Identity Module which is an independent, electronically activated device designed for use in conjunction with a cellular phone to enable the user of the cellular phone to transmit and receive indirect communications by providing access to telecommunication systems and enabling such telecommunication systems to identify the particular Subscriber Identity Module and its installed information. The network company that either issued the Sim-card or provides the network where the user has moved to another network".

239 Ibid s 2 which provides that authorising or procuring another person to intercept a communication is also prohibited.

240 Ibid ss 3-9; also see Roos "Data privacy law" 392-5.

interception direction,[241] if the interception is by a party to the communication,[242] or if it takes place with the consent of a party to the communication.[243] The interception of an indirect communication in connection with the carrying on of a business is also permitted,[244] as is the interception of communication to prevent serious bodily harm[245] or to determine a person's location in an emergency.[246] Interception of communication is also allowed when the interception is authorised by certain other Acts.[247]

*CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens*[248] provides some interesting facts to consider in the light of the RICA. The case dealt with an interlocutory application. The applicant brought an *ex parte* application on an urgent basis, asking to be allowed to use a substituted service to serve the defendant with a notice of the date set for the trial and pre-trial conference via Facebook (by sending the notice to the defendant's inbox).[249] From the background to this case, it appears that the defendant evaded the applicant's (plaintiff in the matter) notices, which is the reason the applicant sought a substituted service. The applicant and his attorney submitted a supplementary affidavit on the status of the defendant's Facebook profile. It is not clear from this supplementary affidavit whether or not the applicant and his attorney had obtained the necessary court order permitting them to intercept the defendant's communications on Facebook. In the event that the necessary court order had not been obtained, it is arguable that the action of the applicant and his attorney violated the regulations of the RICA[250] and the defendant's right to privacy. When the interception of communication is authorised by an order of court, such an

241 Act 70 of 2002 s 3; also see s 1: "Interception direction" means "a direction issued under s 16 (4) or s 18(3)(a) and which authorises the interception, at any place in the Republic, of any communication in the course of its occurrence or transmission, and includes an oral interception direction issued under s 23(7)".

242 Ibid s 4.

243 Ibid s 5.

244 Ibid s 6; also see s 1: 'indirect communication' means "the transfer of information, including a message or any part of a message, whether in the form of speech, music or other sounds; data; text; visual images, whether animated or not; signals or; radio frequency spectrum - or in any other form or in any combination of forms, transmitted in whole or in part by means of a postal service or a telecommunication system".

245 Ibid s 7.

246 Ibid s 8.

247 Ibid s 9; for instance in terms of the provisions of the Correctional Services Act 111 of 1998.

248 2012 (5) SA 604 (KZD).

249 Ibid para 2.

250 Act 70 of 2002.

intrusion is justified.[251] The definition of 'intercept' in the RICA[252] provides some guidelines to determine when interception has occurred. In the *CMC Woodworking Machinery (Pty) Ltd* case, it may be argued that even if one assumes that the defendant (user) had not employ privacy setting on its Facebook profile, the conduct of the applicant and his attorney amounted to an interception as neither of them was a recipient or intended recipient of the defendant's communications. And clearly the interception did not fall within any of the exceptions.[253] On the other hand, if the applicant or his attorney befriended the defendant on Facebook, there would have been no interception on their part, as they would be recipients or intended recipients of the defendant's communications. If this was the case the applicant could have relied on consent as a ground of justification were interception to be alleged.

### 3.7.3 Protection of Personal Information Act 4 of 2013 (the POPI Act)

*3.7.3.1 Objects and scope of the Act*

The purpose of the POPI Act is to give effect to the constitutional right to privacy by: safeguarding personal information; regulating the manner in which personal information may be processed; providing persons with rights and remedies to protect personal information; and establishing an Information Regulator, in order to ensure respect for and promotion, enforcement, and fulfilment of the rights protected by the Act.[254]

The Act applies to the processing of personal information in both the private and public sectors. Personal information is defined as information which relates to an identifiable individual (or data subject) and which is entered into a record by a

---

251 Ibid s 3.

252 Ibid s 1. Interception means "the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the monitoring of any such communication by means of a monitoring device, viewing, examination or inspection of the contents of any indirect communication; and diversion of any indirect communication from its intended destination to any other destination".

253 Ibid ss 3-9.

254 Act 4 of 2013 s 2.

responsible party. [255] A responsible party is a party who determines the purpose and means of such processing.[256] A record includes sound, image, and other electronic information.[257] The Act applies to responsible parties domiciled in South Africa or abroad if they process information using means situated in South Africa.[258] The Act defines 'processing'[259] 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.

The responsible party is accountable for the processing of personal information that is done pursuant to such responsible party's directions. In the context of SNSs, the Internet Service Providers (ISP), application providers, and users of the SNS could all potentially be regarded as responsible parties. The ISP (in this context, the SNSs operator) processes the personal information of users (who are the data subject in that situation), and the users, on the other hand, process personal information of other persons (third parties) when they upload the third parties' personal information. The majority of information uploaded by SNS users (written comments, photographs, or videos) is personal information. Due to the wide definition given to processing, almost any action performed in relation to the information is regarded as the processing of information.

---

255 Ibid s 1. When the POPI Act came into operation it amended the definition of 'personal information' for both the Electronic Communications and Transactions Act and the Promotion of Access to Information Act.

256 Section 2 defines a 'responsible party' to mean "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". Van der Merwe et al *ICT Law* 370 notes that in this context the term 'responsible party' is synonymous with 'data controller'.

257 Ibid s 1. The Act defines a 'record' as "including writing on any material, information recorded on any electronic and computer equipment, labels, books, maps, plans, graphs, drawings, photograph, film, tape or other devices embodying visual images".

258 Act 4 of 2013 s 3.

259 Ibid s 1.

The POPI Act excludes from its scope of application any processing of personal information during the course of a purely personal or household activity,[260] or for exclusively journalistic, literary, or artistic purposes.[261] The question arises whether individual users of SNSs who process personal information of friends for personal purposes (sharing news and photographs) could be excluded from the provisions of the POPI Act under the household exception.

It is submitted that the situation should be evaluated on a case-by-case basis. Not every user of an SNS does so purely for social interaction. SNS websites may also be used for commercial purposes to advertise a product or service. In such an instance the household exception would not apply.

*3.7.3.2 Conditions for processing of personal information*

In order for the processing of personal information to be lawful, the POPI Act requires the responsible party to comply with the conditions for lawful processing.[262] The POPI Act sets out conditions which the responsible party must adhere to when processing personal information.[263] There are eight information protection conditions: accountability; processing limitation; purpose specification; further processing limitation; information quality; openness; security safeguards; and data subject participation. These conditions are similar to the information-protection principles found in the OECD Guidelines[264] and the EU Data Protection Directive.[265] The latter two international instruments are discussed in Chapter 5 below.

Should a SNS user be considered a responsible party within the meaning of the Act, and not afforded the household exception, such user will have to comply with the conditions for processing set out in the POPI Act. This means that the responsible party must comply with the conditions for lawful processing of personal information

260 Act 4 of 2013 s 6(1)*(a)*.
261 Ibid s 7.
262 Sections 4, 8-25.
263 Ibid s 4 provides a brief summary of the conditions which are dealt with in Ch 3 of the Act; Van der Merwe et al *ICT Law* 367-80.
264 Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data.
265 Directive 95/46/EC; see also Roos "Data Privacy Law" in Van der Merwe et al *ICT Law* 371.

set out in Chapter 3 of the Act. These conditions are not discussed further in this dissertation.

## 3.9 PROCEDURAL CHALLENGES

### 3.9.1 Introduction

This section focuses on the procedural challenges involved when a user's right to privacy or identity has been infringed on SNSs. The plaintiff must show a cause of action in order to receive the appropriate relief. In this section I consider the following issues: identifying the wrongdoer on SNSs; the role of an Internet service provider; and legal costs, which may be prohibitive.

### 3.9.2 Identifying the wrongdoer

If a plaintiff wishes to sue for an *iniuria*, he or she must know the identity of the wrongdoer.[266] In cases where there has been an infringement of either privacy or identity on SNSs, the plaintiff can only identify the defendant's SNSs profile. This approach on its own is not conclusive and raises a number of challenges. For instance, the user's profile may be a fake or even an anonymous profile. On the other hand, the advancement in technology makes it possible for the identity of the defendant (user) to be revealed, be it lawfully or unlawfully.[267] Nel[268] notes that

> [m]any defendants in internet defamation actions [the same applies to privacy and identity infringement] claim that revealing their identity for purpose of a defamation suit would be a violation of their constitutionally protect right to free speech, and in some instances even their right to privacy.

---

266 Civil Procedure in Magistrates' Courts Rule B.i; Rule A7.1 and Civil Procedure in the Superior Courts Rule A6.1.The question as to whether or not a particular party has standing to sue and be sued may be dealt with on exception, in which event that party's allegations concerning its legal standing must be accepted as being correct; see also Harms *Amler's Precedents of Pleadings* 72.

267 These are technical, not legal issues which fall outside the scope on this dissertation.

268 Nel 2007 *CILSA* 194.

SNSs or the Internet in general, provide a space where users may communicate or post information using an anonymous profile or pseudonym. Amongst the reasons for communicating anonymously online is to prevent the association of speech with the speaker's identity.[269] Communicating anonymously may allow the user freedom of expression;[270] however, it is clear that the right to freedom of speech cannot be exercised in a way that infringes upon the interests of others whose interests also warrant legal protection from infringement. According to Nel[271]

> ….anonymity may lead to crime, and…that anonymity may undermine free speech in the sense that anonymous speakers face no consequences for speaking carelessly, callously or even criminally.

A proper balance must be struck between the user's need for anonymity and the protection of the plaintiff's personality interests (privacy and identity in this context) from infringement. The task of identifying an anonymous wrongdoer may require sophisticated technical skills, and it is important that whatever method is used to establish the identity must be within the confines of the law.[272] Nel[273] suggests that South Africa could use disclosure (discovery) proceedings. She proposes an extension to rule 35 of the Uniform Rules of Court[274] (rule 23 in the magistrate's court).[275] The rules of court make no provision for discovery before the

---

269 Nel ibid 193, notes that "the ability to conceal one's identity while communicating, has the social benefit of encouraging uninhibited speech, which makes the internet desirable for those who feel persecuted or embarrassed or wish to raise issues which they might consider controversial"; also see Collingwood 2012 *Comp L & Security Rev* 329.

270 Constitution s 16(2) the right in subsection (1) [right to freedom of expression] does not extend to: propaganda; incitement of imminent violence; or advocating hatred based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm.

271 Nel 2007 *CILSA* 198.

272 Act 25 of 2002; Act 70 of 2002; and Act 4 of 2013.

273 Nel 2007 *CILSA* 210 ff.

274 Supreme Court Act 59 of 1959, Uniform Rules of Court 35 Discovery, Inspection and Production of Documents:

> (1) Any party to any action may require any other party thereto, by notice in writing, to make discovery on oath within twenty days of all documents and tape recordings relating to any matter in question in such action (whether such matter is one arising between the party requiring discovery and the party required to make discovery or not) which are or have at any time been in the possession or control of such other party. Such notice shall not, save with the leave of a judge, be given before the close of pleadings.

275 Magistrates' Courts Act 32 of 1944, Civil Procedure Rules in Magistrates' Courts Rule 23 Discovery of Documents**:**

> (1) After the close of pleadings, but not later than 15 days before the date of trial, either party may deliver a notice to the other party calling on him to deliver a schedule specifying the books and documents in his possession or under his control which relate to the action and which he intends to use in the action or which tend to prove or disprove either party's case. Such schedule, verified by affidavit, shall be delivered by the party required to do so within 10 days after the delivery of the aforesaid notice. If privilege be

commencement of an action.[276] She suggests that the extension should allow the discovery proceeding to be instituted before commencement of an action and that the applicant be permitted to request a subpoena against the ISP. Drawing on cases where applications for obtaining discovery before commencement of an action were refused, Nel notes the following guidelines:[277]

- it should be not be used as a 'fishing' expedition;
- the applicant should not have another alternative remedy available to him (for instance the applicant should have already applied for a take-down notice in terms of the ECT Act);
- the applicant cannot obtain discovery against one person for the purpose of bringing action against another person (this means that an applicant cannot apply for discovery in respect of 'friends' of the possible defendant); and
- the court will not come to the assistance of a litigant in this way in order to enable him to ascertain whether or not he has a cause of action.

This area of the law is not well developed in South Africa and it is therefore useful to look at the developments in United States[278] and United Kingdom[279] for guidance in future developments in South Africa.

### 3.9.3 Internet Service Provider

Here I briefly consider the position of an Internet Service Provider (ISP) – I examine the situation where a user, or another person, has suffered injury to his or her privacy or identity and seeks to determine whether or not the ISP can be held liable for the actions of its users. In other words, the plaintiff seeks to hold the ISP liable for

---

claimed for any of the books or documents scheduled, such books or documents shall be separately listed in the Schedule and the ground on which privilege is claimed in respect of each shall be set out.

276 Cilliers, Loots & Nel *Civil Practice of the High Court* 779; also see *Priday v Thos Cook & Son (SA) Ltd* 1952 (4) SA 761 (C) 764; *Walsh v Botha* 1960 (2) SA 323 (O) 325F-G.

277 Nel 2007 *CILSA* 210 ff.

278 Paragraph 4.5.2 below.

279 Pararaph 5.4.3.1 below.

content supplied by a third party. This may happen where the identity of the infringing user cannot be established, or where the defendant is a man of straw.

An ISP, in most instances, grants access to its SNS or network without requiring any form of positive identification or verification of identity from its users. It is not feasible for an ISP to control who uses its SNS or verify the user's personal information upon registration. This fact is humorously captured in Peter Steiner's cartoon entitled *'On the internet, nobody knows you're a dog'.*[280]

The question of whether or not liability is imposed depends on the function or role played by the particular ISP.[281] Where the ISP provides content on the SNS it is clear that the ISP may be sued where the content injures a person's privacy or identity.[282] In the context of SNSs, the ISP does not provide content; most of the content is generated by users. The problem arises where a plaintiff wishes to sue the ISP on the basis of it being liable for the actions of the users of its service.

Chapter XI of the Electronic Communications and Transactions Act limits the liability of service providers[283] for the transmission, routing, temporary storing, caching, or hosting of unlawful material, provided they meet the conditions for eligibility.[284] The service provider must belong to an industry representative body recognised by the Minister of Communications, and the ISP must have adopted and implemented the code of conduct of that body.[285]

---

280 The cartoon symbolises an understanding of Internet privacy which stresses the ability of users to send and receive messages in general anonymity. The cartoon can be viewed at www.google.co.za/search?q=on+the+internet+nobody+knows+you+re+a+dog+cartoon (date of use: 20 December 2016).

281 Roos "Data privacy law" 417.

282 Ibid.

283 Act 25 of 2002 s 70 'service provider' is defined as any person providing information system services.

284 Section 72 provides that the limitations on liability established by this Chapter apply to a service provider only if:

*(a)* the service provider is a member of the representative body referred to in section 71; and

*(b)* the service provider has adopted and implemented the official code of conduct of that representative body.

285 Section 72; http://www.ispa.org.za, the 'Internet Service Provider Association' (ISPA) is a recognised industry representative body.

In the event of the service provider acting as a 'mere conduit' (also referred to as an 'information carrier' in some jurisdictions),[286] the information is merely conveyed from one point to another without any monitoring of or control over the content. Section 73(1) exempts a service provider who transmits, routes, stores, or provides access to data from liability for such activity if: the service provider does not initiate the transmission; does not select the addressee; performs the functions in an automatic, technical manner without selection of the data; and does not modify the data contained in the transmission.[287] The acts of transmission, routing, and provision of access must be performed for the sole purpose of transmitting information. [288]

Section 74(1) exempts a service provider who caches[289] information (also referred to as the 'information distributor' in some jurisdictions) from liability under certain conditions. A service provider that transmits data provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, provided that the service provider does not modify the data; complies with conditions on access to the data; complies with rules regarding the updating of the data, specified in a manner widely recognised and used in the industry; does not interfere with the lawful use of technology, widely recognised and used in the industry, to obtain information on the use of the data; and removes or disables access to the data it has stored upon receiving a take-down notice referred to in section 77.[290]

Section 75(1) provides that a service provider that acts as a 'host' of, for example, a website (also referred to as an' information controller' in some jurisdictions),[291] is not liable for damages arising from data stored at the request of the recipient of the service, provided that the service provider does not have actual knowledge that the data message, or an activity relating to the data message, is infringing the rights of a

286 See Chapters 4 and 5 below.
287 Act 25 of 2002 s 73(1)*(a)-(d)*.
288 Act 25 of 2002 s 73(2).
289 Section 1, 'cache' means high speed memory that stores data for relatively short periods of time, under computer control, in order to speed up data transmission or processing.
290 A 'take-down notice' is discussed below under remedies, para 3.10.2.
291 See Chapters 4 and 5 below.

third party; or is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and upon receipt of a take-down notification referred to in section 77, acts expeditiously to remove or to disable access to the data. Section 75(2) provides that the limitation of liability will only apply if the service provider has designated an agent to receive notifications of infringement, and has provided through its services (including on its web sites in locations accessible to the public) the name, address, phone number, and e-mail address of that agent. A competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law, notwithstanding this limitation of liability.[292]

Where a service provider provides information location tools:[293]

> A service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the service provider—
>
> (*a*) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of that person;
>
> (*b*) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;
>
> (*c*) does not receive a financial benefit directly attributable to the infringing activity; and
>
> (*d*) removes, or disables access to, the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to such data message, infringes the rights of a person.

Therefore, in the context of SNSs, where a service provider falls within the above categories and has further complied with the requirements set out in Chapter XI (Limitation of liability of Service Providers) of the Electronic Communications and Transactions Act, the service provider may not be held liable for the unlawful or wrongful actions of its users, even though the user may be using the service anonymously or is a man of straw.

---

292 Act 25 of 2002 s 75(3).

293 Ibid s 76*(a)-(d).*

In the following section I consider the remedies available to a plaintiff whose personality rights have been infringed on SNSs.

## 3.10 REMEDIES

### 3.10.1 Introduction

A person whose personality has been infringed or who is under threat of possible infringement due to a publication on a SNS, has a number of remedies which he or she might consider.

### 3.10.2 Take-down notification

In a case where a person's privacy or identity has been infringed on SNSs, he or she may lodge a complaint with the ISP requesting that the infringing content be taken down (that is, removed) from the site. The Internet Service Provider's Association (the ISPA), assists complainants with queries, where the ISP concerned is a member of the ISPA.[294] The ISPA uses the procedure prescribed by the take-down notification process in section 77 of the ECT Act.[295] Section 77 provides that a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent, and must include the following

(a) the full names and address of the complainant;

(b) the written or electronic signature of the complainant;

(c) identification of the right that has allegedly been infringed;

(d) identification of the material or activity that is claimed to be the subject of unlawful activity;

(e) the remedial action required to be taken by the service provider in respect of the complaint;

294 See http://www.ispa.org.za/code-of-conduct/take-down-procedure/ (date of use: 20 December 2016).

295 Ibid.

(f) telephonic and electronic contact details, if any, of the complainant;

(g) a statement that the complainant is acting in good faith;

(h) a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct.

A person, who makes use of the take-down procedure in section 77, knowing that the notification materially misrepresents the facts, is liable for damages.[296] A service provider who takes down material in response to a notification, cannot be held liable if the take-down turns out to be wrongful. [297]

The terms and conditions on Facebook provide for a take-down notice. However the court in *Heroldt v Wills*,[298] held as follows:[299]

> There is nothing before me to assure me that Facebook would comply with such a request, … if one wants to stop wrongdoing, it is best to act against the wrongdoers themselves.

In the context of SNSs, a take-down notice seems to be an effective remedy of first instance for a person whose privacy or identity has been infringed, provided the ISP adheres to the take-down notice requests from users or non-users. If this type of remedy could be used successfully, it would help avoid the expensive process of litigation.

### 3.10.3 Interdict

An interdict is an order of court enjoining a respondent to refrain from doing something (a 'prohibitory interdict'), or ordering a respondent to do something (a 'mandatory interdict').[300] An interdict is either interim or final. An interim interdict is a court order that preserves and restores the *status quo* pending the final

296 Act 25 of 2002 s 77(2).
297 Ibid s 77(3).
298 *Heroldt v Wills* 2013 (2) SA 530 para 38.
299 Ibid.
300 Civil Procedure in the Superior Courts Rule A5.1; Civil Procedure in the Magistrates' Courts Rule A2.1.

determination of the rights of the parties.[301] An injured party or a party whose personality interests are threatened, may apply to court for an interdict.[302] An interdict will be granted where there is a threat of infringement or continued infringement of either privacy or identity. The case of *Setlogela v Setlogela*[303] laid down the requirements for a final interdict: a clear right; an injury actually committed or reasonably apprehended; and the absence of another suitable remedy. The same requirements apply to an interim interdict, with the addition of one requirement: the applicant must also prove that the balance of convenience favours the granting of an interim order.[304] In terms of the interim interdict actual harm need not be established on a balance of probabilities.[305]

In the case of *Heroldt v Willis,*[306] the applicant sought an order against the respondent in the following terms: interdicting and restraining the respondent from posting any information relating to the applicant on Facebook or any other social media (the respondent had refused to remove the posting, despite having been requested to do so by the applicant, acting through his attorney). The applicant further sought, in the event that the respondent failed to comply with the above request, that the court place the respondent under arrest for non-compliance with the order for a period of 30 days, or as determined by the court. The court did not agree to this latter request.[307]

In this case, the first two requirements for an interdict, as laid down in *Setlogela* v *Setlogela*, were complied with, namely that the applicant had a clear right to his privacy and the protection of his reputation, and had been defamed.[308] The only issue was with regard to the third requirement: the absence of a suitable remedy. The respondent drew attention to the fact that the applicant had previously, *via* his attorney, threatened to institute an action to claim damages. The respondent

301 Civil Procedure in the Superior Courts Rule A5.6.
302 Neethling, Potgieter & Visser *Delict* 237; also see Roos 2008 *PER* 90.
303 *Setlogelo v Setlogelo* 1914 AD 221 227.
304 Civil Procedure in the Superior Courts Rule A5.7.
305 Ibid.
306 *Heroldt v Willis* 2013 (2) SA 530 para 31.
307 Ibid para 41.
308 Ibid para 30.

suggested that if she was found to have defamed the applicant, his proper remedy would be damages.[309]

The court granted the interdict and ordered the respondent to remove all postings which she had made on Facebook or any other social media site in reference to the applicant. In this case, the court deviated from the conservative requirements for an interdict. Willis J[310] held that:

> 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 social media form a subset of the electronic media but are not coextensive with it: the social media are all part of the electronic media but not all the electronic media are social media. The electronic media were, almost certainly, beyond the imagination of the court when *Setlogelo v Setlogelo* was decided in 1914. Not only can items be posted and travel on the electronic media at a click on a computer in a moment, in an instant, at the twinkling of an eye, but also they can, with similar facility, be removed therefrom. This can also be done at minimal cost. The situation is qualitatively different from the scenario where newspapers have been or are about printed in hardcopy and distributed. 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.

It is evident that in the context of SNSs an interdict provides immediate and effective relief to the plaintiff (user or non-user), and minimises the harm to the plaintiff's (user or non-user) personality interests (privacy and identity in this instance).

### 3.10.4 Protection from Harassment Act 17 of 2011

#### *3.10.4.1 The scope and object of the Act*

The Protection from Harassment Act[311] commenced on 27 April 2013. One of the objectives of the Act is to afford victims of harassment an effective remedy against such conduct. Harassment is defined as conduct that the defendant knows, or ought to know, causes harm to the plaintiff by, inter alia, unreasonably engaging in

309 Ibid para 30.
310 Ibid para 31.
311 Act 17 of 2011.

electronic communication aimed at the complainant or a related person, whether or not conversation ensues; or sending, delivering, or causing the delivery of electronic mail to the complainant or a related person.[312] 'Harm' is defined as any mental, psychological, physical, or economic harm.[313] Postings on an SNS infringing on the plaintiff's privacy could, therefore, amount to harassment in terms of this Act.

*3.10.4.2 Protection order*

A complainant may apply to a magistrate's court for a protection order against the harassment.[314] If the complainant is not represented by a lawyer, the clerk of the court must assist him or her by informing him or her of the relief available in terms of the Act, as well as informing him or her of the right to lodge a criminal complaint of *crimen iniuria* against the defendant.[315] A child may also apply for a protection order without the assistance of a parent or guardian.[316]

A court must consider an application as soon as reasonably possible, and may consider additional evidence as it deems fit – for example, oral evidence or written affidavits.[317] The court may issue an interim protection order against the respondent in a situation where the respondent failed to receive notice of the application. The court, however, must be satisfied that there is *prima facie* evidence that the respondent is engaging in or has engaged in harassment and that harm is being or may be suffered by the complainant or a related person as a result of the harassment if a protection order is not issued immediately. The court must also be satisfied that the protection to be accorded by the interim protection order is likely not to be achieved if prior notice of the application is given to the respondent.[318] The interim order must be served on the respondent who may then show cause on the return date, why the interim order should not be made final.[319]

312 Ibid s1.
313 Ibid s 1.
314 Ibid s 2(1)
315 Ibid s 2(2).
316 Ibid s 2(4).
317 Ibid s 3(1).
318 Ibid s 3(2).
319 Ibid s 3(3).

In cases where the complainant is being subjected to abuse via anonymous, threatening or offensive SMSs, e-mail, etcetera, and he or she is therefore unaware of the harasser's personal details, the court is authorised to issue a directive to an electronic communications service provider demanding the full name, identity number, and address of the harasser sending the text messages, tweets, or e-mails.[320]

The effectiveness of the protection order is ensured by the fact that whenever it issues a protection order or interim protection order, the court must also make an order authorising the issue of a warrant for the arrest of the respondent should the subject not comply with the prohibition, condition, obligation, or order it has imposed.[321]

Given that a complainant may approach a magistrate's court for a protection order, that the order must be given as soon as reasonably possible, and that a warrant for the arrest of the respondent is issued should he or she fail to comply with an order, it is clear that the Protection from Harassment Act provides an inexpensive and effective civil remedy against harassment on SNSs.

### 3.10.5 Claim for damages

In this section I deal with the claim for damages where users' or other persons' personality rights have been infringed on SNSs.[322] Potgieter, Steynberg and Floyd[323] define damage as the diminution, as a result of a damage-causing event, of the utility or quality of a patrimonial or personality interest in satisfying the legally recognised needs of the person involved. Damage consists of both patrimonial and non-patrimonial loss.[324] Neethling[325] holds that in a case where a party has suffered patrimonial loss caused by an *iniuria*, the *actio legis Aquiliae* must be instituted. These authors assert that in practice, the *actio iniuriarum* and *actio legis Aquiliae*

320 Ibid s 4. See also Sewsunker 2013 *De Rebus* 34.
321 Ibid s 11.
322 This section does not look at how the damage is assessed.
323 Potgieter, Steynberg & Floyd *Law of Damages* 20.
324 Ibid 33.
325 Ibid 67.

may be instituted in a single action to claim satisfaction and patrimonial damages, but a plaintiff must make the necessary averments in his or her pleadings to support both actions.[326]

A claim for damages may not always be a useful remedy for infringement of personality on SNSs. The plaintiff may face various stumbling blocks in claiming damages: For example, the identity of the wrongdoer may not be known and as a consequence another procedure has first to be followed to establish such identity. In a case where the identity of the wrongdoer is known, the defendant may be a man of straw, meaning the plaintiff may never be able to receive the damages awarded.

Having considered all the above remedies, the interdict and a protection order under the Harassment Act possibly offer the most effective legal relief in the context of SNSs. Plaintiffs could also consider alternative dispute resolution procedures in preference to litigation as these are often less costly and offer relief within a reasonable time, which helps reduce further damage to the plaintiff's personality rights.[327]

## 3.11 SUMMARY

This chapter focused on the challenges highlighted in Chapter 2. I looked at the two personality rights – privacy and identity – and examined how they have been recognised and developed in South African law, as well as how they may be infringed. The possible grounds of justification that exclude the wrongfulness of infringing conduct were also considered. The chapter further explored the infringement of these personality rights in the context of SNSs and the possible grounds of justification in this regard. I addressed the procedural challenges where either privacy or identity has been infringed in the context of SNSs and finally identified possible remedies available to a plaintiff whose personality has been infringed on an SNS.

326 Ibid 68.
327 Levmore & Nussbaum *The Offensive Internet* 26.

# Chapter 4

# United States of America

## 4.1 INTRODUCTION

In this chapter I discuss the legal position in the United States of America (United States), with particular reference to the protection of the rights to privacy and identity in the context of SNSs. I investigate whether the United States recognises and protects these rights, particularly in the context of SNSs.

The chapter is structured as follows: a brief overview of the United States legal system is given as background to the discussion; the recognition and development of the right to privacy in the United States is discussed; the current constitutional and common-law positions regarding the right to privacy are explained; legislation relevant to SNSs is identified; a comparison is made between a few of the individual states' laws; the application of the established legal principles in the context of SNSs is discussed; procedural challenges are highlighted; and I conclude the discussion with a brief analysis.

## 4.2 OVERVIEW OF THE LEGAL SYSTEM

The United States is a common-law country, in other words the legal system is modelled on the British common-law system.[1] The United States has a Constitution[2] which establishes a federal system of government. In total, the country is made up of 50 states each enjoying a measure of legal independence. The federal government is given specific powers in terms of the Constitution. All powers not specifically granted to the federal government, remain with the states. In the case of conflict

1 Lomio & Spang-Hanssen *Legal Research Method* 13. The American state of Louisiana is the exception as it is regarded as a civil-law state 11.

2 Ibid 10.

between federal and state law, federal law applies.[3] Each state has its own Constitution, government structures, laws, and its own judiciary. The United States Supreme Court and the lower federal courts[4] have jurisdiction to adjudicate on federal laws as well as the United States Constitution. The individual state Constitutions and the laws of each state create state courts, lower courts, and higher courts. The lower courts are referred to as Circuit or District courts. The highest courts are known as Supreme Courts or Courts of Appeal.

The different states may offer different approaches and solutions to the same problem. This provides possible alternative solutions for South African law to consider.

In the following section I look at the recognition of the rights to privacy and identity in the United States. I focus on the following areas: constitutional law; common law; statutory law; and secondary sources.

## 4.3 THE RIGHT TO PRIVACY AND IDENTITY

### 4.3.1 Recognition and development

#### *4.3.1.1 Privacy*

In the United States, the development of hand-held cameras and sensationalist journalism in the 1890s were just a few of the issues which raised concern over privacy and stimulated a discourse on the topic.[5] Other issues included the development of various technologies, such as telephone wiretaps, lie detectors, personality tests, and cameras.[6]

---

3 United States Constitution art VI s 2 declares federal law to be 'the supreme law of the land'.

4 United States Constitution art III, s 1.

5 Solove, Rotenberg & Schwartz *Information Privacy Law* 9-10.

6 Li *Center for Democracy and Technology* 43; Westin *Social and Political Dimensions of Privacy* 435, according to Westin, this period marked the rise of information privacy as an explicit social, political and legal issue of the high-technology age.

The development of the concept of privacy in the United States legal system can be traced back as far as 1890.[7] Before then there was no clear recognition of the right to privacy, either in the United States Constitution or in case law.[8] In that year, two American lawyers, Samuel Warren and Louis Brandeis, wrote their famous article "The Right to Privacy" in which they urged that an invasion of privacy tort action (delictual action) should be developed to protect 'inviolate personality'.[9] Their main concern was that information about an individual's personal life should not be revealed to the public by the press.[10] They argued that a right to privacy is implied at common law in the United States and expressed as 'the right to be left alone'. The courts[11] and legislatures[12] of the different states started to apply the tort of privacy invasion, also to situations other than those where private information had been published.

Another scholar who had a profound impact on the development of the privacy tort was Prosser. According to modern-day privacy scholars, Richards and Solove, "[w]hereas Warren and Brandeis planted the germinal seed for tort privacy, Prosser systematized and organized the law, giving it an order and legitimacy that it had previously lacked."[13] Prosser analysed privacy court cases and in 1960 wrote an article "Privacy" in which he declared that what emerged from those decisions was that the privacy tort was not a single tort, but a complex of four torts, protecting four different interests tied together by the common name 'right to privacy', but otherwise having almost nothing in common save that each represented an interference with a

---

7 *Boyd v United States* 116 US616 (1886) can be considered as the first case in which privacy was protected, although privacy as a concept was not specifically defined. The court referred to "the sanctity of a man's home and the privacies of life".

8 Street & Grant *Law of the Internet* 111.

9 Warren & Brandeis 1890 *Harv L Rev* 193 198-205. Also see Allen 2012 *Fordham L Rev* 1187 1202; Richards & Solove 2010 *Cal L Rev* 1887-8.

10 Roos *Data (Privacy) Protection* 28-9.

11 The Georgia Supreme Court was the first state court to recognise the existence of a right to privacy (*Pavesich v New England Life Insurance Co* 122 Ga 190, 50 SE 68 (1905)). *Pavesich* became the leading case, and in 1938 the first Restatement of Torts s 867 recognised a cause of action against anyone who "unreasonably and seriously interferes with another's interest in not having his affairs known to others or his likeness exhibited to the public" (see Roos *Data (Privacy) Protection* 30 n 23; McQuoid Mason *Privacy* 36-7; Roline & Skalberg 2004 *ALSD Journal of Employment Law and Labor Law* 78.

12 New York state adopted the first privacy legislation in 1903 (NY Sess Laws 1903 ch 132 ss 1-–2). See further Roos *Data (Privacy) Protection* 30 n 23.

13 Richards & Solove 2010 *Cal L Rev* 1887-8.

plaintiff's right 'to be let alone'.[14] I consider these torts in greater detail below under the section on common law.

#### *4.3.1.2 Identity*

Unlike the position in South Africa, the right to identity does not exist as an independent personality right in the United States. As I have pointed out,[15] in South Africa the right to identity has developed from two of the four United States privacy torts – the false-light tort (publicity which portrays the plaintiff in a false light in the public's eye), and the appropriation tort (appropriation, to the defendant's advantage, of the plaintiff's name or likeness). In essence, the right to identity is, therefore, protected under the guise of the right to privacy, but one cannot speak of an identity tort as such in the United States. A right of publicity has recently been developed – this is discussed in greater detail below. It is unclear whether this right should be categorised as a right to identity, an intellectual property right, or both.[16]

Identity theft as a crime does exist; in fact the United States Congress has passed a number of laws to combat identity theft.[17] I do not, however, deal with it in this study, as the study focuses on the private-law consequences of SNSs, and identity theft forms part of criminal law.

---

14 Prosser 1960 *Cal L Rev* 383 385-8. These four torts will be discussed in greater detail below.

15 Chapter 3 para 3.5.2 above.

16 Bartholomew 2011 *Connecticut Law Review* 305-06.

17 Identity Theft Assumption and Deterrence Act of 1998. It terms of 18 USC s 1028, it is a crime "to knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet … any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under applicable state or local law".

### 4.3.2 Common law

I have already pointed out[18] that in the United States the right to privacy is recognised and protected in terms of common law. As said, whilst the famous article written by Warren and Brandeis introduced the concept of the right to privacy, Prosser had a profound impact on the structure and future development of the tort of privacy invasion.[19]

Prosser analysed over 300 cases in which aspects of privacy were protected. He then organised these torts into four categories. He described these four torts as: intrusion upon a plaintiff's seclusion or solitude, or into his or her private affairs; public disclosure of embarrassing private facts about a plaintiff; publicity that places a plaintiff in a false light in the public eye; and appropriation, for the defendant's advantage, of a plaintiff's name or likeness.[20] Prosser's four-tort framework was widely accepted, and in 1977 the Restatement (Second) of Torts accepted this classification.[21] Although the Restatement is regarded as a secondary source which courts are not bound to follow, case law does refer to it.[22]

Recently Prosser's division of privacy into four torts has met with some criticism from scholars. Richards and Solove note that these four categories of privacy torts are narrow and rigid. [23] The classification of privacy into four specific torts has, for them, stultified the development of privacy, and limited its adaptability to evolve in response to the technological changes over the last 50 years.[24]

According to Cohen,[25] "it is becoming increasingly clear that the common law invasion of privacy torts will not help to contain the destruction of informational privacy." Powell[26] concurs, and holds that technological developments necessitate

---

18 See par 4.3.1.1 above.
19 Richards & Solove 2010 *Cal L Rev* 1888.
20 Prosser 1960 *Cal LR* 383, 389.
21 Restatement (Second) of Torts s 652B (s 625E (1977)).
22 See also Turkington & Allen *Privacy Law: Cases and Material* 60.
23 Richards & Solove 2010 *Cal L Rev* 1887, 1890.
24 Ibid 1887, 1889.
25 Cohen 2001 *Geo LJ* 2029, 2043.
26 Powell 2011 *Pace Law Review* 161.

revisiting whether or not privacy concerns differ, and whether or not torts law needs to evolve to protect these concerns.

In the following section I briefly explain – using the Restatement (Second) of Torts[27] – how the four privacy torts may be infringed and the possible grounds for justification. The discussion also considers other torts which protect aspects of privacy, namely, breach of confidentiality, intentional infliction of emotional distress, and the right of publicity. The manifestation of these torts in selected states is also considered.

#### *4.3.2.1 Prosser's privacy torts*

(a) Intrusion upon seclusion

The intrusion upon seclusion tort protects a person's right to privacy when another person intentionally intrudes, physically or otherwise, upon the solitude or seclusion of such person's private affairs. When this happens, the wrongdoer is liable for the invasion of the plaintiff's privacy.

This tort requires that the plaintiff must have had a 'privacy interest' which was intruded upon, but does not require that publicity should be given to the person whose privacy has been invaded. It is also required that the wrongful conduct (intrusion) be 'highly offensive to a reasonable person'.[28] The courts have recognised conduct that may be found to be highly offensive,[29] as including: harassing telephone calls;[30] peeping into home windows;[31] snooping into mail;[32] and secretly recording conversations.[33] In terms of this tort, the intrusion itself renders the defendant liable even though there has been no publication or other use of photographs or

---

27 Restatement (Second) of Torts 1977.

28 Ibid 652B; see also Solove & Schwartz *Privacy Law Fundamentals* 18.

29 In this regard, the requirements for the privacy torts of intrusion and public disclosure, differs from the requirements in the South African law of delict. Neethling, Potgieter & Visser *Law of Personality* 221 indicate that in South African law an act of intrusion or disclosure constitutes a wrongful violation of privacy only if the acquaintance with or disclosure of private facts is both contrary to the *subjective* determination and will of the prejudiced party, and, viewed *objectively*, is unreasonable or contrary to the legal views of the community, that is, if it is *contra bonos mores*. It is not required that the intrusion or disclosure must be 'highly offensive'.

30 *Rogers v Loews L'Enfant Plaza Hotel* 526 F Supp 523 (DDC 1981).

31 *Pritchett v Board of Com'rs of Knox Country* 85 NE 32 (ND Ga 1951).

32 *Doe v Kohn Nast & Graf PC* 866 F Supp 190 (ED Pa 1994).

33 *Fischer v Hooper* 732 A2d 396 (1999).

information outlined.[34] It is arguable that in the context of SNSs, the tort of intrusion upon seclusion will not apply, particularly to information that users' have made public on SNSs.[35] Abril[36] notes that this tort would only apply if the information was uncovered in a furtive way from a place with which the plaintiff had a reasonable expectation of privacy. A furtive way in the context of SNSs, would be snooping into someone's Facebook page.

(b) Public disclosure of private facts

This tort creates a cause of action for the public disclosure of a private matter that is highly offensive to a reasonable person, and that is not of legitimate concern to the public. The Restatement provides that it is not an invasion of privacy, in the case of this tort, to communicate a fact concerning the plaintiff's private life to one person or even to a small group of persons.[37] Many states require that the disclosure must be widespread – however, this is not the same in all jurisdictions.

The state of Illinois requires widespread disclosure,[38] as does the state of Kansas. But in *Peterson v Moldofsky*,[39] a federal court in Kansas held that, because of the ease with which pictures can be further disseminated, a woman may institute a private-facts tort claim even though nude pictures of her were distributed by an ex-boyfriend by email to only five other persons. It is argued that such an approach is effective in the digital age, because it acknowledges that publications are more easily spread via the Internet.[40]

The defendant cannot be held liable for giving further publicity to information about the plaintiff that is already public (re-publication) or that is part of a public record, for

34 Restatement (Second) of Torts 652B, comment (b); *Monroe v Darr* 221 Kan 281, 559 P2d 322 (1977), in a case of intrusion upon seclusion, it was held that the general rule is that punitive damages may be recovered for an invasion of the right to privacy where the defendant has acted with malice. The plaintiff bears the burden of proof that the defendant acted with malice.

35 Abril 2007 *Northwestern Journal of Technology and Intellectual Property* 79; Pabarcus 2011 *William Mitchell Law Review* 411-12.

36 Abril 2007 *Northwestern Journal of Technology and Intellectual Property* 79.

37 Restatement (Second) of Torts 652B, comment (a).

38 Solove & Rotenberg *Information Privacy Law* 99; also see *Miller v Motorola Inc* 560 NE 2d 900 (Ill App 1990).

39 2009 WL 3126229 (D Kan Sept 29, 2009).

40 Walters 2015 *Campbell Law Review* 439.

example, disclosing a person's marital status, date of birth, or the fact that the person has filed a lawsuit.[41]

There is also no cause of action if the plaintiff consented to the publication, or if the private facts are of legitimate public concern.[42]

(c) Appropriation of name or likeness

This tort provides a remedy for a plaintiff against someone who appropriates, for his or her own use or benefit, the name or likeness of the plaintiff. The wrongdoer is liable for the invasion of the plaintiff's right to privacy.[43] This tort protects the interests of an individual in the exclusive use of his or her own identity, in so far as it is represented by his or her name or likeness, and in so far as the use may be of benefit to him, her or to others.[44] The appropriation or use is actionable where the plaintiff's name is used for either commercial or non-commercial purposes. In some states, liability has been limited by means of statute to commercial use of a name or likeness.[45]

From the tort of appropriation of name or likeness, the courts have developed another tort – the tort of invasion of the right of publicity – which provides a remedy for famous people, in that it grants them an exclusive right to exploit the value of their identity as celebrities. The right to publicity is discussed below.[46]

In the context of SNSs, a user may appropriate someone else's name or likeness in order to attract a larger user base or 'followers' and in so doing infringe the privacy of the other person.[47]

---

41 Restatement (Second) of Torts 652D comment (a); also see Walters 2015 *Campbell Law Review* 441.

42 Restatement (Second) of Torts 652D comment (a).

43 Ibid 652C.

44 Ibid 652C comment (a).

45 Ibid 652C comment (b).

46 Para 4.3.2.2 (c).

47 *Shepard's Pharmacy Inc v Stop & Shop Companies Inc* 37 Mass App Ct 516, 524; 640 NE 2d 1112, 1117 (Ct App 1994). In this case restitution was denied because the defendant had made no profit from the use of the plaintiff's photograph.

(d) Publicity that places the plaintiff in a false light in the view of the public

The false-light tort provides a remedy when one publicly discloses a matter that places a person in a false light that is highly offensive to a reasonable person, and the actor had knowledge of, or acted in reckless disregard for, the falsity of the publicised matter and the false light in which the other would be placed.[48] In the case of *Time Inc v Hill,*[49] the United States Supreme Court held that the United States Constitution's First Amendment permits liability in false-light cases only if the plaintiff publicly discloses information with a reckless disregard for the truth, or with actual knowledge of falsity. Not all states recognise the false-light tort.[50]

*4.3.2.2 Another tort that protects privacy: Right of publicity*

The right of publicity, as explained above,[51] developed from the tort of 'appropriation of name and likeness'. This tort action protects the financial interests of celebrities against misappropriation of the intellectual property interest celebrities have in their celebrity personae. In *Jim Henson Productions, Inc v John T Brady & Associates, Inc*,[52] the court distinguished between the tort of appropriation of name and likeness and the action for infringement of the right of publicity as follows:

> The privacy-based action is designed for individuals who have not placed themselves in the public eye. It shields such people from the embarrassment of having their faces plastered on billboards and cereal boxes without their permission. The interests protected are dignity and peace of mind, and damages are measured in terms of emotional distress. By contrast, a right of publicity action is designed for individuals who have placed themselves in the public eye. It secures for them the exclusive right to exploit the commercial

48 Restatement (Second) of Torts 652E.

49 385 US 374 (1967); see too Solove & Schwartz *Privacy Law Fundamentals* 21.

50 In *Lake v Wal-Mart* 582 NW 2d 231 (Minn 1998), the Minnesota Court of Appeal affirmed the recognition of the three invasion of privacy torts, but declined to recognise the tort of false-light publicity. Among the reasons given were the fact that this tort is similar to the action for defamation and the fact that there exists a possible tension between the tort of false light publicity and the First Amendment's protection of free speech. Other states that rejected this privacy tort include Massachusetts, Missouri, North Carolina, New York, Virginia, and Texas. See Osorio 2010 *NYU Annual Survey* 173, 174.

51 See para 4.3.2.1(a), also see para 4.3.1.2 for a discussion on the right to identity.

52 687 F Supp 185, 188-9 (SDNY 1994).

> value that attaches to their identities by virtue of their celebrity. The right of publicity protects that value as property, and its infringement is a commercial, rather than a personal tort. Damages stem not from embarrassment but from the unauthorized use of the plaintiff's property.

From the above distinction, it may seem that the right of publicity in the United States is similar to the independent personality right, namely the right to identity, which is recognised in South African law.[53] However, there are differences. The first difference lies in the fact that the right to identity is available to everyone, while the right of publicity is available exclusively to celebrities. A further distinction is that the right of publicity protects a patrimonial interest, whilst the right to identity protects a personality interest.

In the context of SNSs, it is possible to envisage that an ordinary person (user of SNSs) may gain prominence and fame within the SNSs, and therefore become a celebrity. This has been evident, for instance, on YouTube, where ordinary people upload videos which may go viral in a matter of seconds. An ordinary person who becomes a celebrity on SNSs should be able to use the right of publicity action if the users' name or likeness is appropriated for commercial purposes.

### 4.3.3 Federal Constitutional Law

Here I examine the Constitution of the United States and focus specifically on provisions regarding the protection of privacy. These provisions are found in the Bill of Rights, which consists of the first ten amendments to the Constitution. The United States Constitution is the supreme law of the land; the supremacy clause in article 6 of the Constitution provides that:[54]

> This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.

---

53 See para 3.3 above.

54 Constitution of the United States art VI clause 2.

The Bill of Rights is included in the United States Constitution as amendments, and the Constitution comprises 27 amendments to date. The first ten Amendments, forming the Bill of Rights, were ratified by the states in 1791.[55] The Bill of Rights is a declaration of the American people's rights against the federal government.[56] Before the introduction of the Fourteenth Amendment, the Bill of Rights was limited to the federal government. It was the ratification of the Fourteenth Amendment in 1868 that introduced a mechanism which imposed the guarantees of the Bill of Rights at state level; as a result the Bill of Rights is now binding on state governments.[57] The Fourteenth Amendment provides that:

> No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

The right to privacy is recognised and protected under the United States Constitution as a result of judicial interpretation. The decisions in *Griswold v Connecticut*[58] and *Katz v United States*[59] were the first cases to feature the concepts 'right to privacy' and 'expectation of privacy'.[60] In *Griswold v Connecticut*,[61] the majority opinion held that a legal right to privacy could be found in the penumbra (shadows) of the First,[62] Third,[63] Fourth,[64] Fifth, and Ninth Amendments to the Constitution.[65]

Allen[66] notes that although the founders and framers did not include the word 'privacy' in the text of the written Constitution, rich conceptions of privacy are implicit in any plausible renderings of the text. The First, Third, Fourth, Fifth, and Fourteenth Amendments all possess elements that protect the right to privacy. The First Amendment deals with the protection of freedom of speech, but in some instances it

55 Constitution of the United States Preamble to the Bill of Rights.
56 Kanovitz *Constitutional Law* 24.
57 Ibid.
58 381 US 479 (1965).
59 389 US 347, 359 (1967).
60 Also see Allen 2012 *Journal of Constitutional Law* 890.
61 381 US 479, 484 (1965).
62 Constitution of the United States, Amendment I.
63 Ibid Amendment III.
64 Ibid Amendment IV.
65 Ibid Amendment XIV.
66 Allen 2012 *Journal of Constitutional Law* 887.

may be interpreted also to protect privacy, for example, by protecting the right to speak anonymously.[67] The Third Amendment deals with protection of the home from the quartering of troops without the consent of the owner. The Fourth Amendment protects against unreasonable searches and seizures, while the Fifth Amendment provides a privilege against self-incrimination. This Amendment protects privacy by restricting the ability of the government to force individuals to divulge certain information about themselves that would lead to their prosecution in a criminal proceeding.[68] The Fourteenth Amendment's due-process clause has been interpreted by the courts to protect privacy by protecting the freedom of individuals to make certain choices in regard to procreation, motherhood, and child rearing.[69] In this sense, the right to personal autonomy is also seen as part of the right to privacy.

For the purposes of this study, only the First and the Fourth Amendments' protection of privacy will be discussed as the protection of the privacy of published personal information (as would be the case on a SNS) seems to fall under these two Amendments.

#### *4.3.3.1 First Amendment*

The First Amendment provides that:[70]

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably assemble, and to petition the Government for a redress of grievances.

The First Amendment protects, amongst other rights, the right to freedom of speech, freedom of the press, the right to speak anonymously, and freedom of association. This provision has a strong implicit constitutional value that protects privacy since the freedom of association clause is interpreted to protect individuals from being compelled to disclose the groups to which they belong or contribute.[71]

---

67 Solove & Rotenberg *Information Privacy Law* 20.
68 Ibid 21; also see Allen 2012 *Journal of Constitutional Law* 888.
69 See *Griswold v Connecticut* 381 US 479 (1965) and *Roe v Wade* 410 US 113 (1973).
70 Constitution of the United States, First Amendment.
71 Solove & Rotenberg *Information Privacy Law* 20.

The First Amendment curtails the government's power to dictate what is written, spoken, or read.[72] This Amendment restricts liability for causes of action relating to the disclosure of both true and false information.[73] The rights protected under this Amendment are not absolute, which means that certain categories of speech are not protected by the First Amendment.[74] For instance, the disclosure of false information regarding another person, may lead to the person disclosing this information being held liable in terms of the tort of defamation (libel or slander). Other categories which may be excluded from the First Amendment include: obscenity;[75] fighting words;[76] threats;[77] incitement of immediate unlawful action; and child pornography.[78] In the context of SNSs, for instance, the right to speak anonymously may be prone to lead to abuse of other users' personality rights. Therefore a balance should be struck between one's interest in anonymity and the interests of others' personality rights.[79]

#### *4.3.3.2 Fourth Amendment*

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment has been interpreted by the courts to apply where a person exhibits a reasonable expectation of privacy. It aims to protect citizens from the government. Thus, whenever a government official conducts a search and seizure, the Fourth Amendment is activated.[80] Initially, the Supreme Court interpreted this

---

72 Kanovitz *Constitutional Law* 45.
73 Solove, Rotenberg & Schwartz *Privacy, Information, and Technology* 25.
74 Kanovitz *Constitutional Law* 51. Also see Burns *Communications Law* 28. She notes that the privilege granted by the right to freedom of speech is limited by, for example, the law of copyright, law of delict, libel laws, laws which protect national security, and so on.
75 *Miller v California* 413 US 15 (1973).
76 *Chaplinsky v New Hampshire* 315 US 568 (1942).
77 *Watts v United States* 394 US 705, 89 S Ct 1399, 22 L Ed 2d 664 (1969).
78 *New York v Ferber* 458 US 747 (1982).
79 Solove, Rotenberg & Schwartz *Privacy, Information, and Technology* 428.
80 Ibid 61.

amendment narrowly, protecting only against the physical intrusion upon private property by a law enforcement officer. In the case of *Olmstead v United States*,[81] the Supreme Court decided that wiretapping does not violate the Fourth Amendment, as no search and seizure of anything tangible, or any physical trespass had occurred. The majority of the Supreme Court concurred that police wiretapping did not constitute an illegal search under the Fourth Amendment. This was the position until 1967. Justice Brandeis wrote a dissenting judgment, contending that the central interest protected by the Fourth Amendment was not property, but the 'right to be let alone'.

The position changed in *Katz v United States*.[82] Prior to the *Katz* decision, there was legal uncertainty as to whether or not the Fourth Amendment covered government-initiated electronic surveillance or intangible interests. It is inevitable that these electronic devices improved the law enforcement's investigative techniques. In the *Katz* case, police 'believed' that a listening device placed in a telephone booth was not prohibited wiretapping, since it did not penetrate the wall of a phone booth, and was therefore a justified intrusion. The court held that the Fourth Amendment 'protects people, not places' and that police must obtain a warrant when a search takes place in a public pay phone on a public street. In order to determine whether or not a right to privacy in terms of the Fourth Amendment exists, the court developed a 'reasonableness standard'. The reasonableness standard involves the following inquiry: whether a person has exhibited an actual (subjective) expectation of privacy; and whether the expectation is one that society is prepared to recognise as reasonable. In a case where a search is conducted with a warrant supported by probable cause, the search is reasonable, with a few exceptions.

The advent of new technologies has an impact on the application and development of the reasonable expectation of privacy test. In *Kyllo v United States*,[83] two Federal Bureau of Investigation (FBI) agents used a thermal imaging device to scan parts of petitioner, Kyllo's, triplex on suspicion that he was illegally growing marijuana inside his house. The scan was performed from the passenger seat of Agent Elliott's vehicle across the road from the front of the house and also from the street at the

81 1928 227 US 438.

82 1967 389 US 347.

83 533 US 27, 29 (2001); see also Candy 2012 *Drake Law Review* 237.

back of the house. With the information that was gathered, the government discovered that the defendant was indeed growing marijuana illegally inside his home. A Federal Magistrate Judge issued a warrant authorising a search of the petitioner's home. In this case, the Supreme Court held that the government's use of sense-enhancing technology not in 'general public use' without a search warrant violated the Fourth Amendment. The Supreme Court emphasised the requirements of a warrant and probable cause. This case is another illustration how the advance in technology affects the degree of privacy of the citizens protected in the Fourth Amendment.

In the following section I look at some of the legislation protecting privacy at the federal level.

### 4.3.4 Legislation

*4.3.4.1 Introduction*

In the first part of this section I look at some of the relevant legislation protecting privacy at the federal level. In the United States, there are many pieces of legislation which regulate and protect privacy interests. These pieces of legislation cover different areas, such as law enforcement and government records,[84] data security,[85] consumer data,[86] medical and genetic data,[87] and employment.[88] Congress often enacts legislation to address an imminent threat to privacy. These pieces of legislation are applied and interpreted together with the United States Constitution and common law. This section will first of all discuss the laws most relevant in the area of SNSs.

---

84 Fair Credit Reporting Act of 1970; Bank Secrecy Act of 1970; Cable Communications Policy Act of 1984; Foreign Intelligence Surveillance Act of 1978; Electronic Communications Privacy Act of 1986; Communications Assistance for Law Enforcement Act of 1994; Identity Theft and Assumption Deterrence Act of 1998; Children's Online Privacy Protection Act of 1998; Gramm-Leach-Bliley Act of 1999; USA-PATRIOT Act of 2000; CAN-SPAM Act of 2001; and Video Voyeurism Prevention Act of 2004.

85 Privacy Act of 1974; Family Educational Rights and Privacy Act of 1974; Rights to Financial Privacy Act of 1978; Privacy Protection Act of 1980; Computer Matching and Privacy Protection Act of 1988; and Video Privacy Protection Act of 1988.

86 Telephone Consumer Protection Act of 1991.

87 Health Insurance Portability and Accountability Act of 1996;

88 Employee Polygraph Protection Act of 1988; Driver's Privacy Protection Act of 1994; and Personal Responsibility and Work Opportunity Reconciliation Act of 1996.

International instruments such as the Organisation of Economic Cooperation and Development (OECD) Guidelines of 1980, and the EU Data Protection Directive of 1995, also influence the privacy laws in the United States. The OECD Guidelines and the EU Directive are discussed in Chapter 5. The 'Privacy Shield' agreement reached between the United States and the EU to ensure compliance with the EU Directive is therefore discussed.

In the last part of this section I consider the application of some of the laws discussed in the context of SNSs.

*4.3.4.2 Electronic Communications Privacy Act of 1986 (ECPA)*

The ECPA was passed by the United States Congress in 1986. The Congress noted the growth in wiretapping carried out in the absence of a legal sanction, and without the consent of any of the parties to the conversation.[89] Furthermore, the evidence derived in this way was being used by public and private parties in court and administrative proceedings. This created a *lacuna* in the effective protection of the privacy of wire,[90] oral,[91] and electronic communications.[92] Congress found it necessary to define a uniform basis for the circumstances and conditions under which the interception of wire or oral communications may be authorised, to prohibit any unauthorised interception and use of the contents of such communications, as evidence in courts and administrative proceedings.[93]

The ECPA is a federal law which governs wiretapping and electronic eavesdropping. The ECPA was enacted in an attempt to keep pace with the prevalence of electronic

89 Rotenberg *Privacy Law Sourcebook* 103.

90 18 USC s 2510(1) interprets 'wire communication' to mean "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce".

91 18 USC s 2510(2) interprets 'oral communication' to mean "any oral communication uttered by a person exhibiting an expectation that such communications is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication".

92 18 USC s 2510(12) interprets 'electronic communication' to mean "any transfer of signs, signals, writings, images, sounds, data, or intelligence or any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include any wire or oral communication".

93 18 USC s 2515.

communications. The ECPA regulates wire,[94] oral,[95] and electronic communications.[96] The ECPA divided electronic surveillance into three sections or titles: the Wiretap Act;[97] the Stored Communications Act;[98] and the Pen Register Act.[99] All these Acts are briefly discussed below. However, it is notable that only the Stored Communications Act has a direct bearing on SNSs within private law. On the other hand, the Wiretap Act and the Pen Register Act focus more on effective law enforcement and foreign intelligence gathering, in conjunction with other relevant legislation.[100]

In the following paragraphs I look at the scope of application of the three Acts.

(a) Wiretap Act (Title I) of Electronic Communications Privacy Act of 1986

In terms of the Wiretap Act,[101] it is a federal crime to engage in wiretapping or electronic eavesdropping, to possess wiretapping or electronic eavesdropping equipment, to use or disclose information obtained through illegal wiretapping or electronic eavesdropping, or to disclose information secured through court-ordered wiretapping or electronic eavesdropping.[102] This applies to any employee or agent of the United States or any state or political subdivision thereof, as well as any individual, partnership, association, joint stock company, trust, or corporation.[103]

The Wiretap Act applies to the intentional interception of communications simultaneously with their transmission – in other words, while the communication is being transmitted.[104] The Act defines 'interception' as the aural or other acquisition of

94 Ibid s 2510 (1).
95 Ibid s 2510 (2).
96 Ibid s 2510 (3).
97 Wiretap Act 18 USC ss 2510-2522 (2006).
98 Stored Communications Act 18 USC ss 2701-2712 (2006).
99 18 USC ss 3121-3127 (2007).
100 USA PATRIOT Act of 2001; Intelligence Authorization Act for Fiscal Year 2001; 21st century Department of Justice Appropriations Authorization Act of 2002; Department of Homeland Security Act of 2002; USA PATRIOT Improvement and Reauthorization Act of 2006; and Foreign Intelligence Surveillance Act 1978 Amendments Act of 2008.
101 The Wiretap Act is also referred to as the revised Title III (Title III of the Omnibus Crime Control and Safe Street Act).
102 18 US s 2511. Also see Doyle *Overview of the ECPA* 7 available at https://www.hsdl.org/?view&did=725508 (date of use: 20 December 2016).
103 18 USC s 2510 (6).
104 *Noel v Hall* 568 F 3d 743, 749 (9th Cir 2009). The court held that replaying of tapes containing a recorded phone conversation does not amount to a new interception in violation of the

the contents of various kinds of communication by means of electronic, mechanical or other devices.[105] In order for a government official lawfully to intercept the contents of a communication using an electronic, mechanical, or any other device, the official is required to obtain a court order. Section 2518 requires that an application for a court order to intercept must contain details that justify the interception, information regarding how the interception will be conducted, and information on the duration of the interception.[106] There are recognised exceptions which exclude the application of the Wiretap Act. First of all, if one of the parties to the communication consents to the interception the Wiretap Act will not apply.[107] There is also an exception which permits the service provider, "whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service….".[108]

In cases where the provisions of the Wiretap Act have been violated, there are two possible remedies available to the plaintiff. Firstly, the aggrieved party may move to supress the contents of any wire or oral communication intercepted or evidence obtained (in terms of the exclusionary rule of the rules of evidence).[109] Secondly, the responsible party could be held liable for damages of a minimum of $1 000 per violation or up to five years' imprisonment.

---

Wiretap Act. See also *United States v Szymuszkiewicz* 622 F 3d 701, 705-06 (7th Cir 2010). The court held that an employee surreptitiously programming his supervisor's computer so that the server forwards duplicates to the employee of all e-mails sent to the supervisor, constitutes an interception in violation of Title III.

105 18 USC s 2510 (4).

106 Ibid s 2518.

107 Ibid s 2511 (2)(c). In other words, one of the parties to the communication may secretly record his or her own phone conversation; it is not illegal under federal wiretap law.

108 18 USC s 2511 (2)(a)(i). In terms of s 2511, a service provider may intentionally disclose intercepted communications to the proper authorities when criminal activity is afoot; with the consent of the originator, addressee, or intended recipient; or to any intermediary provider.

109 18 USC s 2518 (10)(a).

(b) The Stored Communications Act (Title II) of Electronic Communications Privacy Act of 1986

The Stored Communications Act (SCA Act)[110] applies to stored communications or records held by ISPs. The SCA Act makes it a federal crime intentionally to access, without authorisation, a facility through which an electronic communication service is provided, thereby obtaining, altering, or preventing access to a wire or electronic communication while it is in 'electronic storage' in such a system.[111] 'Electronic storage' is defined as encompassing temporary, intermediate storage incidental to transmission, as well as backup storage.[112] Before a government official may gain access to these communications, section 2703 requires him or her to obtain a court order, subpoena, or warrant.

In a case where there has been an infringement of the SCA Act, there is a remedy available to the plaintiff. If found guilty, the responsible party will be held liable for damages, with a minimum of $1 000 per violation or up to one year's imprisonment, if the violation was for commercial gain.

The case of *Juror Number One v The Supreme Court of Sacramento*[113] was a petitioned appeal to the Court of Appeal in California. The applicant in the matter was 'juror number one' (fictitiously named) in the assault case of *People v Christian*.[114] The respondent learned that the applicant had, in violation of an admonition by the court (juror misconduct), posted something about the case on his Facebook account while the case was still before the court. The trial court then entered an order in accordance with the SCA Act, requiring the juror to sign a consent form authorising Facebook to release, for in-camera review, all the items posted during the trial. The juror filed a petition for a writ of prohibition. The applicant's petition was an attempt to stop the respondent from enforcing its order. This was based on the ground that such an order, if enforced, would violate the

110 Ibid ss 2701-2711.
111 Ibid s 2701 (a).
112 Ibid s 2711 (1).
113 206 Cal App 4th 854; 2012 Cal 142 Cal Rptr 3d 151.
114 Sacramento County Superior Court case number 08F09791.

provisions of the SCA Act, as well as the Fourth and Fifth Amendments in terms of the Federal Constitution.[115]

The court drew a distinction between posting for public viewing and posting to a closed group of friends. The former refers to a situation where a user posts information on the 'Timeline' (previously referred to as the 'Wall')[116] on Facebook or a profile page on MySpace, which is similar to the 'Timeline' feature on Facebook. The court held that a party does not forfeit his SCA Act protection by making his communications available to a closed group. It also held that the SCA Act protection applies only to an attempt, either by the court or by relevant parties, to compel Facebook, as the service provider, to disclose the requested information. In this case, the attempt was directed at juror number 1 and not at Facebook. Mauro J concurred in this view. The court held that the applicant had failed to demonstrate any expectation of privacy with regard to his Facebook posts, and that such posts constituted misconduct on the part of the applicant.[117]

The petition for writ of prohibition was therefore denied. The Court of Appeal held that the juror's right to privacy with regard to his Facebook posts is not absolute, and that a balance had to be struck between the interests of the parties involved in the trial, and their interests in a fair trial.

(c) Pen Register Act (Title III) of Electronic Communications Privacy Act of 1986

The Pen Register Act applies to pen registers or trap-and-trace devices.[118] The government must obtain a court order to install pen register and trap-and-trace

115 206 Cal App 4th 854; 2012 Cal 142 Cal Rptr 3d 151 para [9].

116 See Chapter 3 above.

117 See also *Moreno v Hanford Sentinel Inc* 91 Cal Rptr (Cal Ct App 2009).The court held that postings on publically accessible MySpace pages were not private, and as such, the plaintiff could not have a reasonable expectation of privacy in terms of the information published to her profile.

118 18 USC s 3127(3), defines a 'pen register' as a "device or process" that records outgoing "dialing, routing, addressing or signalling information," but "such information shall not include the contents of any communication"; 18 USC s 3127(4) defines a 'trap and trace device' as a "device or process" that captures incoming "dialing, routing, addressing and signaling information" but "such information shall not include the contents of any communication".

devices. Pen registers are useful for a number of reasons, including the following: to aid in identifying a person making annoying or obscene calls; to keep records of monthly bills for calls; to check overbilling; and many more. The court must grant the order sought if the government has shown that the information likely to be obtained by the installation and use is relevant to a criminal investigation. The Pen Register Act is not applicable in the context of SNSs and will therefore not be discussed in any detail.

#### *4.3.4.3 Safe Harbour privacy principles and the 'Privacy Shield'*

(a) Background

From time to time the United States promulgates information privacy laws which are intended to protect the privacy of personal information while at the same time allowing for the free flow of information. As noted above, the approach towards the protection of privacy in the United States is piecemeal and based on self-regulation. The same trend is found in the field of data privacy. Roos notes that: "American-policy makers prefer to deal with data-privacy issues as and when such issues become a problem; a specific event usually 'triggers' the legislative process".[119] The Working Party set up in terms of article 29 of the 1995 European Union Directive on Data Protection, viewed the United States' information privacy laws as not meeting the adequacy standard as set in article 25 of the Directive.[120] Only if a country provides an adequate level of protection to personal data, will a European Union data controller be allowed to transfer personal data from the European Union country to the other country. This finding could potentially have meant that the flow of personal information between the European Union and the United States would come to a standstill.

---

Section 216 of the USA PATRIOT Act of 2000 has amended these definitions to read "a device or process which records or decodes dialling, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication attached."

119 Roos "Data protection law" 349. The EU Directive on Data Protection is discussed in Ch 5; Roos 2007 *SALJ* 414.

120 Directive 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. This Directive is discussed in the next chapter.

Therefore, in 1998 the United States began to negotiate with the European Union for a 'European Union-United States Safe Harbor Agreement' (Safe Harbour Agreement).[121] The negotiations were aimed at ensuring continued trans-border flows of personal data and compliance with the requirements of article 25 of the EU Directive on Data Protection. After two years of negotiations, the United States Department of Commerce and the Internal Market Directorate of the European Commission reached an agreement in 2000. The Safe Harbour Agreement has seven privacy principles: notice; choice; onward transfer; security; data integrity; access; and enforcement,

In terms of the agreement, United States' companies voluntarily agreed to adhere to these privacy principles. Once they had signed up to the agreement, they had to ensure compliance with the EU Directive, as non-compliance could lead to prosecution by the Federal Trade Commission (FTC). After self-certifying their compliance with the agreement, these companies were presumed to provide adequate protection to the privacy of personal information and could continue to receive personal data from the European Union.

(b) Critique of the Safe Harbour Agreement

From the outset, the Safe Harbour Agreement met with criticism. The European Commission noted in its 2013 report[122] that the Safe Harbour Agreement was based on voluntary self-certification by the companies. As a result, any lack of transparency from the participants and shortcomings in enforcement, undermined the foundations on which the Safe Harbour scheme was construed.[123] Other concerns stemmed from whether all self-certified companies complied with the transparency requirements. The reports also noted that some companies still fell short of fully incorporating all Safe Harbour privacy principles. It also noted that some privacy principles of self-certified companies were often unclear as regards the purposes for which data had

121 Roos "Data Protection Law" 350.

122 European Commission Functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU (2013) 4.

123 Ibid 5.

been collected and the right to choose whether or not data could be disclosed to third parties. This raised issues of compliance with the privacy principles of 'notice' and 'choice'.

(c) *Schrems v Data Protection Commissioner*

On 6 October 2015, the Court of Justice of the European Union (CJEU) in *Schrems v Data Protection Commissioner,*[124] invalidated decision 2000/520 of the European Commission which approved the Safe Harbour scheme as providing for an adequate level of protection for personal data when assessed against the standard set by EU data protection law.

The background to this case is that in 2013 Schrems, an Austrian citizen, lodged a complaint with the Irish Data Protection Commissioner, asking, in essence, the Commissioner to exercise its statutory powers to prohibit Facebook Ireland from transferring his personal data to the United States. Facebook stores the information of its European users on servers located in Ireland before transferring it to the United States. Schrems contended in his complaint that the law and practice in force in the United States did not ensure adequate protection for the personal data held in its territory against the surveillance activities engaged in in the United States by public authorities.[125] The Irish High Court rejected the complaint as under the 2000 decision of the European Commission, the Safe Harbour Agreement was held to provide adequate protection.

The issue was referred to the CJEU which declared the Safe Harbour decision invalid. It was, inter alia, pointed out that once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of the indiscriminate surveillance and interception carried out by them on a large scale.[126]

After the ruling of the CJEU, the Article 29 Working Party made an urgent call on the member states and the European institutions to open discussions with United States'

124 EUCJ Case C-362/13 6 October 2015.
125 Para 25.
126 Para 31.

authorities in order to find political, legal, and technical solutions which would enable data transfers that respect fundamental rights to the territory of the United States.[127]

On 2 February 2016 the European Commission and the United States agreed on a new framework for transatlantic data flows: the EU-US Privacy Shield. The European Commission announced that the new arrangement will include the following three elements.[128]

1. *Strong obligations on companies handling Europeans' personal data and robust enforcement***.** United States' companies wishing to import personal data from Europe will need to commit to robust obligations on how that personal data is processed and individual rights guaranteed. The Department of Commerce will monitor that companies publish their commitments, which makes them enforceable under United States law by the United States Federal Trade Commission. In addition, any company handling human resources data from Europe will have to commit to complying with decisions by European DPAs.

2. *Clear safeguards and transparency obligations on United States' government access to personal data*. For the first time, the United States has given the European Union written assurances that the access of public authorities for law enforcement and national security, will be subject to clear limitations, safeguards, and oversight mechanisms. The United States has ruled out indiscriminate mass surveillance of personal data transferred to the United States under the new arrangement. There will be an annual joint review to monitor the functioning of the arrangement on a regular basis, which will include the issue of national security access. The European Commission and the United States Department of Commerce will conduct the review and invite national intelligence experts from the United States and European Data Protection Authorities to attend.

127 EU art 29 DP WP *Statement of the Working Party* (Brussels) 16 October 2015.

128 "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield" (Strasbourg 2 February 2016). Press release available at http://europa.eu/rapid/press-release_IP-16-216_en.htm (date of use: 13 October 2016).

3. *Effective protection of European Union citizens' rights with several redress possibilities*. Any citizen, who considers that his or her data has been misused under the new arrangement, will have several avenues of redress. Companies have deadlines within which to reply to complaints. European DPAs can refer complaints to the Department of Commerce and the Federal Trade Commission. In addition, alternative dispute resolution will be provided free of charge. For complaints on possible access by national intelligence authorities, a new Ombudsperson will be created.

This new framework will protect the fundamental rights of Europeans where their data is transferred to the United States and ensure legal certainty for businesses.

## 4.4 PRACTICAL APPLICATION TO SNSs

The Internet is arguably a public space by default. This has often raised the question of whether an Internet user retains or has a reasonable expectation of privacy while he or she is online. Ganguly[129] holds that the advent of the Internet makes traditional privacy protection more important than ever, as privacy becomes easier to violate. It is trite that the 'reasonable expectation of privacy' is the test or standard for determining whether or not a person has a right to privacy that should to be protected by law.

With regard to the reasonable expectation of privacy requirement, Grant[130] is of the view that in both society and the online world, there are situations which are not covered by the reasonable expectation of privacy. However, the *Katz* decision is an example which shows that even in a public place, there are some matters that remain private and thus warrant protection. Hogde[131] holds that on SNSs, users' messages (or posts) may be received by a large number of recipients, and that this has the potential to diminish the expectation of privacy. In *United States v*

129 Ganguly 2008-2009 *Wis Int LJ* 1151.
130 Street & Grant *Law of the Internet* 135.
131 Hodge 2006 *South Illin Univ LJ* 105.

*Rodriguez,*[132] it was held that although individuals generally have a reasonable expectation of privacy on their home computers, for Fourth Amendment purposes they do not enjoy such an expectation of privacy in the case of transmissions over the Internet, or e-mails which have already reached the recipient. In contrast, Newell[133] is of the view "that the subjective expectation of privacy in information posted to limited-access social media websites also described as the notion of 'network privacy' is an expectation that society recognises as reasonable in the twenty-first century". Therefore, it may be concluded that a user does retain a reasonable expectation of privacy where the communications are to a closed group and where adequate privacy settings have been put in place.[134]

## 4.5 PROCEDURAL CHALLENGES

An ISP often gives users access to SNSs or networks without requiring any form of positive identification or verification of the users' true identity. Here I address whether an Internet Service Provider (ISP) can be held liable for content posted by a user whose identity is unknown to the plaintiff, either because the defendant is anonymous or is using a pseudonym. I also discuss whether or not the ISP would be liable if the wrongdoer could not be located. Lastly, I discuss whether, in the case of an anonymous user, an ISP may be compelled to reveal the user's identity.

### 4.5.1 Liability of an Internet Service Provider for third-party content

The Communications Decency Act[135] (CDA) provides immunity to website operators and other 'interactive computer services'[136] for liability regarding content posted by third parties which may potentially be tortious (wrongful) in nature, even when the

132 532 F Supp 2d 332 (DPR 2007).

133 Newell 2010-2011 *Rich JL & Tech* 7.

134 Also see para 3.6 above.

135 Communications Decency Act of 1996 s 230.

136 Ibid. 'Interactive computer service' means "any information service, system or access software provider that provides or enables computer access by multiple users to a computer server, including a service or system that provides access to the Internet, and such systems operated or services offered by libraries or educational institutions".

website operator or interactive computer service has become aware of the tortious nature of the content. Section 230 provides:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

The immunity applies to either a provider or a user (defendant) of an interactive computer service; where the cause of action treats the defendant as the publisher or speaker of the alleged tortious or unlawful content; and where the content is provided by another 'information content provider'.[137] This means that online intermediaries that host or re-publish speech, are protected against liability for information posted by third parties. In the context of SNSs, the ISP generally does not provide content; most of the content is generated by users. Therefore this immunity will apply in the context of SNSs.

The case of *Zeran v America Online Inc*[138] is the leading case dealing with section 230. In this case an unknown user advertised T-shirts on a message board operated by America Online (AOL). The T-shirts contained offensive slogans relating to the bombing of Oklahoma City's federal building. The unknown user gave Zeran's name and address as the contact information (this was Zeran's business number) for the advertisement. Those who had an interest in purchasing a T-shirt had therefore to contact Zeran. As a result, he received a high volume of angry and derogatory calls, including death threats. Zeran notified AOL of his predicament and AOL then removed the post and terminated the account of the unknown user. The unknown user then created another post, again using Zeran's contact details. Zeran sued AOL for failing to remove the advertisement more speedily, alleging that AOL had been negligent. AOL advanced section 230 of the CDA as a defence. The district court for the Western District of Oklahoma granted judgment in favour of AOL and Zeran appealed the decision. The decision was later affirmed by the Fourth Circuit court, which stated that:

> By its plain language, section 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, section 230 precludes courts from entertaining claims

---

137 Ibid. 'Information content provider' means "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service".

138 129 F 3d 327 (4th Cir 1997).

> that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions - such as deciding whether to publish, withdraw, postpone or alter content - are barred.[139]

The immunity provided under section 230 of the CDA has not escaped criticism. Solove[140] is of the view that "the law is hampered because it overprotects free speech. In particular, the Communications Decency Act section 230 promotes a culture of irresponsibility when it comes to speech online". Furthermore, the author states that he would

> recommend that section 230 be modified to have a notice-and-takedown system rather than complete unmitigated immunity, Whenever bloggers or website operators know that a comment posted by another is tortious, the law should create an incentive for them to remove it. If a person promptly removes a tortious comment after being notified, then that person would be immune. If the person fails to remove the comment, only then would the person be subjected to potential liability.

The immunity provided under section 230 of the CDA is similar to that provided by South Africa[141] and the United Kingdom.[142]

### 4.5.2 Anonymous users

In the United States, the use of a pseudonym or the decision to remain anonymous in online communication is considered to be a democratic right protected under the First Amendment.[143] It is clear that anonymity may be used to protect a user's right to freedom of speech, and Barendt[144] notes that the freedom to choose anonymity is one aspect that guarantees the right to privacy. However, neither free speech nor privacy is an absolute right, which means that when these rights are invoked, a balance should always be struck with the rights of others. In a case where a personality right has been infringed, the plaintiff will seek to determine the identity of the anonymous user, in order to succeed in the redress sought.

---

139 129 F 3d 327 (4th Cir 1997) 330.

140 Solove in Levmore & Nussbaum *The Offensive Internet* 25.

141 See para 3.9.3 above.

142 See para 5.4.3.2 below.

143 Sobel 2000 *VA JL & Tech* para [3] available at www.vjolt.net (date of use: 1 September 2014); Moore *Privacy Rights* 103, notes that the ability to speak freely sometimes relies heavily upon anonymity.

144 Barendt "Privacy and Freedom of Speech" 15.

In the case of a law enforcement officer or government entity who seeks to pierce the veil of online anonymity, the position is governed by the ECPA, which requires the law enforcement officer to obtain a warrant according to the procedural requirements stipulated in the ECPA.[145] Section 2703(c)(1)(A) of the ECPA provides that:[146]

> A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity, obtains a warrant issued using the procedure described in the Federal Rules of Criminal Procedure (or in case of a State court, issued using State warrant procedures) by a court of competent jurisdiction.

In a civil suit, once the plaintiff has filed a complaint suing a fictitious 'John Doe', the next step would be to serve a subpoena on the ISP, with the permission of the court, which seeks to determine the identity of the anonymous poster.[147] It is then the duty of the ISP to notify its user of the pending subpoena, which will provide him or her with an opportunity to oppose the subpoena. Whether or not an ISP notifies its user when there is a pending subpoena is determined by the ISP's privacy policy.[148] According to Larson and Godfread,[149] "the Federal Rules of Civil Procedure are largely silent or unclear on the matter of anonymous defendants, leaving various jurisdictions to develop different methods of dealing with anonymous parties".

Thus, in the United States, the civil process of unmasking an anonymous user may have a negative effect in two respects before the defendant is afforded an opportunity to oppose the unmasking. Firstly, it may infringe upon the defendant's freedom of speech, and secondly, it may infringe upon the defendant's right to privacy.[150]

In *Columbia Insurance Co v Seescandy.com*,[151] the court required the plaintiff to identify the relevant party with sufficient specificity to enable the court to determine if

---

145 18 USC s 2518 (Wiretap Act); s 2703(a) (Stored Communications Act); and s 3123(a) (Pen Register Act).

146 18 USC s 2703 (c)(1)(A).

147 Sobel 2000 *VA JL & Tech* para [14]; see also Larson & Godfread 2011 *William Mitchell LR* 339.

148 Ibid.

149 Larson & Godfread 2011 *William Mitchell LR* 337.

150 Ibid 339.

151 *Columbia Insurance Co v Seescandy.com* 185 FRD 573 (ND Cal 1999).

the defendant was a real person or entity who could be sued in federal court. In order to lift the veil of anonymity, the plaintiff must approach the court to subpoena the ISP, in order to compel the ISP to reveal the identity of the anonymous user. The plaintiff should also show the court all the steps taken to locate the anonymous defendant.[152]

In *In re Subpoena Duces Tecum to America Online, Inc,*[153] the court identified three criteria which will convince the court to order a non-party (ISP) to provide information concerning the identity of a subscriber. These requirements are: the court must be satisfied by the pleadings or evidence supplied to it; the party requesting the subpoena must have a legitimate, good faith basis to contend that it may be a victim of conduct actionable in the jurisdiction where the suit is filed; and the subpoenaed identity information is central to advance that claim.

Larson and Godfread[154] note that most ISPs or website operators have little incentive to either comply with a request to identify an anonymous speaker, or to use their resources to protect anonymous speakers. They cite the immunity granted by section 230 of the CDA as one of the reasons for this as ISPs or website operators run little risk of liability for tortious claims that arise as a result of content created by anonymous third parties.[155]

In the United States, when an infringement of a personality right such as the right to privacy has occurred (under either the Constitutional or tort law) in the context of SNSs, it is clear that an SNS may not be held liable for the content published by third parties, whether anonymous or not. The duty to find an anonymous defendant ultimately falls to the plaintiff. It therefore appears that without successfully identifying the anonymous user, the plaintiff has no legal recourse.

## 4.6 CONCLUSION

152 Ibid.

153 *In re Subpoena Duces Tecum to American Online Inc* 52 Va Cir 26 (2000) and *Columbia Insurance Co v Seescandy.com* 185 FRD 573 (ND Cal 1999) adopted the same approach.

154 Larson & Godfread 2011 *William Mitchell LR* 348.

155 Ibid.

In this chapter I have considered the recognition, protection and regulation of the right to privacy and the right to identity in the United States. I examined various sources in this regard, namely constitutional law (at both federal and state level), legislation, common law, and case law. From my discussion, it is clear that the United States Federal Constitution does not explicitly protect the rights to privacy and identity. However, United States' case law has helped develop the right to privacy through judicial interpretation. For instance, although the United States Constitution does not provide for dignity, the courts have interpreted the Constitution to include dignity.[156]

The implied protection of the rights to privacy and identity in the United States Constitution applies only within a vertical relationship – the relationship between the state and its citizens. Consequently, in the context of SNSs, the constitutional provisions implicitly dealing with privacy may not apply between users as this falls outside of the vertical application of the Constitution. At federal level it is challenging to draw a clear distinction between public and private law protection of privacy. The common law also offers protection to both the vertical and horizontal relationship. In the context of SNSs, particularly when there are two private parties, the common law has a role to play, especially in the absence of legislation.

Furthermore, the United States often enacts piecemeal legislation whenever an interest is under threat. The enacted legislation may be less or more stringent than the provisions of the United States' Constitution. South African law may draw some lesson from the United States' legal position specifically on how it deals with anonymous defendants in the context of SNSs.[157]

156 *Schmerber v California* 384 US 757, 767 (1966).
157 Para 4.5.2 above; also see para 3.9.2 above.

# Chapter 5

# International documents and the European Union

## 5.1 INTRODUCTION

In this chapter I discuss some of the important documents relating to the protection of the right to privacy and the right to identity (as a part of the right to dignity[1]) in the context of SNSs issued by international organisations and the European Union (EU). The chapter is divided into three parts. The first part deals with documents issued by international organisations which contribute to the development and protection of the right to privacy and data protection. The second focuses on the EU legal instruments in this area. Lastly, I explore the legal position in the United Kingdom (UK) as an example of the application of EU law in a specific EU member state.[2]

Some of these documents are human rights documents which consider the right to privacy and the right to dignity (encompassing the right to identity) as fundamental human rights. However, the majority of the legal instruments I discuss are data protection legal instruments. As said, data protection laws become relevant whenever personal information is processed,[3] and so, in essence, protect a person's right to privacy and right to identity.[4]

1 As said, the right to identity is usually protected under the guise of privacy or dignity; also see para 3.3.1 above.

2 Britain is leaving the European Union sometime in the future. On 23 June 2016 UK held an EU Referendum where the people of the UK were required to vote on whether to stay within or exit the EU. They voted to leave – see para 5.4 below.

3 Para 1.1 above.

4 Neethling et al *Neethling's Law of Personality* 270-1.

## 5.2 INTERNATIONAL DOCUMENTS

The Internet and SNSs operate on an international platform which allows the trans-border communication and processing of personal information. This may lead to the infringement of one's rights to privacy or identity in a country other than one's own. Although this study does not cover the issue of international jurisdiction, it is necessary to highlight a few of the notable international documents that have influenced national laws in different jurisdictions, including South Africa. Some of these international documents were discussed and incorporated in the South African Law Reform Commission's (SALRC) discussion paper on privacy and data protection.[5]

I refer to international documents issued by the United Nations (UN), the Organisation for Economic Cooperation and Development (OECD), the Council of Europe, the African Union (AU), and the EU. Other organisations have also issued privacy and data protection documents – for example, the Asia-Pacific Economic Cooperation (APEC) and the Association of Southeast Asian Nations (ASEAN), but as the influence of these documents on South African law is minimal, I do not consider them further.

### 5.2.1 United Nations

#### *5.2.1.1 Introduction*

The UN is an international organisation that was established in 1945 after the Second World War. South Africa was one of the 51 founding member states.[6] The Charter of the UN serves as the constitutive document that guides the operation of the UN and member states.[7] Article 1 of the Charter sets out the purposes of the UN

5 South African Law Reform Commission "Privacy and data protection" Project 124 discussion paper 109 October 2005.

6 Between 1974 and 1994 South Africa's membership was suspended owing to international opposition to the policy of apartheid.

7 Charter of the United Nations 24 October 1945 1 UNTS XVI available at http://www.un.org/en/documents/charter (date of use: 10 February 2016).

which include maintaining international peace and security, promoting human rights, fostering social and economic development, protecting the environment, providing humanitarian aid, and to be a centre of harmonisation for nations in order to achieve these common ends.

The principal judicial organ of the UN is the International Court of Justice (ICJ). It was established by Chapter XIV of the Charter and settles legal disputes submitted to it by states in accordance with international law.[8]

The following paragraphs briefly explore important documents issued by the UN in which the right to privacy and the right to dignity (and by extension the right to identity) are protected as fundamental human rights.

#### *5.2.1.2 Universal Declaration of Human Rights*

The UN General Assembly adopted the Universal Declaration of Human Rights (UDHR) in 1948.[9] It arose from the experience of the Second World War and was adopted to define the meaning of the terms 'human rights' and 'fundamental freedoms' which appear in the Charter; it is therefore considered to be a constitutive document of the UN.[10] The UDHR, together with two other UN instruments, the 1966 International Covenant on Civil and Political Rights (ICCPR)[11] and the International Covenant on Economic, Social and Cultural Rights (ICESCR),[12] form the so-called International Bill of Human Rights.[13]

The General Assembly proclaimed the UDHR as

---

8 Ibid arts 92-96.

9 UN General Assembly Universal Declaration of Human Rights 10 December 1948 217 A (III). The Union of South Africa abstained from voting in 1948 in order to protect its system of apartheid.

10 Everything explained today "Universal Declaration of Human Rights Explained" available at http://everything.explained.today/Universal_Declaration_of_Human_Rights/ (date of use: 10 February 2016).

11 United Nations International Covenant on Civil and Political Rights 16 December 1966 999 UNTS 171 and 1057 UNTS 407 / [1980] ATS 23 / (1967) 6 *ILM* 368.

12 United Nations International Covenant on Economic, Social and Cultural Rights 16 December 1966 999 UNTS 171 and 1057 UNTS 407 / [1980] ATS 23 / (1967) 6 *ILM* 368.

13 United Nations "What we do: Protect Human Rights" available at http://www.un.org/en/sections/what-we-do/protect-human-rights/index.html (date of use: 10 February 2016).

> a common standard of achievement for all peoples and all nations, to the end that every individual and every organ of society, keeping this Declaration constantly in mind, shall strive by teaching and education to promote respect for these rights and freedoms and by progressive measures, national and international, to secure their universal and effective recognition and observance, both among the peoples of Member States and themselves and among the peoples of territories under their jurisdiction.[14]

There are at least three notable provisions in the UDHR which are relevant to our topic: article 1 (human dignity), article 12 (right to privacy), and article 19 (freedom of expression).

Article 1 deals with the protection of human dignity. It provides:

> All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

Article 12 deals with the protection of privacy and provides:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 19 protects freedom of expression:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The UDHR is not a legally binding treaty but forms the inspiration for numerous international human rights treaties and declarations, regional human rights conventions, domestic human rights bills, and constitutional provisions.[15] It is also strongly reflected in the Constitution of South Africa.[16]

---

14 Ibid, Preamble.

15 United Nations "Human Rights Day" 10 December 2008 available at http://www.un.org/en/events/humanrightsday/2008/ihrl.shtml (date of use: 10 February 2016).

16 Constitution of the Republic of South Africa, 1996, ss 10, 14 and 16.

#### *5.2.1.3 International Covenant on Civil and Political Rights*

The ICCPR was adopted in 1966 and came into force in 1976 after its ratification by the required number of countries.[17] Privacy is protected in article 17(1):

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.

In terms of article 17(2), everyone has the right to the protection of the law against such interference or attack, but the Covenant itself provides no clear legal mechanism by which individuals can enforce privacy rights.

#### *5.2.1.4 United Nations Guidelines for the Regulation of Computerised Personal Data Files*

The Guidelines for the Regulation of Computerised Personal Files (Guidelines) were adopted in 1990.[18] The Guidelines give member states 'orientations' to follow when implementing regulations concerning computerised data files. They set out non-binding principles concerning the minimum guarantees that should be included in national legislation.[19]

(a) Scope and application

The Guidelines recommend that they should be made applicable by states to public and private computerised files and, optionally, also to manual files.[20] They further recommended that organisations designate the authority statutorily competent to supervise the observance of the Guidelines.[21]

---

17 The International Covenant on Economic, Social and Cultural Rights was adopted and ratified at the same time.

18 UNGA Guidelines for the Regulation of Computerized Personal Files GA res 45/95 14 December 1990.

19 Ibid.

20 Ibid para 10.

21 Ibid para 8.

(b) Principles concerning the minimum guarantees that should be provided in national legislations

The Guidelines adopted the following principles: principle of lawfulness and fairness; principle of accuracy; principle of purpose specification; principle of interested-person access; and principle of non-discrimination.[22]

*Principle of lawfulness and fairness.* Information about persons should not be collected or processed in unfair or unlawful ways, or used for ends contrary to the purposes and principles of the Charter of the United Nations.

*Principle of accuracy.* Persons responsible for the compilation or keeping of files have certain obligations in respect of the accuracy of the data. They must carry out regular checks on the accuracy and relevance of the data. The data must be kept as complete as possible in order to avoid errors of omission. And, finally, data must be kept up to date.

*Principle of purpose-specification.* The purpose for which a file is used should be specified, legitimate, and brought to the attention of the person concerned. This is to ensure that: (a) the personal data collected and recorded remain relevant and adequate for the purposes specified; (b) none of the personal data is used or disclosed, except with the consent of the person concerned and for purposes compatible with those specified; (c) and the period for which the personal data is kept does not exceed that which would enable the achievement of the purpose specified.

*Principle of interested-person access.* This principle gives everyone, irrespective of nationality or place of residence, certain rights in respect of their personal information. All persons, who provide proof of their identity, have the right to know whether information concerning them is being processed, and to obtain a copy of the information in an intelligible form, without undue delay or expense. All persons also have a right to require that appropriate rectifications or erasures be made in the case of unlawful, unnecessary, or inaccurate entries, and, when they are being communicated, to be informed of the addressees. They are also entitled to a

[22] Ibid paras 1-5.

remedy, if need be, from a supervisory authority. The cost of any rectification must be borne by the person responsible for the file.

*Principle of non-discrimination.* Data that is likely to give rise to unlawful or arbitrary discrimination may not be compiled. Such information includes information on racial or ethnic origin, colour, sex life, political opinion, religious, philosophical and other beliefs, as well as membership of an association or trade union. Certain exceptions are allowed. This principle is similar to the sensitivity principle in other data protection documents.

*Power to make exceptions.* Exceptions may be provided for in regard to the principle of fairness and lawfulness of processing, and the principle of access to information, but only if this is necessary to protect national security, public order, public health, or morality, as well as the rights and freedoms of others – in particular persons being persecuted (the so-called 'humanitarian clause'). Such exceptions must be expressly specified in a law or equivalent regulation, their limits must be expressly stated, and appropriate safeguards must be spelled out. Exceptions may also be made to the principle of non-discrimination. These exceptions must be subject to the same safeguards as those prescribed above, and may be authorised only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination.

*Principle of security.* Appropriate measures should be taken to protect the files against dangers such as accidental loss or destruction, unauthorised access, fraudulent misuse of data, or contamination by computer viruses.

*Supervision and sanctions.* The law of every country must designate the supervisory authority which is to be responsible for supervising observance of the above principles. This authority must be impartial, independent vis-à-vis persons or agencies responsible for processing data, and be technically competent. Criminal penalties and individual remedies should be available for the violation of the provisions of the national law implementing the principles.

*Trans-border data flows.* This principle aims to promote the free flow of data across national borders. It states that when the legislation of the countries involved in a

transborder data flow, offer comparable safeguards for the protection of privacy, information should be able to circulate freely. If there are no reciprocal safeguards, undue limitations on such circulation may not be imposed and, if they are, they should be limited to what is required for the protection of privacy.

### 5.2.2 African Union

#### *5.2.2.1 Introduction*

The AU was established in 2002, replacing the Organisation of African Unity (OAU) which was established in 1963. The objectives of the AU are: to promote the unity and solidarity of African states; coordinate and intensify states' cooperation and efforts to achieve a better life for the people of Africa; defend states' sovereignty, territorial integrity, and independence; eradicate all forms of colonialism from Africa; promote international cooperation, having due regard to the UN Charter and the UDHR; coordinate and harmonise members' political, diplomatic, economic, educational, cultural, health, welfare, scientific, technical, and defence policies. All African states – save for Morocco – are members of the AU.[23]

#### *5.2.2.2 Human Rights Charters*

The AU adopted the African Charter on Human and Peoples' Rights (ACHPR) [24] in 1981,[25] and the African Charter on the Rights and Welfare of the Child (ACRWC) in 1990.[26] The ACHPR does not provide for a right to privacy, but the ACRWC does. Article 10 of the ACRWC provides:

---

23 See African Union website www.au.int (date of use: 2 March 2016); The Central African Republic (CAR) has been suspended since 25 March 2013 (PSC/PR/COMM.(CCCLXIII)) and is suspended from all AU activities until constitutional order in CAR is re-established permanently, available at http://au.int/en/AU_Member_States (date of use: 21 December 2016).

24 Also known as the Banjul Charter.

25 Organisation of African Unity (OAU), African Charter on Human and Peoples' Rights 27 June 1981, CAB/LEG/67/3 rev 5 (1982) 21 *ILM* 58. Entered into force 1986.

26 OAU African Charter on the Rights and Welfare of the Child 11 July 1990, CAB/LEG/24.9/49 (1990). Entered into force 1999.

Protection of Privacy

No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.

The African Commission on Human and Peoples' Rights issued a Declaration of Principles on Freedom of Expression in Africa in 2002 which also refers to privacy when it states in article XII.2:

Privacy laws shall not inhibit the dissemination of information of public interest.

Apart from these human rights documents referring to the right to privacy, the AU has also adopted a Convention on data protection.

#### *5.2.2.2 African Union Convention on Cyber Security and Personal Data Protection*

In June 2014 the AU adopted the Convention on Cyber Security and Personal Data Protection at the African Union's Summit in Malabo, Equatorial Guinea.[27] The Convention covers a very wide range of online activities, including electronic commerce, data protection, and cybercrime, with a special focus on racism, xenophobia, child pornography, and national cyber security. The Convention will only come into force once fifteen of the 54 AU member states have ratified it.

(a) Objectives

The aim of the Convention as regards personal data is that states should commit to establishing legal frameworks that strengthen fundamental rights and public freedoms, particularly the protection of physical data. Privacy violations should be punished, but the principle of free flow of personal data should not be prejudiced.[28] States should establish mechanisms that will ensure that data processing respects the fundamental freedoms and rights of natural persons, but at the same time

27 AU Convention on Cyber Security and Personal Data Protection EX.CL/846(XXV) (2012). The text of the Convention is available at https://ccdcoe.org/sites/default/files/.../AU-270614-CSConvention.pdf.

28 AU Convention art 8(1).

recognise the prerogatives of the state, the rights of local communities, and the purposes for which the businesses were established.[29]

(b) Scope of application

The Convention applies to any collection, processing, transmission, storage, or use of personal data by a natural person, the state, local communities, and public or private corporate bodies. Subject to certain exceptions, its application extends to any automated or non-automated processing of data that forms part of a file. The processing should be undertaken in the territory of a state member of the AU. The Convention applies to the processing of data relating to public security, defence, research, criminal prosecution, or state security, subject to certain exceptions provided for by other laws.[30]

Data processing undertaken by a natural person within the exclusive context of his or her personal or household activities is excluded from the scope of the Convention, provided, however, that the data are not for systematic communication to third parties or for dissemination. Also excluded are temporary copies produced by technical means for the purpose of automatic, intermediate, and temporary storage of data in order to offer the best possible access to users of the service.[31]

Any processing for journalistic or research purposes, or for artistic or literary expression, is deemed acceptable, if conducted within the ambit of professional codes of conduct.[32]

(c) Basic principles governing the processing of personal data

The Convention has six basic principles governing the processing of data: the principles of consent and legitimacy; lawfulness and fairness; purpose, relevance, and storage; accuracy; transparency; confidentiality; and security.[33] Sensitive

29 AU Convention art 8(2).
30 Ibid art 9(1).
31 Ibid art 9(2).
32 Ibid art 14(3).
33 Ibid art 13.

personal data (ie data revealing racial, ethnic and regional origin, parental filiation, political opinion, religious or philosophical beliefs, trade union membership, sex life; and genetic information (or, more generally, data on the state of health of the data subject) may not be processed, unless certain specific exemptions are applicable.[34]

(d) Data subject rights and data controller obligations

In terms of the Convention, a data subject has a right to information; right of access; right to object; and a right of rectification or erasure.[35] A data controller has obligations relating to confidentiality, security, storage, and sustainability.[36] A data controller also has an obligation to make a declaration before the data protection authority in regard to the data processing, unless: the processing activities are exempted from the scope of the Convention; the processing is undertaken in order to maintain a register for private use; or the processing is undertaken by a non-profit making association or body with a religious, philosophical, political or trade union aim.[37]

(e) Special processing activities

The Convention prohibits profiling or automated decision making,[38] and regulates data matching. Data matching (referred to as 'interconnection of files') may only take place after authorisation by the data protection authority,[39] and should assist in achieving legal or statutory objectives which are of legitimate interest to data controllers.[40] Data processing involving a national identification number, genetic information, biometric information, and information on offences, convictions and security measures, are also subject to prior authorisation.[41] Direct marketing is also addressed as part of the chapter on Electronic Transactions. Direct marketing using any form of indirect communication is prohibited unless the individual has given prior

34 Ibid art 14.
35 Ibid arts 16-19.
36 Ibid arts 20-23. The sustainability obligation is a novel one, and states that the data controller must take appropriate measures to ensure that processed personal data can be utilised regardless of the technical device employed in the process. In particular, it must be ensured that technological changes do not constitute an obstacle to the utilisation.
37 Ibid art 10.
38 Ibid art 14(5).
39 Ibid art 10(4).
40 Ibid art 15.
41 Ibid art 10(4).

consent to such direct marketing.[42] Direct marketing by means of e-mail is only allowed if: the particulars of the addressee have been obtained directly from him or her; the recipient has given consent to be contacted by the marketing partners; and the direct marketing concerns similar products or services provided by the same individual or corporate body.[43]

(f) Data protection authority (DPA)

Each AU member state is required to have a national data protection authority that must be an independent administrator with certain powers and duties.[44] Most data processing activities may only take place after a declaration has been made before the DPA.[45] For certain sensitive processing activities, the DPA must give prior authorisation.[46] Certain processing activities may only take place in terms of legislation or a regulatory Act, and in such a situation a DPA must give 'informed advice' before the Act or regulation is enacted.[47]

(g) Cross border transfers

A data controller may not transfer personal data to a non-member state of the AU unless such a state ensures an adequate level of protection for the privacy, freedoms, and fundamental rights of persons whose data are being processed, or unless the data controller has requested authorisation for such transfer from the national protection authority.[48]

(h) Conclusion

42 Ibid art 4(3).
43 Ibid art 4(4).
44 Ibid art 11 and 12.
45 Ibid art 10(2).
46 Ibid art 10(4).
47 Ibid art 10(5).
48 Art 14.

The provisions on personal data protection in the Convention were clearly influenced by the EU Directive.[49] It is still too early to determine whether it will have an influence on the adoption of data privacy laws in Africa.

### 5.2.3 Organisation for Economic Cooperation and Development

The OECD is an international organisation established in 1948. It comprises of 34 of the leading industrialised states, including all the EU member states and the United States. South Africa is a non-member economy with which the OECD has a working relationship. The OECD Council adopted a resolution on 16 May 2007 to strengthen the cooperation with South Africa, as well as with Brazil, China, India and Indonesia, through a programme of enhanced engagement.[50]

The mission of the OECD is to promote policies that will improve the economic and social well-being of people around the world. It provides a forum in which governments can work together to share experiences and seek solutions to common problems, be they social, economic, or environmental. It aims to set international standards on a range of issues.[51]

In the next section I examine the OECD Guidelines on data protection which are relevant to the development and recognition of the rights to privacy and identity.

#### *5.2.3.1 OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (OECD Guidelines on Data Protection)*

The OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (OECD Guidelines) were adopted in 1980[52] and revised in 2013.[53]

49 Greenleaf & Georges (2014) *Privacy Laws & Business International Report* 18.
50 See OECD website at http://www.oecd.org/southafrica (date of use: 20 December 2015).
51 See OECD website at http://www.oecd.org/about/ (date of use: 20 December 2015).
52 OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Paris (23 September 1980).
53 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy available at http://www.org (date of use: 20 December 2015).

The OECD Guidelines were the first international statement on data protection,[54] and contain a set of data protection principles that set minimum standards for member states, who may supplement the conditions with additional measures. The OECD Guidelines are not legally binding on member states, but merely recommendations to guide member states[55] contemplating adopting or revising national legislation. The OECD Guidelines on data protection have influenced both national and international data protection laws.[56] They remain an influential statement of the foundations of privacy protection.[57]

(a) Scope

The OECD Guidelines apply to personal data, whether in the public or private sectors, which, because of the way in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties.[58] Consequently, these Guidelines neither distinguish between the processing of personal data in the private and public sectors, nor between manual or automatic processing of personal data.

(b) The OECD Guidelines data protection principles

There are eight basic data protection principles.

(i) *Collection limitation principle*. There should be limits to the collection of personal data and such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

(ii) *Data quality principle*. Personal data should be relevant, accurate, and kept up to date taking into account the purpose for which they will be used.

---

54 See Kirby 2011 *International Data Privacy Law (IDPL)* 6.

55 Roos "Data protection law" 321.

56 South African Law Reform Commission Discussion Paper 109, Project 124, October 2005. Reference was here made to the OECD Guidelines on data protection and they influenced South Africa's data protection law, which contributed to the promulgation of the Protection of Personal Information Act 4 of 2013.

57 Bygrave *Data Privacy Law* 50.

58 OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data s 2; also see Roos "Data protection law" 378.

(iii) *Purpose specification principle*. Personal data should be used only for purposes specified at the time of its collection; subsequent use of the data should be for the same or a compatible purpose.

(iv) *Use limitation principle*. Any disclosure or use of personal data should be for the purpose initially specified, unless the data subject has consented to a different purpose or a different purpose has been authorised by law.

(v) *Security safeguards principle.* Personal data should be protected by reasonable security safeguards against risks such as unauthorised access, destruction, use, modification, or disclosure.[59]

(vi) *Openness principle.* There should be a general policy of openness as regards developments, practices, and policies in respect of personal data. Means should be readily available to establish the existence and nature of personal data, the main purposes for which they are used, and the identity and usual residence of the data controller.

(vii) *Individual participation principle*. Data subjects have the right to participate in the processing of their data. Therefore, they have a right to access their personal data, and to be given reasons for any denial of such access. They also have a right to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended

(viii) *Accountability principle.* A data controller should be accountable for implementing the above principles.[60]

The Guidelines were reviewed in 2013 and now also require that a data controller should have a privacy management programme in place. This should include privacy policies, employee training and education, provisions for sub-contracting, an audit

---

59 In September 2015 the OECD Council adopted the Recommendation on Digital Security and Risk Management for Economic and Social Prosperity (Digital Security and Risk Management Recommendation (DSRMR)). The DSRMR was developed as a result of a growing number of uncertainties relating to the use of the digital environment. An increase in digital security threats and incidents has led to significant financial, privacy, and reputational consequences, as well as physical damage. The DSRMR should be seen as complementary to the OECD Guidelines on data protection. The OECD Council emphasised "that digital security risk management provides a robust foundation to implement the 'Security Safeguards Principle' in the OECD Privacy Guidelines", and that the DSRMR and the OECD Privacy Guidelines mutually reinforce each other. See OECD Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document (2015) 7.

60 OECD Guidelines on data protection paras 7-14; www.oecd.org (date of use: 29 May 2016). Also see Jay *Data Protection* 9.

process, and privacy risk assessment. The revisions also introduced mandatory data security breach notification – the privacy enforcement authority and individuals should be notified when a significant breach which is likely to affect individuals adversely has occurred.[61]

### 5.2.4 Council of Europe

The Council of Europe should not be confused with the European Council; the latter institution is discussed below.[62] The Council of Europe was established in 1949 after the Second World War as a structure for political cooperation between the democratic European countries. At present it comprises 47 member states of which 28 are members of the EU.

In 1950, delegates representing various European states met in Rome to discuss human rights. These discussions led to the enactment of the European Convention on Human Right (ECHR).[63] The ECHR was signed into law by ten member states.[64]

All Council of Europe member states must sign up to the ECHR. The aims of the Convention are to protect human rights, democracy, and the rule of law. The judicial organ of the Council of Europe is the European Court of Human Rights which oversees the implementation of the Convention in the member states.[65]

The ECHR is 'soft law'; in order for it to be binding it must ratified by the member states. In the United Kingdom, for example, the ECHR has been implemented through the Human Rights Act 1998.[66] The ECHR requires of member states to provide an effective remedy against human rights violations. These remedies can be found in states' human rights or tort laws.[67]

---

61 OECD Guidelines on Data Protection para 15.

62 Kuner *European Data Protection Law* 48.

63 Council of Europe European Convention for the Protection of Human Rights and Fundamental Freedoms ETS 5 (4 November 1950). The Convention entered into force in 1953.

64 Belgium, Denmark, France, Ireland, Italy, Luxembourg, Netherlands, Norway, Sweden and the United Kingdom.

65 Council of Europe "Who we are" available at http://www.coe.int/en/web/about-us/who-we-are (date of use: 15 February 2016).

66 Act of 1998.

67 Van Dam *European Tort Law* 23.

*5.2.4.1 European Convention on Human Rights (ECHR)*

Article 8(1) of the ECHR guarantees the right to privacy. It refers to “the right to respect for private and family life, home and correspondence.” Article 8(2) lays down the conditions under which restrictions of this right are permitted.

> Article 8 – Right to respect for private and family life
>
> 1 Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The provisions of article 8 are broad enough to cover data protection and a tort of privacy invasion.

Article 10 of the ECHR guarantees freedom of expression:

> 1 Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2 The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

The right to privacy and the right to freedom of expression enjoy equal status and neither articles 8 nor 10 takes precedence over the other. When deciding whether it is appropriate to bar the disclosure of private information, a balance must be struck between freedom of expression and the right to privacy. For instance, a court is likely

to permit publication of matters of legitimate public interest. Also, information will not be protected against publication if it is already public knowledge.[68]

As said, the European Court of Human Rights (ECtHR) in Strasbourg oversees the implementation of the Convention in the member states. Individuals can bring complaints of human rights violations to the Strasbourg Court once all avenues of appeal have been exhausted in the member state concerned. An applicant need not be a national of one of the member states.[69]

The ECtHR has heard several complaints from individuals about infringements of article 8. In *Bărbulescu v Romania*[70] the ECtHR heard a complaint by a Romanian engineer who was fired from his work because he used his Yahoo Messenger account, which was created to respond to clients' enquiries, for personal purposes. The company had a policy that strictly forbade employees to use computers, photocopiers, telephones, telex, and fax machines for personal purposes. The engineer had sent personal messages to family members and his fiancée. When confronted by the employer about his unauthorised personal use, he denied such use. The employer then showed him a printout of personal messages he had sent. He sued his employer on the ground that his right to private life under article 8 of the ECHR had been infringed.

The court pointed out that it has consistently held that the notion of private life is a broad concept that encompasses, for example, the right to establish and develop relationships with other human beings, and the right to identity and personal development.[71] The court has also held that telephone calls from business premises are *prima facie* covered by the notions of 'private life' and 'correspondence' for purposes of article 8(1).[72] E-mails sent from work, and information derived from the monitoring of personal Internet usage, should also be protected under article 8.[73] In all of these instances an employee has a reasonable expectation of privacy. The

---

68 Giliker & Beckwith *Tort* 468.

69 Council of Europe *Handbook*4 available at www.echr.coe.int/Documents/Handbook (date of use: 15 February 2016).

70 [2016] ECHR 61.

71 See *Niemietz v Germany* 16 December 1992 Series A no 251 B § 29; *Fernández Martínez v Spain* [GC] no 56030/07 § 126 ECHR 2014 (extracts).

72 See *Halford v The United Kingdom* (1997) 24 EHRR 523 and *Amann v Switzerland* [GC] no 27798/95 § 43 ECHR 2000‑II.

73 *Copland v The United Kingdom* no 62617/00 § 41 ECHR 2007- I.

court therefore had to decide whether in the case under discussion the applicant had a reasonable expectation of privacy when communicating from the Yahoo Messenger account that he had registered at his employer's request. The court noted that it was not disputed that the applicant's employer's internal regulations strictly prohibited employees from using the company's computers and resources for personal purposes. The court was, therefore, of the opinion that the case differed from previous cases in which the personal use of an office telephone was allowed or, at least, tolerated. The court was satisfied that the applicant's 'private life' and 'correspondence' within the meaning of article 8 were limited by these measures, but as the employer had accessed the applicant's Yahoo Messenger account in the belief that it contained professional messages, the employer had acted within its disciplinary powers and such access had therefore been legitimate.[74]

The result of this case is that, according to the ECtHR, where an employer has banned the use of a computer or the Internet for personal purposes, the employee does not have a reasonable expectation of privacy in regard to personal information exchanged in a communication using the computer or the Internet. By analogy, one could probably argue that an employee, who uses a social network service such as Facebook on an employer's computer during working hours, would also not have a reasonable expectation of privacy. On the other hand, Facebook entries are usually made for personal purposes, and an employer would find it difficult to argue that he or she thought the information on Facebook dealt with work issues.

In 2010 Bowen[75] analysed the ECtHR decisions on 'private life' and distilled six categories of protected interests. These are:

- *Physical and psychological (or moral) integrity*, that is, matters impacting on a person's body or mental health (such as physical assault and caning, sexual assault, conditions of detention, searches, etc).[76] These rights are similar to the personality right to bodily integrity in South African law.

---

74 [2016] 31496/08 ECHR 61 para [57].

75 Bowen ALBA *Article 8 and "private life": The protean right* The Constitutional and Administrative Law Bar Association Seminar 2 March 2010 6-8.

76 Costello-Roberts (1995) 19 EHRR 112; *Gaskin v United Kingdom* (1989) 12 EHRR 36; *Raninen v Finland* (1998) 26 EHRR 563; *Shelley v UK* (2008) 46 EHRR SE16.

- *The right of autonomy or self-determination*, or "the right to conduct one's life in a manner of one's own choosing".[77] This protects a person's right to refuse medical treatment, and the right to choose the timing and manner of one's own death.[78]
- *The right to identity and personal development*, which, inter alia, includes the right to choose a name, gender identification, sexual orientation, and sexual life, and whether to have a child or not to have a child.[79] The scope of this right goes far wider that the right to identity under South African law.
- *The right to establish and develop relationships with other human beings*. This includes the right of prisoners to associate with each other and to maintain contact with their families. Relationships that are not close enough to fall within 'family life' are also protected under this aspect.[80] One could ask whether the right to form on-line friendships could also be protected under this right.
- *The protection of private sphere and private space (privacy)*. This is the core value and protects, amongst others, against telephone tapping, publication of confidential information, and surveillance.[81] It may extend to personal interactions taking place in a public place if the person has a reasonable expectation of privacy in that situation.[82] Communications on Facebook will fall into this category.
- *State action having financial consequences, such as taxation*.[83]

Identity and privacy as defined in South African law are thus protected by the right to 'private life'. The right to establish relationships with other human beings is of course also relevant in the SNSs environment.

---

77 *Pretty v UK* (2002) 35 EHRR 1 par 62.

78 *Pretty v UK* (2001) 35 EHRR 1; *R (Purdy) v DPP* [2009] UKHL 45; [2009] 3 WLR 403.

79 *Stjerna v Finland* (1997) 24 EHRR 195; *Goodwin v UK* (2002) 35 EHRR 18*; R (B) v MOJ* [2009] EWHC 2220 (Admin); *Dudgeon v UK* (1983) 5 EHRR 573; *Norris v Ireland* (1991) 13 EHRR 186; *Laskey v UK* (1997) 24 EHRR 39; *EB v France* [GC] (2008) 47 EHRR 21.

80 *McFeeley v UK* (1981) 3 EHRR 161; *McCotter v UK* (1993) 15 EHRR CD98; *Wakefield v UK* No 15817/89 (1 October 1990); *Slivenko v Latvia* (2004) 39 EHRR 24.

81 See *Halford v the United Kingdom* (1997) 24 EHRR 523.

82 *Peck v UK* (2003) 36 EHRR 719; *Von Hannover v Germany* (2005) 40 EHRR 22.

83 Bowen "*Article 8 and 'private life': The protean right"* 8.

*5.2.4.2 Council of Europe Convention on Data Protection*

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was signed in 1981, and came into force in 1985 after ratification by the required number of countries.[84] It is based on article 8 of the ECHR,[85] but it was felt that article 8 was not adequate to protect all personal information and that a more proactive approach was needed.[86] The Convention was the first legally binding international instrument with worldwide significance for data protection.[87] It is open for signature by member states and for accession by non-member states.[88]

The purpose of the Convention is "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him".[89] The Convention applies to automated personal data files and automatic processing of personal data in the public and private sectors.[90]

Chapter Two of the Convention sets out the basic principles for data protection. These include principles regarding the quality of data, special categories of data, data security, and the rights of data subjects.[91] Chapter Three of the Convention deals with the "Trans-border flows of personal data and domestic laws".[92]

---

84 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data No 108/1981 (Convention 108/1981).

85 See, eg, *MS v Sweden* 20837/92 [1997] ECHR 49 where the ECtHR has stated that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by article 8 of the ECHR.

86 Hustinx "The reform of EU data protection" 63.

87 Council of Europe Directorate General of Human Rights and Legal Affairs *Data Protection: Compilation of Council of Europe Texts* 2010 8; also see Greenleaf "A world data privacy treaty?" 94.

88 Convention 108/1981, art 23 provides:

> 1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

Also see Greenleaf (2008) 94 *Privacy Laws & Business International* 13-14.

89 Convention 108/1981 art 1.

90 Ibid art 3.

91 Ibid arts 5-7.

92 Ibid art 12.

An Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Trans-border Data Flows was adopted in 2001. The Protocol requires the establishment of national supervisory bodies and the setting of standards for trans-border data flows to non-contracting states.[93]

In 2010 the Committee of Ministers of the Council of Europe met to respond to rapid technological and globalisation trends that have brought new challenges for the protection of personal data.[94] The Consultative Committee of the Council of Europe adopted the final proposals.[95]

Roos[96] notes that the Convention has been an important stimulus for data privacy legislation in member countries of the Council of Europe.

#### *5.2.4.3 Council of Europe Recommendations*

The Committee of Ministers of the Council of Europe, which is the decision-making body of the Council, may make recommendations to member states on matters for which the Committee has agreed on 'a common policy'. These recommendations are not binding, but are very influential. Several recommendations dealing with the protection of privacy in specific sectors have been issued over the years, such as a recommendation on the protection of medical data, on the protection of privacy on the Internet, on the protection of personal data collected and processed for insurance purposes, and a recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling.[97]

---

93 Council of Europe Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows (2001).

94 Recommendation 679 for a Council Decision authorising the opening of negotiations on the modernisation of Council of Europe Convention for the protection of individual with regard to automatic processing of personal data (EST 108), and the conditions and modalities of accession of the European Union to the modernised Convention (16 November 2012); also see Roos "Data privacy law" 377.

95 The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (EST 108) available at https://www.coe.int/...documents/T-PD(2012)RAP29Abr%20E%20-%20Abridged%2.

96 Roos "Data privacy law" 382.

97 Recommendation (97)5 on the Protection of Medical Data (13 Feb 1997); Recommendation (99)5 on the protection of privacy on the Internet (23 Feb 1999); Recommendation (2002)9 on

### 5.2.5 Conclusion

In this section, dealing with international instruments, I have established that both the right to privacy and the right to identity are considered worthy of protection at the international level. Privacy is usually expressly identified, whereas identity is protected indirectly, sometimes as part of privacy, other times as part of dignity. I also established that these rights must be balanced against other fundamental rights, in particular the right to freedom of expression. I further pointed out that data protection laws also come into play when personal information is processed, for example by publishing it online.

In the following section I consider the law of the EU.

---

the protection of personal data collected and processed for insurance purposes (18 Sept 2002); Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 Nov 2010).

## 5.3 EUROPEAN UNION (EU)

### 5.3.1 Introduction

In this section I consider EU law as regards the right to privacy and identity in order to establish how the law of the EU applies to and influences the laws of its member states, as well as states outside the EU. The recognition and development of the right to privacy and the right to identity at EU level, particularly in the context of SNSs, are investigated. The rights to privacy and identity are often interlinked,[98] and both these rights may be protected as human rights and also under tort law or the law of delict. Data protection law also protects the right to privacy and identity of persons when their personal information is processed – for example when someone posts personal information regarding another person on a website – and I therefore also consider data protection laws. The transposition of EU laws into the law of member states is also examined.

It should always be remembered that all the EU member countries are also members of the Council of Europe and have all ratified the ECHR. Decisions by the ECtHR on this Convention are therefore applicable in EU member countries.

### 5.3.2 Overview of the legal system

The European Community (EC), the predecessor to the EU, was set up after World War II with the aim of bringing an end to wars between neighbouring countries and achieving economic and political stability. The EC had six founding members: Belgium, France, Germany, Italy, Luxembourg, and the Netherlands.[99] The EU currently comprises of 28 member states.[100] Each member state in the EU has full sovereignty and independence, and may act independently on an international

98 Bruggemeier, Ciacchi & O'Callaghan *Personality Rights in European Tort Law* 9.

99 http://europa.eu/about-eu/eu-history (date of use: 08 May 2014).

100 Ibid. Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

level.[101] The EU often adopts legislation (such as Regulations, Directives, and Decisions) with the aim of harmonising specific areas of the law. *Regulations* are directly binding upon all member states without the need for implementation into national law. *Directives* do not have a direct legal binding effect on member states; their provisions need to be transposed into the national laws of the member states. *Decisions* are binding upon whomever they are addressed to, and are aimed at individual governments, groups, or individuals. EU law generally takes precedence in the case of conflict with the national law of member states.[102]

A majority of the EU member states follow a civil-law system, as opposed to a common-law system.[103]

The EU is made up of the following institutions: the European Parliament; the European Commission; the Council of the European Union; the European Council; and the Court of Justice of the European Union (CJEU).[104] All of the above institutions have a unique and an important role within the EU.

The European Parliament is the law-making body and represents the EU citizens. Its members are directly elected by EU voters every five years.[105] The individual member states are allocated a number of seats in the European Parliament. The European Parliament meets in Brussels, Luxembourg, and Strasbourg.[106]

The European Commission serves as the EU's executive body and promotes its general interests. It is based principally in Brussels and Luxembourg. It is responsible for proposing new laws and for their implementation once they have been adopted by the Parliament and the Council of the EU. It is also responsible for implementing policies and the EU budget. The European Commission monitors the

---

101 Kuner *European Data Protection Law* 5. This is in contrast to the United States where the federal states may not act independently at international level.

102 Ibid 34.

103 The main feature of civil law is that it is contained in codes. The courts' task is to apply and interpret the law in the code. Whereas civil law is a codified system, common law is based mainly on case law. In common caw, earlier judicial precedents should be respected – a principle known as *stare decisis.* In a civil law system case law does not have binding force and the doctrine of *stare decisis* does not apply. See Pejovic (2001) 32 *Victoria University of Wellington Law Review* 817; Lomio & Spang-Hanssen *Legal Research Methods in the US and Europe* 102.

104 See www.europa.eu/about-eu (date of use: 8 May 2014).

105 Kuner *European Data Protection Law* 5; www.europarl-europa.eu (date of use: 8 May 2014).

106 Kuner *European Data Protection Law* 7.

treaties and the executive administration of the EU.[107] The European Commission can take action against any member state which fails to implement a Directive within the time limit provided, and for contravention of European laws.[108]

The Council of the EU is an institution which represents member states' governments. It comprises of government ministers. The national ministers from each member state meet in the Council to adopt laws and to coordinate policies. This institution is, therefore, also involved in the enactment of EU legislation.[109]

The European Council, (which should not be confused with the Council of the EU referred to above, or with the Council of Europe both of which have been discussed previously), defines the general political direction and priorities of the EU. The European Council brings together EU leaders to set the EU's political agenda. It represents the highest level of political cooperation between EU countries. This institution does not exercise legislative functions, and is not involved in the enactment of EU legislation.[110]

The Court of Justice of the European Union – not to be confused with the ECtHR which is the judicial organ of the Council of Europe – is the judicial authority of the EU. It ensures the uniform application and interpretation of EU law. It has its seat in Luxembourg and is composed of one judge per member state (currently 28) and is assisted by eleven Advocates-General. A member state may bring a matter before the European Court of Justice. The courts of an EU member state may also refer a question on EU law to this court for interpretation. The European Commission may also bring a matter against a member state for failing to implement an instrument of EU law.[111]

Although not an official EU institution, reference can also be made to the European Data Protection Supervisor situated in Brussels. This is an independent supervisory authority responsible for monitoring compliance by the European Commission institutions and bodies as regards their data protection obligations. It covers only the processing of personal data by EC institutions and bodies. Processing of personal

107 Ibid 5.
108 Ibid 37.
109 See www.consilium.europa.eu (date of use: 8 May 2014).
110 See www.consilium.europa.eu/en/european-council/ (date of use: 5 October 2016).
111 Kuner *European Data Protection Law* 7.

data in the member states, falls under a particular state's national legislation adopted in compliance with its obligations under EU law.

### 5.3.3. EU legislation on privacy and data protection

#### *5.3.3.1 Charter of Fundamental Rights of the European Union*

The Charter of Fundamental Rights of the EU[112] protects both the right to privacy and the right to protection of personal data as two distinct fundamental human rights. It recognises the right to privacy in article 7 and the right to the protection of one's personal data in article 8.

Article 7 provides:

> **Respect for private and family life**
>
> Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 provides:

> **Protection of personal data**
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

Limitations may be placed on these rights, but in order to be justified, the limitations must be provided for by law, must respect the essence of the rights limited, and,

112 EU Charter of Fundamental Rights of the European Union 2010 *OJ* (C 83) 02. The Charter became legally binding on the EU institutions and on national governments on 1 December 2009, with the entry into force of the Treaty of Lisbon (EU Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community 2007/C 306/01).

subject to compliance with the principle of proportionality, must be necessary and genuinely meet objectives of general interest recognised by the EU, or the need to protect the rights and freedoms of others.[113]

In *Volker und Markus Schecke v Land Hessen*[114] these limitation principles were considered by the CJEU. In this case the two applicants were German farmers who received agricultural aid from two EU agricultural funds. The website of the German Federal Office for Agriculture and Food made available to the public the names of beneficiaries of aid from these funds, the place at which those beneficiaries reside, and the annual amounts received. The two farmers asked the Administrative Court, Wiesbaden (Germany) to require the Land of Hesse not to publish the data relating to them. The court took the view that the EU rules – which imposed the obligation to publish those data – amounted to an unjustified interference with the fundamental right to the protection of personal data, and the national court therefore requested the CJEU to examine the validity of those rules.

The CJEU took the view that, while it is true that in a democratic society taxpayers have a right to be kept informed of the use made of public funds, the fact none the less remains that striking a proper balance between the various interests involved makes it necessary for the institutions concerned, before adopting the disputed provisions, to ascertain whether publication, via a single, freely-accessible website in each member state, of data naming each of the beneficiaries concerned and the precise amounts received by each of them – with no distinction being drawn regarding the duration, frequency, or nature and amount of the aid received – did not go beyond what was necessary for achieving the legitimate aims pursued.

The court held that by imposing an obligation to publish personal data relating to each natural person who was a beneficiary of aid under the funds, without drawing a distinction based on relevant criteria such as the periods during which those persons received such aid, the frequency of such aid, or the nature and amount thereof, the

113 Charter of Fundamental Rights art 52. All EU member states are also state parties to the European Convention of Human Rights and Fundamental Freedoms (discussed above) which protects the right to privacy in art 8.

114 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* ECLI:EU:C:2010:662 para [48].

Council and the Commission had exceeded the limits imposed by compliance with the principle of proportionality.[115]

One of the rights that can come into conflict with the right to privacy and the right to data protection is the right to freedom of expression which is protected in article 11 of the Charter.

Article 11 provides:

> **Freedom of expression and information**
>
> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
>
> 2. The freedom and pluralism of the media shall be respected.

The Directive on Data Protection[116] (which I discuss below) also provides for a balancing of the right to privacy with the right to freedom of expression by stating, in article 9, that member countries must allow for exemptions to the provisions of the Directive where personal data are processed solely for journalistic purposes, or for purposes of artistic or literary expression, if the exemptions are necessary in order to reconcile the right to privacy with the rules governing freedom of expression.[117]

An example of the interaction between the right to data protection and the right to freedom of expression is to be found in a case where two Finnish media companies published the tax data of 1,2 million natural persons. The data were lawfully obtained from the Finnish tax authorities and were a matter of public record. However, the Finnish Data Protection Board forbade the companies to collect, save, and process the taxation data on so large a scale in future. The case was referred to the CJEU for a preliminary ruling.[118]

---

115 Ibid para [79].

116 EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data 95/46/EC *OJ L* 281/31 (Data Protection Directive or Directive 95/46/EC).

117 Dir 95/46/EC art 9.

118 The courts of the EU member states may refer questions about the interpretation of European Union law that arise in disputes which have been brought before them, to the CJEU for a preliminary ruling. The CJEU does not decide the dispute itself. It is for the national court to dispose of the case in accordance with the court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

The CJEU held that the publication of the tax data amounted to 'a processing of personal data' within the meaning of the EU Directive on data protection. The court also held that the activities of the media could be classified as 'journalistic activities' within the meaning of that term in article 9 of the Directive, if their object was the disclosure to the public of information, opinions, or ideas, irrespective of the medium used to transmit them. The court further ruled that these activities are not limited to media undertakings and may be undertaken for profit-making purposes. As the case was referred to the CJEU for a preliminary ruling, the CJEU left it to the national court to determine whether this was the situation in this specific case.[119]

After proceeding at national level, the case was subsequently heard by the ECtHR which held that the prohibition by the Finish Data Board was a legitimate interference in the applicants' right to freedom of expression and information.[120] The ECtHR accepted the finding by the Finnish authorities that, in this instance, the publication of personal data could not be regarded as journalistic activity, in particular because the journalistic-purposes exception was to be interpreted strictly. The court noted that the media companies were not subjected to a general prohibition on publishing private persons' tax information, but only to a limited prohibition. [121]

#### *5.3.3.2 EU Data Protection Directives (and proposed Regulation)*

As I have indicated, the European Union treats the protection of personal data as a matter of great importance, protecting it as a fundamental right.[122] Several Directives protecting personal data have been adopted since 1995, the first of which was the Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, adopted in 1995.[123] This Directive is usually referred to as the 'Data Protection Directive' or the 'General Data Protection Directive'. Other Directives have since been adopted which have translated the

119 C-73/07 *Satamedia Case* ECLI:EU:C:2008:727.
120 *Satakunnan Markkinapörssi Oy And Satamedia Oy v Finland* App no 931/13 ECtHR (21 July 2015) para 55.
121 Ibid para 63.
122 Charter of Fundamental Rights of the European Union of 2000 art 8.
123 Directive 95/46/EC.

general principles of the 1995 Directive to specific areas. Of relevance for the current discussion are the Directives on electronic communications. The most recent Directive on electronic communications is the so-called 'e-Privacy Directive' of 2009.[124]

The European Commission recently proposed a reform package stating that the current rules on data protection needed to be modernised in light of rapid technological developments and globalisation. The reform package consists of a proposal for a General Data Protection Regulation[125] intended to replace the 1995 Data Protection Directive, as well as a Directive for the law enforcement area.[126] The Regulation was adopted on 27 April 2016 and will come into effect from 6 May 2018.[127] However, currently the 1995 Data Protection Directive remains the principal legal instrument on data protection in the EU.

As the 1995 Data Protection Directive has had a major influence on the South African Protection of Personal Information Act 4 of 2013, I address certain aspects of the Directive relevant to the topic under discussion in some detail.

(a) General Data Protection Directive

---

124 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws ( e-Privacy Directive or Directive 2009/136/EC). This Directive is sometimes referred to as the 'Cookie Directive' because it deals with cookies in art 5(3).

125 European Commission Proposal for a regulation of the European Parliament and of the Council 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) Brussels (25 January 2012) 2012/0011 (COD).

126 European Commission Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement free movement of such data Brussels (25 January 2012) COM(2012)10Final.

127 European Commission Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Regulation (EU) 2016/680) art 59 (1).

The EU Directive on data protection evolved from the earlier OECD Guidelines and Convention on data protection, but sets a higher level of protection for data subjects.[128]

*Aim*

The purpose of the Directive is to ensure the free flow of personal data between EU member states while at the same time ensuring a 'high level of protection' for the fundamental rights and freedoms of individuals –the right to privacy in particular. This it aims to achieve by setting standards for the protection of personal information that will ensure an equivalent level of protection in all the member countries, and by prohibiting member states from inhibiting the free movement of personal data between them on grounds related to the protection of the rights of individuals.[129]

*Scope*

The Data Protection Directive applies to the processing of personal data by a data controller where the processing is done wholly or partly by automatic means, or by non-automatic means, provided that the personal data form part of a filling system, or are intended to form part of a filling system.[130]

The data controller is the natural or juristic person, public authority, agency, or other body which determines the purposes for which and the means by which data are processed.[131] The EU Working Party on data protection[132] has pointed out that in the context of social network services (SNSs), several persons can qualify as data

128 Roos 2012 *SALJ* 400, 405.

129 Directive 95/46/EC Recitals 3, 7, 8, 9 and 10. The Data Protection Directive starts with 72 Recitals. Recitals in Directives are preliminary statements that explain the background to the Directive. Recitals always start with 'whereas…'. According to Bennett & Raab 1997 *Inf Soc* 245, 249 the "'whereas' statements state intentions, place this Directive in the context of other values and policies, help interpretation and reflect the variety of interests that shaped its content". See also Greenleaf (1995) 2 *Int Priv Bul* 11.

130 Directive 95/46/EC art 3.

131 Ibid art 2(d).

132 Ibid art 29(1) establishes a Working Party on the Protection of Individuals with regard to the Processing of Personal Data (also referred to as the Article 29 Working Party). It has advisory status and acts independently. It is composed of representatives of the member states' Data Protection Authorities (DPAs). Its tasks are set out in article 30 of the Data Protection Directive, and in article 15 of the Data Retention Directive. (The Data Retention Directive is discussed below.) The Article 29 Working Party plays an important and influential role in interpreting EU Data Protection law. It provides interpretative documents in the form of opinions and recommendations. Although the opinions and recommendations do not have legal binding effect, they often influence the adoption of legal binding rules.

controllers. First, the SNS can be a controller in that it provides the means for the processing of user data, and provides all the basic services related to user management (such as registration and deletion of accounts). The SNS provider also determines the use that may be made of user data for advertising and marketing purposes. Second, third-party providers of applications may also be data controllers. Third, the SNS user can act as a controller when he or she discloses personal information of third parties on the website, unless an exemption applies.[133]

*Exemptions from Directive*

In the context of SNSs two specific exemptions or exclusions need to be examined. First of all, article 3(2) excludes from the Directive as a whole, the processing of personal data by a natural person in the course of a purely personal or household activity.[134] The Directive explains in Recital 12, that activities which are exclusively personal or domestic include correspondence and the holding of records of addresses.

The meaning of 'purely personal or household activity' came under scrutiny by the CJEU in the *Bodil Lindqvist* case.[135] Mrs Lindqvist worked as a catechist in the parish of a church in Alseda (Sweden). She set up Internet pages at home on her personal computer in order to allow parishioners preparing for their confirmation to obtain information they might need. At her request, the administrator of the Swedish Church's website set up a link between those pages and that site. The webpages set up by her contained information about her and eighteen colleagues in the parish, including, in some cases, their full names, and in others only their first names. She also described the jobs held by her colleagues and their hobbies. In some instances family circumstances and telephone numbers were mentioned. She also stated that one colleague had injured her foot and was on half-time on medical grounds. Lindqvist had not informed her colleagues of the existence of the pages or obtained their consent, nor had she notified the *Datainspektionen* (the Swedish supervisory authority for the protection of electronically transmitted data) of her activity. She

133 EU Art 29 DP WP Opinion 5/2009 on online social networking WP 5-6.
134 Directive 95/46/EC art 3(2).
135 Case C-101/01 *Bodil Lindqvist* ECLI:EU:C:2003:596. See also C-73/07 *Satamedia case* ECLI:EU:C:2008:727 para [44].

removed the pages in question as soon as she became aware that they were not appreciated by certain of her colleagues.

The public prosecutor brought a prosecution against Lindqvist charging her with breaching the Swedish data protection law[136] on the grounds that she had processed personal data by automatic means without giving prior written notification to the data protection authority; processed sensitive personal data (injured foot and half-time on medical grounds) without authorisation; and had transferred personal data to a third country without authorisation. I refer to second and third grounds later in the discussion.

The case was referred to the CJEU for a preliminary ruling on certain questions. The following rulings are of interest for the current discussion:

- The act of referring, on an Internet page, to various persons and identifying them by name or by other means – for instance by giving their telephone numbers or information regarding their working conditions and hobbies – constitutes the processing of personal data wholly or partly by automatic means within the meaning of the Data Protection Directive.[137]

- Further, such processing of personal data is not covered by any of the exceptions in article 3(2) of the Data Protection Directive, as the exception in article 3(2) must be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people.[138]

The EU Data Protection Working Party has nevertheless argued that the 'purely personal or household activity' exemption may apply to users of SNS, provided that

136 Personuppgiftslag (SFS 1998:204).

137 Case C-101/01 *Bodil Lindqvist* ECLI:EU:C:2003:596 para [27].

138 Ibid, paras [47] and [48]. Bygrave considers this a sensible result, but nevertheless wishes that the court had given more guidance as to when a webpage with personal data will be sufficiently private in order to qualify for the household and personal use exemption (see Bygrave "Data privacy law" 259, 268.

the privacy settings allow the user to publish the personal data to self-selected contacts only. However, when an SNS allows access to profile information beyond self-selected contacts – for example, when access is provided to all members within the SNS, or if the personal data can be indexed by search engines – access goes beyond the personal or household sphere. Also, if an SNS user decides to extend access to his or her profile beyond self-selected 'friends', the SNS user can be regarded as a data controller. [139]

Another exclusion which may be relevant is article 9 which requires that the processing of personal information 'solely for journalistic purposes or the purpose of artistic or literary expression' should be exempted from certain provisions of a data protection Act adopted by a member state.[140] In those cases, the Working Party points out, a balance needs to be struck between freedom of expression and the right to privacy.[141] The two exemptions (for 'purely personal or household activity' and 'solely for journalistic purposes or the purpose of artistic or literary expression') are increasingly overlapping in situations where an SNS user 'publishes' personal data online.[142] The Working Party points out:

> It would be wrong to say that all of an individual's personal online activity is being done for the purposes of journalism or artistic or literary expression. However, the advent of 'citizen' bloggers and the use of social networking sites to carry out different forms of public expression, mean that the two exemptions have become conflated. The interaction between the two exemptions – and their scope - could have a significant impact on competing rights.[143]

It argues further that "an inappropriate level of scrutiny and regulation of natural persons' personal or household processing activities by DPAs could inhibit individuals' freedom of speech and could in itself constitute a breach of the

---

139 EU Art 29 DP WP Opinion 5/2009 on online social networking WP 6.

140 Member states must make provision for exemptions or derogations from the provisions relating to the lawfulness of processing, the rules relating to the transfer of data to third countries, and the provisions relating to the supervisory authority and the Working Party established by the Directive, if the exemptions are necessary in order to reconcile the right and privacy with the rules governing freedom of expression – Directive 95/46/EC art 9.

141 EU Art 29 DP WP Opinion 5/2009 on online social networking WP 6. Also see C-73/07 *Satamedia case* ECLI:EU:C:2008:727 discussed above.

142 See EU Art 29 DP WP Statement of the Working Party on current discussions regarding the data protection reform package Annex 2: Proposals for Amendments regarding exemption for personal or household activities (27 February 2013) 1.

143 Ibid.

individual's right to privacy."[144] It proposes that the exemption for 'exclusively personal or household purposes' should remain,[145] but that the law must provide far clearer guidelines to help DPAs to determine whether the processing falls within the scope of the exemption or not. The Working Party has suggested that a combination of certain factors could be used to determine whether or not a specific instance of processing falls within the scope of personal or household processing. These factors are: [146]

- Is the personal data disseminated to an indefinite number of persons, rather than to a limited community of friends, family members, or acquaintances?
- Is the personal data about individuals who have no personal or household relationship with the person posting it?
- Does the scale and frequency of the processing of personal data suggest professional or full-time activity?
- Is there evidence of a number of individuals acting together in a collective and organised manner?
- Is there the potential for adverse impact on individuals, including intrusion into their privacy?

Another case in which the CJEU had to interpret the purely personal or household-exemption concerned the use of CCTV cameras by a private household. A Czech citizen, Ryneš, installed a CCTV camera after his house had been vandalised on several occasions. The camera covered not only his property, but also a public footpath. After an incident of vandalism, two persons were identified from the CCTV footage and arrested. One of them questioned whether the use of CCTV footage was permissible under the Czech data protection law implementing the Directive. Ryneš argued that the exemption for purely personal and household use applied. The Czech Supreme Administrative Court, *Nejvyšší správní soud*, referred the

144 Ibid 2.
145 Regulation (EU) 2016/680, art 2(2)*(d)*.
146 EU Art 29 DP WP Statement of the Working Party on current discussions regarding the data protection reform package Annex 2: Proposals for Amendments regarding exemption for personal or household activities *(*27 February 2013) 4.

following question to the CJEU: "Does the operation of a camera system affixed to a family home for the purposes of protecting the property, health and life of the home owner constitute data processing 'by a natural person in the course of a purely personal or household activity' within the scope of Article 3(2) of Directive 95/46/EC albeit that this system also captures images of a public space?" The CJEU answered this question in the negative

> … the answer to the question referred is that the second indent of Article 3(2) of Directive 95/46 must be interpreted as meaning that the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision.[147]

It is clear that one should not interpret this exception too widely. If a public element is present, the processing is probably not being done for personal or household purposes.

*Data protections principles*

In terms of the Directive, personal data may only be processed if this is done fairly and lawfully.[148] This will be the case if the data complies with principles relating to data quality, and the data processing complies with certain criteria.[149]

*Data quality*. Data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes. They must also be: adequate, relevant and not excessive; accurate and, where necessary, kept up to date; not be stored for longer than is necessary; and then solely for the purposes for which they were collected. The responsibility for complying with these principles rests on the data controller.[150]

*Criteria for making data processing legitimate*. Personal data may be processed only if: the data subject has given his or her unambiguous consent; or processing is necessary for the performance of a contract to which the data subject is party; or processing is necessary for compliance with a legal obligation to which the controller

147 Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* ECLI:EU:C:2014:2428.
148 Directive 95/46/EC art 6(1).
149 Ibid arts 1 and 2.
150 Ibid art 6.

is subject; or processing is necessary to protect the vital interests of the data subject; or processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party; or processing is necessary for the purposes of a legitimate interest pursued by the controller or by the third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.[151]

Special categories of personal data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life) receive heightened protection. These data may be processed only in a limited set of circumstances. These are: where a data subject has given express consent; or processing is necessary for the controller to meet legal obligations with respect to employment law; or processing is necessary to protect the vital interests of a data subject (or another person), and the data subject is physically or legally incapable of giving consent; or processing is carried out by a non-profit organisation whose aim is to advance an agenda related to one of the categories of sensitive data; or the data are manifestly made public by the data subject; or processing is necessary to establish or defend legal claims; or is required by a health professional in the course of providing treatment or managing health-care services.[152]

In the *Bodil Lindqvist* case[153] referred to above, the CJEU interpreted the meaning of health data. It held that a reference to the fact that an individual has injured her foot and is on half-time on medical grounds, constitutes personal data concerning health within the meaning of article 8(1) of the Directive (ie sensitive personal information).[154] Discussing a friend's illness on Facebook could therefore be considered as processing sensitive information.

*Data subject rights*

The Directive requires that the data subject be informed of the data processing activities and their purpose, as well as of his or her right of access and right to rectify

151 Ibid art 7.
152 Ibid art 8(2).
153 Case C-101/01 *Bodil Lindqvist* ECLI:EU:C:2003:596.
154 Ibid para [51].

incorrect personal data.[155] Other rights afforded the data subject include the right to object to certain processing activities,[156] the right to object to processing of personal data for direct marketing,[157] and the right not to be subjected to automated individual decisions.[158] Exemptions and restrictions may be imposed on the data subject's rights for purposes of national security, defence, public security, the prosecution of criminal offences, an important economic or financial interest of a member state or of the EU, or the protection of the data subject.[159]

*Data controller obligations*

A data controller must notify the data protection authority before any processing activities take place.[160] The controller must also implement appropriate security measures to protect personal data. [161]

*Judicial remedies*

Every person has the right to a judicial remedy for any breach of the rights guaranteed by national law applicable to the processing in question.[162] In addition, any person who has suffered damage as a result of the unlawful processing of their personal data is entitled to receive compensation for the damage suffered.[163]

*Transfer of personal data to third countries*

Transfers of personal data from a member state to a third country may only take place if the third country offers an adequate level of data protection.[164] However, although transfers may not take place when an adequate level of protection is not guaranteed, there are a number of exceptions to this rule listed in the Directive, for example, if the data subject himself or herself agrees to the transfer, in the event of the conclusion of a contract, if it is necessary on public interest grounds, but also if

155 Directive 95/46/EC arts 10 and 11.
156 Ibid art 14(1).
157 Ibid art 14(2).
158 Ibid art 15.
159 Ibid art 13.
160 Ibid art 18.
161 Ibid art 17.
162 Ibid art 22.
163 Ibid art 23.
164 Directive 95/46/EC art 25.

binding corporate rules or standard contractual clauses have been authorised by the member state.[165]

In the *Bodil Lindqvist* case[166] the question was raised whether in the facts of that case, personal data had been transferred to a third country. The CJEU held that there will have been no transfer of personal data to a third country within the meaning of article 25 of the Data Protection Directive where an individual in a member state loads personal data onto an Internet page which is stored with his or her hosting provider which is established in that state or in another member state, thereby making those data accessible to anyone who connects to the Internet, including people in a third country. The court emphasised that the information was not being automatically sent from the server to other Internet users, and that there was no evidence that the information had actually been accessed from outside of Europe. The court pointed out that if article 25 were interpreted to mean that there is a transfer of data to a third country every time personal data are loaded onto an Internet page, that transfer would necessarily be a transfer to all the third countries with the technical means needed to access the Internet. The special regime provided for by the Directive would thus necessarily become a regime of general application as regards operations on the Internet. Therefore, if the Commission found, pursuant to article 25(4), that even one third country did not ensure adequate protection, the member states would be obliged to prevent any personal data from being placed on the Internet. Accordingly, it must be concluded that article 25 of Directive 95/46 is to be interpreted as meaning that operations such as those carried out by Lindqvist do not as such constitute a transfer of data to a third country.[167]

This aspect of the case was criticised by Poullet as being based on weak arguments. He argued that "[e]ven if the website is not as such exporting data, by his/her conscious operation, although he/she has deliberately created the risk of exportations by placing personal data on his/her website." He argues that articles 25 and 26 are applicable to the situation in *Lindqvist*.[168]

---

165 Ibid art 26.

166 Case C-101/01 *Bodil Lindqvist* ECLI:EU:C:2003:596.

167 Ibid paras [69] - [70].

168 Poullet "Transborder Data Flows and extraterritoriality: The European Position" 5 available at www.europarl.europa.eu/meetdocs/2004_2009/.../dv/..._/poullet_en.pdf (date of use:10 March 2016).

Kuner also argues that some of the court's reasoning can be faulted, for example, whether or not the data were actually accessed, should be irrelevant. The key question should be whether the data could have been accessed. He argues:[169]

> Failing to consider as data transfers situations when data were not being automatically transmitted to other countries seems untenable, given that the intention to make data available to other countries may exist just as much when they are merely made accessible as when they are actively transmitted, and that technological advancements will probably blur the distinction to a point where it can no longer be maintained.

Kuner nevertheless praises the court for its willingness to consider the international implications of its ruling, and its decision not to apply the EU restrictions on international data transfers "past a point of reasonableness".[170] According to Kuner, there continues to be a lack of clarity regarding the definition of 'data transfer', particular with regard to a situation where individuals post their personal data on an Internet site. (This would, of course, also be the situation in the case of a social network service.) He points out that the question of whether a data transfer has taken place, is sometimes another way of asking whether the data protection law of a particular country is applicable to the processing. He argues that while data controllers should not be able to evade their responsibilities by claiming that no transfer has taken place, not every interaction of an individual with a website should be regarded as a data transfer. Kuner concludes that the definition of a data transfer depends on the facts of a particular case.[171]

He argues that in practice, the likelihood that a finding will be made that a data transfer has taken place, is higher in the following circumstances: [172]

- Where the data controller has an establishment in the country of the individual whose data are processed.
- When the controller in some way targeted the individual.
- When the controller has some degree of control over the means used by the individual to process data.

169 Kuner *Transboder Data Flows and Data Privacy Law* 13.
170 Ibid.
171 Ibid.
172 Ibid 14.

On the other hand, it is less likely that it will be found that a data transfer has taken place in the following situations:[173]

- The individual has initiated contact with the controller without being targeted by the controller.
- When the controller does not have any operations in the in the individual's country.
- When the controller does not have control over the purpose to be served or means which the individual uses to process the data.

It is evident that in the case of social network services, where the majority of the SNSs and their servers are located in the USA, personal data are transferred across borders when these services are used outside of the USA.

It should perhaps be mentioned that the Directive does have an 'applicable law' provision, providing which national law is applicable to a particular processing activity. This provision is based on territoriality: the national law of the country where the data controller is present applies. If the data controller is not situated in a country but is making use of equipment in a particular country, the national law will apply.[174]

Kuner argues that in many instances trans-border data flow regulations serve the same function as rules on applicable law. When data is transferred from Europe to third countries, EU standards of data protection are applied to the transfer as well as to any further transfers that may take place.[175]

According to the EU Working Party on data protection, the combined effect of the applicable law provisions of the Directive (establishment of the data controller in the territory of the EU, or the use of equipment in the EU) has the result that the Directive is applicable to SNS providers even if their headquarters are located outside of the EU.[176]

---

173 Ibid.

174 Directive 95/46/EC art 4(1)*(a) & (c)*.

175 Kuner *Transboder Data Flows and Data Privacy Law* 125.

176 See EU Art 29 DP WP Opinion 5/2009 on online social networking WP 5 and Opinion 1/2008 on data protection issues related to search engines WP 8.

(b) e-Privacy Directive[177]

The Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (e-Privacy Directive) was adopted in 2002[178] and amended in 2009.[179] The e-Privacy Directive replaced the 1997 Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector,[180] in order to adapt Community legislation to developments on the Internet, and thus to "provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technology used".[181] The e-Privacy Directive is intended to particularise and complement the Data Protection Directive.[182] This Directive aims to harmonise the provisions of the member states required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communications sector, and to ensure the free movement of such data and of electronic communication equipment and services in the community.[183] The e-Privacy Directive also extends its protection to juristic persons.[184]

The e-Privacy Directive applies to the processing of personal data in connection with the provision of publicly available electronic communication services in public communication networks in the EU.[185] It lays down the rules applicable to the processing by network and service providers of traffic[186] and location data[187]

177 Directive 2002/58/EC.

178 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector *Official Journal* L 201/37.

179 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services; Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws *Official Journal* L 337/11.

180 Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Private Life in the Telecommunications Sector *Official Journal* L 24/1.

181 Tzanou "Data Protection" 279.

182 Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector 2002/58/EC art 1(2).

183 Ibid art 1(1).

184 Ibid art 1(2); also see Recital 12. The 1995 Data Protection Directive only protects natural persons.

185 Ibid art 3.

186 Ibid art 2(b) 'traffic data' means "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof".

generated by using electronic communication services. Such data must be erased or made anonymous when no longer needed for the transmission of a communication. Traffic data that are necessary for billing or interconnection payment may be processed up to the end of the period during which the bill may lawfully be challenged or payment pursued. Traffic data may be processed for marketing purposes and the provision of value added services, if the subscriber or user to whom the data relate has given his or her consent.[188]

The e-Privacy Directive regulates unsolicited electronic communications ('spam'). Such communications are only allowed if the person addressed has given prior consent to receive the communications (ie has opted in).[189] If the person is an existing customer, the company of which he or she is a customer may send him or her electronic offers of similar products or services, unless the subscriber has opted out of receiving such communications.[190]

The Directive (as amended in 2009) also deals with the use of cookies. It requires that websites must obtain informed consent from visitors before they store information on a computer or any web-connected device.[191] It is mostly by using cookies that information is stored by a website on the hard drive of a user's computer. Cookies are used for tracking visitors to a site. For cookies that are deemed to be "strictly necessary for the delivery of a service requested by the user" the consent of the user is not required.[192] An example of a 'strictly necessary' cookie is one that is used to complete a transaction when a user has placed an order ('add

---

187 Ibid art 2(c) 'location data' means "any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service".

188 Ibid art 5 (confidentiality of communications), art 6 (traffic data), and art 9 (location data other than traffic data).

189 Ibid, art 13(1) provides:

> The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.

190 Ibid art 13(2).

191 Article 5(3) (as amended by Directive 2009/136/EC). Directive 2009/136/EC is sometimes referred to as the Cookie Directive. The EU Data Protection Working Party has issued guidance on the obtaining of consent for the use of cookies – see Working Document 02/2013 providing guidance on obtaining consent for cookies WP 208 (2013).

192 Article 5(3).

to basket' or 'continue to checkout') when shopping online. The browser uses the information in the cookie to complete a successful transaction.[193]

Social network sites such as Facebook uses cookies for various purposes, including authentication of users, to support security features, to make advertising more personal, to localise the user, and for analytics and research.[194]

(c) Proposals for reform

On 12 January 2012, the Vice-President of the European Commission announced proposals to reform the Data Protection Directive in order to strengthen online privacy rights and boost Europe's digital economy. At the time of the adoption of the Data Protection Directive, the Internet was still in its infancy.[195] One of the objectives of the proposals is to deal with many of the challenges raised by SNS.[196]

Although the current framework for data protection in the EU is sound as far as its objectives and principles are concerned, it is not implemented in a consistent manner in all the EU member states. Reform of the EU Data Protection Directive is therefore necessary in order to ensure a more coherent implementation in the different member states. The proposal is therefore that the new data protection regime will be implemented as a Regulation that will have direct application in all the member states.[197]

The proposed Regulation is more detailed and stricter than the Directive. Some of the old data subject rights are strengthened, and some new rights are introduced. It introduces a 'right to be forgotten' by strengthening the data subjects' right to request the deletion of personal data. Another new right is that of 'data portability'. New

193 See Roos "Data privacy law" 402.

194 See Facebook Help Center "Cookies, Pixels & similar technologies" available at https://www.facebook.com/help/cookies/ (date of use: 20 December 2016).

195 See Hustinx "The reform of EU data protection" 65-6, explaining the 'drivers' of the EU review.

196 *Social Media and the Law: A Handbook for UK Companies* 18 available at http://www.linklaters.com/Insights/Social-media-law-A-handbook-UKcompanies (date of use: 20 December 2016).

197 See Blume "Will it be a better world? The proposed EU Data Protection Regulation" 2012 *IDPL* 130; "The myths pertaining to the proposed General Data Protection Regulation" 2014 *IDPL* 269; Mantelero "Competitive value of data protection: The impact of data protection regulation on online behaviour" 2013 *IDPL* 229. For a discussion of the key elements of the proposals, see Reding "The European data protection framework for the twenty-first century" 2012 *IDPL* 119.

restrictions are imposed on the processing of data of children under the age of thirteen years. Under the proposals, data controllers have to carry out a data protection impact assessment where processing operations present specific risks to the rights and freedoms of data subjects. A breach notification duty is imposed on data controllers, and stronger sanctions are proposed. It is no longer required of data controllers to notify the data protection authority of any processing activity before it takes place. Instead, new obligations to document data processing activities and to appoint internal data protection officers are introduced. The article 29 Working Party is replaced by a European Data Protection Board with a broader mandate. The provisions regarding the transfer of personal data across borders, has been widened to include not only third countries, but also international organisations, territories, and processing sectors within the third country.[198]

The Regulation has been adopted and will come into effect as from 6 May 2018.[199]

## 5.4 UNITED KINGDOM[200]

### 5.4.1 Introduction

The United Kingdom (UK) is a union of previously independent countries: England, Wales, Scotland, and Northern Ireland.[201] The UK has three different legal systems. England and Wales have a unified legal system and follow English law (also known

198 See Roos "Data privacy law" 401.

199 Regulation (EU) 2016/680 art 59 (1).

200 On 23 June 2016 the United Kingdom held a referendum to decide whether it should leave or remain within the European Union (European Union Referendum Act of 2015). Fifty-two per cent voted to leave the European Union. Article 50 of the Treaty of European Union consolidated version of 2012, provides that:

> 1. Any Member State may decide to withdraw from the Union in accordance with its own constitutional requirements.
>
> 3. The Treaties shall cease to apply to the State in question from the date of entry into force of the withdrawal agreement or, failing that, two years after the notification referred to in paragraph 2, unless the European Council, in agreement with the Member State concerned, unanimously decides to extend this period.

European Union law still applies in the United Kingdom, since the United Kingdom has yet to act in terms of art 50.

201 Lloyd *Cyber Law in the United Kingdom* 13.

as common law).[202] Northern Ireland applies Northern Ireland law, which is similar to English law. The Scottish legal system is a mix of civil law and common law. The Supreme Court of the United Kingdom is the final court of appeal in the UK for civil cases, and for criminal cases from England, Wales and Northern Ireland.[203] It also hears cases of the greatest public or constitutional importance affecting the whole population.[204]

### 5.4.2 Recognition and development of the right to privacy in English law

In English law, protection of privacy can be found to some extent in constitutional law, tort law, and statutory law.

The UK does not have a written constitution. Statute law, case law, and constitutional conventions are the sources of its constitutional law. The UK is currently a signatory to the ECHR which protects the right to private life in article 8.[205] The UK adopted the Human Rights Act 1998 to implement the ECHR in UK law. It is especially the introduction of the Human Rights Act that has influenced the recognition and protection of the right to privacy in English law.

Traditionally, English common law did not recognise a general right to privacy.[206] Under the influence of the Human Rights Act, the action for the protection of privacy has developed under the guise of two equitable wrongs, namely breach of confidence, and misuse of private information. The law of confidence has evolved immensely within the commercial sphere where it is used to protect trade secrets and business information from rivals.[207] It has also developed to include other situations which are not business-orientated, but relate to personal information or to matters of public concern.[208]

---

202 See www.supremecourt.uk.
203 Ibid.
204 Ibid.
205 See para 5.3.3.1.
206 Burchell *Personality Rights* 369; also see Collingwood 2012 *Computer Law & Security Review* 328.
207 Warby, Moreham & Christie *Privacy and the Media* 165.
208 Fridman *Fridman on Torts* 528.

*5.4.2.1 Constitutional law: Human Rights Act 1998*

Before the enactment of the Human Rights Act, the ECHR had not been incorporated into United Kingdom law and as a result it could not be invoked before the UK courts. Furthermore, the UK did not initially accept individual petition to the European Court of Human Rights (ECtHR). In 1966 the UK government changed its position on the question of individual petition and since that date individuals who claim that their rights under the ECHR have been violated by the UK government have been able, once they have exhausted their domestic remedies, to take their case to the ECtHR in Strasbourg.[209]

The provisions of the ECHR have been implemented in the UK through the adoption of the Human Rights Act 1998 which came into force in 2000. The Act gives effect to the rights and freedoms guaranteed under the ECHR.[210] The Act declares that the Convention rights "are to have effect for the purposes of this Act subject to any designated derogation or reservation".[211] English courts must take decisions of the ECtHR into account when determining cases involving a Convention right.[212] Legislation should also be interpreted as far as possible in a way that will be compatible with the Convention rights.[213]

The ECHR protects privacy in articles 8(1) and 8(2). These two articles are incorporated in the Human Rights Act of 1998.[214] They guarantee that individuals have the right to respect for their private and family lives, their homes, and their correspondence.[215] Public authorities may not interfere with the exercise of these rights, except where this is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic

209 UK Equality and Human Rights Commission "The UK and the European Court of Human Rights" Research Report 83 (2012) v-vi.
210 Human Rights Act, 1998, Preamble.
211 Ibid s 1.
212 Ibid s 2.
213 Ibid s 3.
214 Ibid Sch 1 part 1 art 8(1) and (2).
215 Ibid art 8(1).

well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[216]

It is notable that article 8(1) specifically guarantees protection for four aspects of an individual: private life, family life, home, and correspondence.[217] 'Private life' includes bodily integrity, personal autonomy, personal information, personal identity, and not being subjected to surveillance.[218] Though some of these concepts are not mentioned in the article itself, they have developed through case law.[219]

The right protected by article 8(1) is not an absolute right. Article 8(2) provides an internal limitation: interference is allowed where it is in accordance with the law,[220] is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. An infringement may be justified where the other party exercises his or her right to freedom of expression in terms of article 10 of the ECHR.[221]

In terms of article 8(2) of the Human Rights Act, the interference that is prohibited is between the citizens and the state. This is similar to the approach in the ECHR. Thus, this provision has vertical application; as a result this may arguably not cure the *lacuna* of a lack of a privacy tort between citizens in an horizontal application.

However, since article 8 imposes a positive obligation on the state to respect and promote the interests of private and family life, it has been held in case law that the

---

216 Ibid art 8(2).

217 Ibid art 8(1).

218 Bowen "*Article 8 and 'private life': The protean right"* 6-7.

219 UK Equality and Human Rights Commission Research Report 83 "The UK and the European Court of Human Rights" (2012) 261. Also see echr-online.info art 8.

220 The Regulation of Investigatory Powers Act, 2000, for example, allows interception of telephone calls by appropriate authorities with an interception warrant.

221 Human Rights Act 1998 art 10: Freedom of Expression

1. Everyone has the right of freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality or the judiciary.

individual is entitled to complain to the state about breaches of his or her private life committed by other individuals.[222] Bowen points out that: "Article 8 … also imposes positive obligations on States to take measures to protect individuals from the actions of non-State actors …". These measures include "… establish[ing] an effective independent judicial system so that responsibility for conduct infringing Convention rights may be determined and those responsible made accountable". [223]

*5.4.2.2 Common law: Breach of confidence and misuse of private information*

In common law private information has, in certain circumstances, received protection from disclosure under the claim for breach of confidence. In order to establish breach of confidence, the plaintiff must establish that the information was confidential, that is, the information had been disclosed in circumstances that implied an obligation of confidentiality.[224] This action was subject to three limiting principles.[225]

- "The principle of confidentiality only applies to information to the extent that it is confidential. Once it has entered the public domain, in the sense that the information in question is so generally accessible that, in all the circumstances, it cannot be regarded as confidential, then the principle of confidentiality can have no application to it.
- The duty of confidence applies neither to useless information, nor to trivia.
- Although the basis of the law's protection of confidence is that there is a public interest that confidences should be preserved and protected by the law, nevertheless that public interest may be outweighed by some other countervailing public interest which favours disclosure. This limiting principle may require a court to carry out a balancing operation, weighing the public interest in maintaining confidence against a countervailing public interest favouring disclosure".

222 See *McKennit v Ash* [2006] EWCA Civ 1714 para [9]; *Campbell v MGN Limited* [2004] UKHL 22 paras [17] and [18].

223 Bowen "*Article 8 and 'private life': The protean right"* 5.

224 See *Prince Albert v Strange* (1849) ER 1171; *Duchess of Argyll v Duke of Argyll* 1967 Ch 302; *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804.

225 *Attorney General v The Observer Ltd* [1990] 1 AC 109, 282.

In *Campbell v MGN Ltd*,[226] the *Daily Mirror* newspaper had published a series of stories about a famous model, Naomi Campbell. These stories related to her attending Narcotics Anonymous (this was accompanied by a photograph of her leaving a place where Narcotics Anonymous held meetings), including details of her undergoing treatment for drug addiction. The claimant had previously publicly denied her drug addiction. She admitted during trial that this had been a lie. The *Daily Mirror* claimed that it had acted in the public interests to correct her public denial. Campbell admitted that there was a public interest justifying publication of the fact that she was a drug addict and was undergoing therapy, but claimed damages for breach of confidentiality, and compensation under the Data Protection Act, 1998, (DPA) for the publication of additional details. Morland J awarded damages to the claimant in the court *a quo*. This is after the court had found the defendant to have committed a breach of confidence and breach of the DPA. This decision was overturned by the Court of Appeal which reasoned that the claimant's celebrity status made the details of her attending Narcotics Anonymous 'newsworthy'. This decision was reversed by the House of Lords.

The House of Lords pointed out that the action for breach of confidence has been developed under the influence of human rights instruments and decisions of the ECtHR, to embrace private, in addition to confidential, information.[227] The values enshrined by articles 8 and 10 of the ECHR have become part of the cause of action for breach of confidence.[228] Under influence of these instruments, it was accepted that the privacy of personal information was worthy of protection. [229]

Another factor that influenced this development was an acknowledgement of the artificiality of distinguishing between confidential information obtained through a violation of a confidential relationship, and similar information obtained some other way. [230]

---

226 *Campbell v MGN Limited* [2004] UKHL 22 para [2].
227 Ibid paras [16] and [17].
228 Ibid.
229 Ibid para [46].
230 Ibid.

The development resulted in the law dispensing with the requirement that there should be a pre-existing relationship of confidence. The law now imposes a duty of confidence whenever a person receives information in circumstances in which he or she knows, or should know, that it is fair and reasonable to regard the information as confidential. The action has been developed to protect information in respect of which there is a reasonable expectation of privacy. This action is sometimes referred to as 'misuse of private information'.[231]

However, officially the cause of action remains 'breach of confidence'. It has been pointed out that:[232]

> In its present form breach of confidence thus embraces two differing forms of protection:
> - old-fashioned breach of confidence which upholds confidential relationships and the duty of good faith; and
> - misuse of private information (the new element to this cause of action) which upholds human autonomy and dignity in respect of private information regardless of whether a breach of confidence is involved.

In order to determine whether information is private, the Court of Appeal in *Douglas v Hello! Ltd* asked:[233]

> What is the nature of 'private information'? It seems to us that it must include information that is personal to the person who possesses it and that he does not intend shall be imparted to the general public. The nature of the information, or the form in which it is kept, may suffice to make it plain that the information satisfies these criteria.

In other words, if a person determines that personal information should not be disclosed to other persons, such information should be considered private information.

#### *5.4.2.3 Legislation: Data Protection Act, 1998*

The Data Protection Act, 1998, came into force in 2000. It repealed the former Data Protection Act, 1984. The provisions of the Human Rights Act and those of the

231 Deacon, Lipton & Pinker *Privacy and Personality Rights* 151-2.
232 Ibid 174-5.
233 [2006] QB 125 para [83].

ECHR created a legal framework for the development and adoption of the Data Protection Act.[234] The Data Protection Act gives effect to the Data Protection Directive.[235] The Freedom of Information Act[236] amended the Data Protection Act, 1998.[237] The Freedom of Information Act makes provision for the disclosure of information held by public authorities or by persons providing service to them.[238]

The Data Protection Act creates a framework which deals with the protection of personal data.[239] The Act does not apply specifically to a person or an organisation, but to any activities involving the 'processing' of personal data in the United Kingdom, or processing where equipment situated in the United Kingdom is used for the processing of personal data.[240] Section 1 defines a 'data controller' to mean, "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".[241]

The Act sets out eight data protection principles which must be complied with whenever there is 'processing' of personal data.[242] These principles are:

> 1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
>
> (a) at least one of the conditions in Schedule 2 is met, and
>
> (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
>
> 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
>
> 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

---

234 Act of 1998.

235 Directive 95/46/EC.

236 Act of 2000.

237 Ibid s 73.

238 Ibid s 1.

239 Information Commissioner's Office *Guide to Data Protection* 2010.

240 Data Protection Act, 1998, s 5 which explains the application of the Act. Also see s 1 which defines 'processing'. It states that 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 or the information or data.

241 Ibid.

242 Data Protection Act 1998 Sch 1.

4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. 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.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The DPA also creates the office of the Information Commissioner, who is the custodian of the DPA. This is an independent authority which has a duty to protect the privacy of personal data and a responsibility to ensure access to information.[243] The Information Commissioner may also give clarity on the interpretation of the provisions of the DPA.[244] However, the Information Commissioner's interpretation of the DPA only has a persuasive effect; conclusive interpretation of the DPA rests with the courts.[245]

*Data Protection Act and SNSs*

The posting of personal information on a SNSs amounts to processing of personal data and must therefore comply with the Data Protection Act. In the context of SNSs, the Social Networking Providers and users' of SNSs are data controllers as per the definition in the Data Protection Act, in that they "determine the purposes and means of the processing of personal data", as they provide the Social Networking platform.

The question arises whether individual users of the SNSs are also data controllers when they upload personal information about themselves or third parties on their individual webpages. The Data Protection Act exempts certain forms of data

243 Information Commissioner's Office *Guide to Data Protection* 2010. Also see Freedom of Information Act 2000. The information Commissioner has the following duties: promoting good practice in handling personal data, and giving advice and guidance on data protection; keeping a register of organisations that are required to notify him about their information-processing activities; helping to resolve disputes by deciding whether it is likely or unlikely that an organisation has complied with the Act when processing personal data; taking action to enforce compliance with the Act where appropriate; and bringing prosecutions for offences committed under the Act.

244 Ibid.

245 Ibid.

processing from the provisions of the Act. One such exemption, relevant to the current discussion, is the domestic purpose exemption found is section 36. In terms of this section an individual who processes personal data solely for personal, family, or household affairs (including recreational purposes) are exempt from the data protection principles and the provisions of Parts II (Rights of Data subjects and others) and III (Notification by Data Controllers). This exemption does not apply where the website operator processes personal data for 'non-domestic purposes', for example, where an individual uses a SNS website for running a sole-trader business – in other words for corporate or business purposes. In such a case the normal Data Protection Act rules will apply to the individual user, and he or she will be treated as a 'data controller'.

However, there is no clear guidance for the case where an individual user uses his or her profile for mixed purposes, that is, for domestic and non-domestic purposes. This is probably because, as Garrie et al[246] assert, the Data Protection Directive, which has been implemented in the United Kingdom through the Data Protection Act, was drafted long before the Web 2.0 era, and therefore did not consider issues surrounding social networking. The Information Commissioner's Office advises that in such a situation the individual will either have to comply with the Data Protection Act whenever he or she uses his or her profile for non-domestic purpose, or alternatively register a separate profile. The domestic purpose exemption does not cover organisations that use SNSs or online forums; the organisation, therefore, must comply with the Data Protection Act in the normal way. Examples would be if the organisation:

- posts personal data on their own or a third party website;
- downloads and uses personal data from a third party website; or
- runs a website which allows third parties to add comments or posts about living individuals, and they are the data controller for website content.

246 Garrie et al 2010 *Int'l L & Mgmt Rev* 128.

### 5.4.3 Practical issues when applying data protection rules in the SNSs environment

Here I address the question of liability once an infringement of a personality right (such as privacy or identity) has occurred on an SNSs. I consider the position in the UK specifically. I also discuss the position of a UK Internet Service Provider (ISP) where the identity of the user is unknown to the plaintiff, either because the user is anonymous, or is using a pseudonym.

#### *5.4.3.1 Procedural challenges: Wrongdoer and anonymity*

A person, whose personality rights have been infringed in the context of an SNS, may bring a claim in a court against the wrongdoer if the identity of the wrongdoer is known to the claimant. However, if the identity of the wrongdoer is known only to the Social Network Provider – for example, where the claimant is posing as someone else or using a pseudonym – the positions is more complicated. In such an instance it is possible in the UK to seek a special disclosure order – the so-called *Norwich Pharmacal Order*[247] – against the Social Networking Provider. A *Norwich Pharmacal Order* is a court order that requires a third party who is (innocently or not) involved or 'mixed up' in the wrongdoing, to disclose documents or information, such as the identity of the wrongdoer.[248] The purpose of the order is to enable a prospective claimant to obtain the necessary information, such as the name of the proper defendant, before instituting legal action.[249] It is an equitable remedy and it is in the discretion of the court whether to grant it or not.[250]

Collingwood[251] notes that disclosure orders may facilitate the identification of a wrongdoer, who may then ultimately be pursued through the courts, but they should not be taken lightly, particularly because revealing the details of an individual

247 The order is named after the case in which such an order was first issued: *Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] AC 133.

248 The order will not be given against someone who is a mere witness in the case – see *Harrington v Polytechnic of North London* [1984] 1 WLR 1293 and *Ashworth Hospital Authority v MGN Ltd* [2002] UKHL 29; [2002] 1 WLR 2033.

249 See Van der Merwe *ICT Law* 529.

250 *Totalise plc v The Motley Fool* [2001] EWCA Civ 1897.

251 Collingwood 2012 *EJLT* 6.

expecting to rely on the protection of anonymity, clearly involve major data protection issues given their intrusive nature.

In *Applause Store Productions Ltd and Firsht v Grant Raphael,*[252] Mathew Firsht and his company, Applause Store, successfully sued for libel and misuse of private information. The defendant allegedly created a false Facebook profile in the name of Mathew Firsht and linked a false Facebook group (titled 'Has Mathew Firsht Lied To You?') to the profile. The fake profile and Group page alleged that the Matthew Firsht was gay, owed business associates money, and had lied about paying it back. In other words, it contained private information and was also defamatory of the plaintiff. The claimant obtained a *Norwich Pharmacal* order against Facebook for disclosure of the registration data provided by the user responsible for creating the false material, including the e-mail addresses and IP addresses of all computers used to access Facebook by the owner of those e-mail addresses.[253] Facebook provided the claimant with evidence showing that the profile was created on a computer using an IP address that matched the defendant's computer. The court found in favour of the plaintiff.

Sometimes it may be difficult to identify the author of harmful content because the perpetrators have used anonymous profiles or public computers to perpetrate their wrongful acts.

In the case of *The author of a Blog v Times Newspapers Ltd,*[254] the court had to determine whether the claimant had a reasonable expectation of privacy in that his identity would not be revealed to the general public by the *Times Newspaper*, even though the Newspaper had deduced his identity by legal means. The blogger argued that he had a reasonable expectation of privacy in respect of his identity as the anonymous author of the blog, and that there was no countervailing public interest justifying its publication. The court held against the blogger because the information did not have the necessary quality of confidence required, nor did the blogger have a reasonable expectation of privacy since blogging is a public activity.

252 [2008] EWHC 1781.
253 Ibid para [10].
254 [2009] EWHC 1358 QB.

In conclusion, one can say that in the right circumstances it is possible to force a UK Internet Service Provider to disclose the identity of an anonymous third party who has infringed the privacy of a claimant.

*5.4.3.2 ISP liability*

Savin[255] highlights three essential roles of the ISP: first, they enable the flow of information between the users without contributing to the content; second, they act as guardians of the users' identity and anonymity; and thirdly, they are in a unique position to prevent or mitigate the damage that may be inflicted by other users' activities.

Under the repealed Defamation Act[256] an ISP was liable for defamatory third-party content if it knew, or should have known, of the defamatory content when the service provider published it. It is not clear whether the service provider could be liable for breach of privacy or identity under the Defamation Act. However, it is arguable that the rules applied under the Defamation Act may also be applied in the case of an infringement of privacy or identity in the context of SNSs.

The Defamation Act, 2013, came into force on 1 January 2014. Its introduction brought significant changes with regard to the liability of website operators. It introduced a defence to shield website operators from damage claims resulting from publication of defamatory user-generated content.

Section 5 provides a defence for a website operator if an action for defamation is brought against the operator in respect of a defamatory statement posted on the website.[257] The defence is applicable if a website operator can show that it did not post the defamatory statement on the website.[258] The website would not be successful in the defence if the claimant shows that:

(a) it was not possible for the claimant to identify the person who posted the statement;

255 Savin *EU Internet Law* 104.
256 Act of 1998 s 1.
257 Defamation Act of 2013 s 5(1).
258 Ibid s 5(2).

(b) the claimant gave the operator a notice of complaint in relation to the statement; and

(c) the operator failed to respond to the notice of complaint in accordance with any provision contained in regulations.[259]

If the same principles could be applied in respect of postings infringing on privacy and identity, the ISP would escape liability if it could show that it was not responsible for posting the information, and was not informed by the plaintiff of the infringement.

## 5.12 SUMMARY

In this chapter I examined a selection of the most important international documents which have influenced national laws on the protection of personality rights (such as the right to privacy and the right to identity). I focused on the protection of the rights to privacy and identity both as human rights and in private law (tort law or the law of delict) within the EU, and more specifically the UK as a member state. The focus was on the legislation of the EU and how it has been transposed and applied within the UK. I also considered how these laws have been adapted as a result of the development of new technologies (particularly the Internet).

[259] Ibid s 5(3)*(a)-(c)*.

# Chapter 6

# Summary, conclusions and recommendations

## 6.1 SUMMARY

This chapter provides a conclusion to this study. It gives a brief summary of the study, some conclusions, and then recommendations.

In the study I sought to investigate whether South African law adequately protects the interests that form the object of the right to privacy and the right to identity, particularly in the context of SNSs. Other related questions investigated included: who should be held responsible for the user-generated content uploaded on SNSs; the role of the ISP; and how anonymous defendants should be dealt with. A comparative law approach was adopted to conduct the investigation.[1]

The focal point of the study was the use of SNSs and certain personality rights (namely, the right to privacy and the right to identity) that may be infringed by the use of SNSs. I argued that these two rights are affected when users share or communicate information, about either themselves or others, on SNSs.[2] I showed how the right to privacy and right to identity may overlap[3] which is why these two personality rights were discussed together.

In order to contextualise the study, the following assumptions were adopted: that the Internet is an important medium of communication; that people retain their personality rights when using the Internet (and specifically SNSs); and that the law must protect people's rights when they use SNSs. The research was limited to the protection of the right to privacy and right to identity in the context of SNSs and the delictual perspective was my focus. I further limited the study to the personality rights of natural persons.

1 Paragraph 1.3; Chs 4 and 5 above.
2 Paragraph 3.1 above.
3 Paragraph 3.6; also see para 3.3.1 above.

In order to provide a background, in Chapter 2 I dealt with the concept of SNSs and explained their functionality. This provided an historical background to the development of SNSs; the nature of SNSs was explained; and a description was given of SNSs in general. I also examined the use of SNSs and described the functionality and usage of specific SNSs.

Furthermore, in the study I investigated two personality rights (particularly the right to privacy and right to identity). In Chapter 3 I turned my attention to the South African position. I first considered the common law and the constitutional law position as regards the recognition and development of these personality rights, together with how they may be infringed. The possible grounds of justification that exclude the wrongfulness of infringing conduct were also examined.[4] I explored the infringement of these personality rights in the context of SNSs and the possible grounds of justification applicable in this regard and also addressed the procedural challenges where either privacy or identity has been infringed in the context of SNSs. Here I addressed the possible remedies available to a plaintiff whose personality rights have been infringed through the use of an SNS. I also highlighted that the rights to privacy and identity may be interlinked with data protection which means that data protection becomes relevant when there is processing of personal information on SNSs.[5] This discussion focused on the POPI Act in order to address the processing of personal information in the context of SNSs.[6] I indicated that the POPI Act excludes any processing of personal information during the course of a purely personal or household activity from its sphere of application. I concluded that it is not clear how this exception may apply in the context of SNSs.[7]

For a comparative law perspective, I looked first at the legal system of the United States of America in Chapter 4 and highlighted the recognition, protection, and regulation of the rights to privacy identity in the United States at federal level. I here considered constitutional law, legislation, common law, and case law as sources of the rights I analysed. The common law played an important role with regard to the

4 Paragraph 3.2 above.
5 Paragraph 1.1 above.
6 Paragraph 3.7.3 above.
7 Paragraph 3.7.3.1 above.

recognition and the protection of the right to privacy.[8] The right to identity does not exist as an independent personality right; it is protected under the guise of the right to privacy,[9] and under the right of publicity.[10] From the discussion, it emerged that although the United States Federal Constitution (Bill of Rights) does not protect privacy explicitly by name, the right to privacy is recognised and protected under the United States Constitution as a result of judicial interpretation.[11] The right to privacy is also protected in terms of legislation; I indicated that the Congress often enacts a pieces of legislation to address an imminent threat to privacy. As a result, there is a plethora of legislation addressing privacy and focussing on different areas, such as law enforcement and government records, data security, consumer data, medical and genetic data, and employment.[12] I further focused on legislation relevant in the context of SNSs.[13] I also examined the position with regard to the transfer of personal data between the United States and the European Union and focused on the Safe Harbour Agreement, the implications of the *Schrems v Data Protection Commissioner*[14] decision on the Safe Harbour Agreement,[15] and the newly enacted EU-US Privacy Shield.[16]

In Chapter 5 I continued with a comparative study, here examining a selection of the most important international instruments which have influenced national laws dealing with the protection of personality rights (such as the rights to privacy and identity). This discussion was necessary as the Internet and SNSs operate on an international platform which allows trans-border communication and processing of personal information. In this context, I considered international documents establishing or issued under the auspices of the following organisations: the UN, AU, the OECD, the Council of Europe, and the EU. South Africa is a member state of the AU,[17] UN,[18] and the OECD.[19] The discussion briefly looked at the Council of Europe, a structure responsible for political cooperation between the democratic European countries,

8 Paragraph 4.3.1.1 above.
9 Paragraph 4.3.1.2 above.
10 Paragraph 4.3.2.2 above.
11 Paragraph 4.3.3.1 above.
12 Paragraph 4.3.4.1 above.
13 Paragraph 4.3.4.2 above.
14 EUCJ Case C-362/13, 6 October 2015.
15 Paragraph 4.3.4..3 above.
16 Paragraph 4.3.4.3 above.
17 Paragraph 5.2.2.1 above.
18 Paragraph 5.2.1.1 above.
19 Paragraph 5.2.3 above.

before I turned my focus to the EU. The recognition and development of the right to privacy and the right to identity at the level of EU Regulations, Directives and Decisions, particularly in the context of SNSs, were investigated. I pointed to the important role the EU has played and its immense influence on the development of data protection legislation. I also considered the proposed reform package of the European Commission – reform which seeks to modernise the rules on data protection in light of rapid technological developments and globalisation.[20]

In order to show how EU laws apply to member states, I next explored the legal position in the UK. Here I once again focused focussed on the protection of the right to privacy and identity in constitutional law, common law (tort law), and statutory law. I also discussed the applicability of the Data Protection Act of 1988 on SNSs users, the liability of ISPs, and the identification of anonymous users.

## 6.2 CONCLUSION

The study has noted how SNSs have brought convenience or improvement to the lives of its users.[21] The legal consequences of the use of SNSs have also been identified.[22] It can consequently be concluded that the law must evolve or adapt in line with new technological developments in order adequately to protect society's needs. SNSs provide an important platform for the free flow of information amongst users and third parties. The Internet is unique in that a conversation that occurs online leaves a digital footprint, in contrast to the physical or offline world where a conversation between two people will only be remembered for a short while by the parties involved, and no physical trace of it will remain. This does not mean that SNSs require unique laws or even new laws which differ from those which apply in the 'real' world. The existing rules could be adjusted or fine-tuned to make them effective in the context of SNSs.

---

20 Paragraph 5.3.3.2 above.
21 Chapter 2 above.
22 Paragraph 3.9 above.

On the basis of my discussion in Chapter 3,[23] I conclude that the South African common law (under the *actio iniuriarum*) provides adequate protection for the interests that form the object of the right to privacy and the right to identity when these interests are infringed in the SNSs context. Although SNSs could be considered a public space, the *boni mores* will nonetheless regard the user's claim to a right to privacy (and identity) reasonable if the SNS user used the privacy settings on SNSs in an appropriate manner, and did not accept an excessive number of 'friends'.

While the study focused on private law, the influence and importance of the Constitution on these concepts could not be ignored. The right to privacy and right to identity were considered under the Constitution.[24] In *NM v Smith (Freedom of Expression Institute as* Amicus Curiae*)*,[25] the Constitutional Court emphasised that "the precepts of the Constitution must inform the application of the common law." The legal rules forming the basis of the *actio iniuriarum* should be developed in a manner that "recognises both the importance of privacy and the importance of freedom of expression." [26] In my view, the user of an SNS has a reasonable expectation of privacy in the same circumstances under which the *boni mores* will accept the user's claim to a right to privacy as reasonable. I opine that the *actio iniuriarum* remains relevant and important in offering protection for infringement of privacy and identity in the context of SNSs.

Several pieces of legislation are also important in order to provide adequate protection for the interests that form the object of the right to privacy and the right to identity in the context of SNSs. These include: the Electronic Communications and Transactions Act,[27] the Promotion of Access to Information Act,[28] the Regulation of Interception of Communications and Provision of Communication Related Information Act,[29] the Protection from Harassment Act,[30] and the Protection of

---

23 Paragraphs 3.2.2.1; 3.2.3.1 & 3.3 above.
24 Paragraphs 3.1; 3.2.1.2; 3.2.2.2; 3.2.3.2 and 3.3.1 above.
25 2007 (5) SA 250 (CC) para 31.
26 Ibid para 47.
27 Act 25 of 2002; para(s) 3.9.9 and 3.10.2 above.
28 Act 2 of 2000; para 3.7.1 above.
29 Act 70 of 2002; para 3.7.2 above.
30 Act 17 of 2011; para 3.10.4 above.

Personal Information Act.[31] I conclude that the legislation that is currently in place is effective in regulating SNSs. Of course, as the technology advances, these laws might need to be fine-tuned.

In Chapter 3 I discussed the remedies at the disposal of users of SNSs. I concluded that apart from the *actio iniuriarum,* alternative remedies should be considered. A take-down notice under the ECT Act, for instance, offers an effective remedy of first instance for a person whose privacy or identity has been infringed, provided the ISP adheres to such take-down notice requests from users or non-users. If this type of remedy could successfully be used, it would help avoid the expensive process of litigation.[32] An interdict in the context of SNSs provides immediate and effective relief to the plaintiff (user or non-user) and minimises the harm to plaintiffs' (user or non-user) personality interests (privacy and identity in this instance).[33] A protection order under the Harassment Act offers another possible remedy which offers speedy legal relief in the context of SNSs which may assist in minimising further damage to the plaintiff's personality rights.[34]

From the comparative discussion, I drew certain conclusions, for example, that SNSs operate on an international platform which allows trans-border communication and processing of personal information. Also, the United States does not have comprehensive data protection legislation. I therefore concluded that the international documents on human rights and data protection which I discussed, contribute to the development of the international data protection legal framework and continue to influence data protection in the different jurisdictions that have yet to adopt data protection laws. It is notable that the EU data protection legislation and standards have a major influence in jurisdiction beyond Europe; in South Africa this influence culminated the promulgation of the Protection of Personal Information Act 4 of 2013.[35]

As to the question of liability of an ISP for third party content, I concluded that both the United States and the United Kingdom provide some form of immunity for the ISP. In the United States protection is provided under section 230 of the

31 Act 4 of 2013; para 3.7.3 above.
32 Paragraph 3.10.2 above.
33 Paragraph 3.10.3 above.
34 Paragraph 3.10.5 above.
35 Paragraphs 3.7.3; 5.3.3.2 above.

Communications Decency Act,[36] while in the United Kingdom protection is extended in terms of section 5 of the Defamation Act.[37]

The study posed a question regarding identifying an anonymous user as possible defendant. In this regard I concluded that both the United States and the United Kingdom have adopted procedures to assist the plaintiff, namely, the John Doe proceedings[38] and the *Norwich Pharmacal Order* proceedings respectively.[39]

## 6.3 RECOMMENDATIONS

I first offer some recommendations for users of SNSs. Users should take the following precautions when using SNSs.

- Users should acquaint themselves with the terms of use and the privacy policy of the relevant SNSs they wish to join. It is also important to check the terms of these policies regularly as SNSs may change them at any time.

- Users should set privacy settings to the maximum. Users must be conscious of the dangers when sharing personal information on SNSs. They should avoid uploading their and other people's sensitive personal information, and never divulge more personal information than is absolutely necessary on any SNS.

- Users should be selective in accepting friends – users who have hundreds of friends who have unlimited access to their private information, run the risk that their expectation of privacy will not be considered reasonable by the *boni mores*.

As far as the development of South African law is concerned, I offer the following recommendations.

---

36 Paragraph 4.5.1 above.
37 Paragraph 5.4.3.2 above.
38 Paragraph 4.5.2 above.
39 Paragraph 5.4.3.1 above.

- At present the common law protects the right to privacy and identity of SNSs users, but courts are encouraged to develop the common law when necessary to keep up with any future technological developments that may limit this protection.

- The newly formed Privacy Regulator should take note of new developments in the area of SNSs and make recommendations to the legislature about changes to the law as necessary. One area that will need her immediate attention is the applicability of the household exemption to the users of SNSs. This study recommends that the Information Regulator should provide some clarity or formulate guidelines to clarify the applicability of the household exemption to SNSs users. The proposals of the EU's article 29 Data Protection Working Party could be adopted in South Africa.[40] The following factors could be identified as indicative of a situation when the household exemption should not be available to SNSs users:
    - the personal information is disseminated to an indefinite number of persons, rather than to a limited community of friends, family members, or acquaintances;
    - the personal information relates to individuals who have no personal or household relationship with the person posting it;
    - the scale and frequency of the processing of personal information suggest professional or full-time activity;
    - there is evidence of a number of individuals acting together in a collective and organised manner;
    - there is a potential adverse impact on individuals, including intrusion into their privacy.

- With regard to the procedure for identifying an anonymous user as possible defendant, it is recommended that the position in United States and the United Kingdom be used to guide future developments in South Africa. I agree with Nel's proposals in this regard, namely that:[41]

40 Paragraph 5.3.3.2(a) above.
41 Nel 2007 *CILSA* 210 ff.

- the discovery procedure used to identify the anonymous user should be not be used as a 'fishing' expedition;
- the applicant should not have another alternative remedy available (for instance the applicant should have already applied for a take-down notice in terms of the ECT Act);
- the applicant cannot obtain discovery against one person for the purpose of bringing action against another person (this would mean an applicant cannot apply for discovery against 'friends' of the prospective defendant);
- the court should not come to the assistance of a litigant to identify an anonymous user in order to enable him to establish whether or not he has a cause of action;
- in any approach used to identify an anonymous defendant, it is important for the procedure to take into account the possible defendant's right to privacy, freedom of expression, and the provisions of the RICA Act.[42]

[42] Paragraph 3.7.2.2 above.

# Bibliography

## BOOKS, CHAPTERS IN BOOKS, AND THESES


Abdulrauf *Legal Protection of Data Privacy in Nigeria*

Abdulrauf LTA *Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* (LLD Thesis UP 2015)

Barendt "Privacy and Freedom of Speech"

Barendt E "Privacy and Freedom of Speech" in Kenyon AT & Richardson M (eds) *New Dimensions in Privacy Law***:** *International and Comparative Perspectives* (Cambridge University Press 2006)

Benedek, Bauer & Kettemann *Internet Governance and the Information Society*

Benedek W, Bauer V & Kettemann MC *Internet Governance and the Information Society: Global Perspectives and European Dimensions* (Eleven International Publishing 2008)

Brown *Success Secrets*

Brown G *Social Media 100 Success Secrets: Social Media, Web 2.0 User-Generated Content and Virtual Communities - 100 Most Asked Mass Collaboration Questions* (Emereo Publishing 2012)

Bruggemeier, Ciacchi & O'Callaghan *Personality Rights in European Tort Law*

Bruggemeier G, Ciacchi AC & O'Callaghan P *Personality Rights in European Tort Law: The Common Core of European Private Law* (Cambridge University Press 2010)

Burchell *Personality Rights*

Burchell JM *Personality Rights and Freedom of Expression: The Modern* Actio Injuriarum (Juta & Co Ltd 1998)

Burchell *Principles of Delict*

Burchell JM *Principles of Delict* (Juta & Co Ltd 1993)

Burns *Communications Law*

Burns YM *Communications Law* 2 ed (LexisNexis 2009)

Bygrave *Data Privacy Law*

Bygrave LA *Data Privacy Law: An International Perspective* (Oxford University Press 2014)

Chatfield *Myspace.com Handbook*

Chatfield TB *The Myspace.com Handbook: The Complete Guide for Members and Parents* (Atlantic Publishing Group Inc Florida 2007)

Coertser PPJ *Reg op Identiteit*

Coetser PPJ *Die Reg op Identiteit* (unpublished LLM dissertation University of South Africa 1986)

Council of Europe *Handbook*

Council of Europe *Handbook on European Data Protection Law* (2014) available at Handbook_data_protection_ENG.pdf

Currie & de Waal *Bill of Rights Handbook*

Currie I & de Waal J *The Bill of Rights Handbook* 6th ed (Juta & Company Ltd 2007)

David & Brierley *Major Legal Systems in the World Today*

David R & Brierley JEC *Major Legal Systems in the World Today: An Introduction to the Comparative Study of Law* (Simon and Schuster 1978)

Davies & Merchant *Learning and Social Participation*

Davies JA & Merchant G *Web 2.0 for Schools: Learning and Social Participation  New literacies and digital epistemologies* vol 33 (Peter Lang 2009)

Deacon, Lipton & Pinker *Privacy and Personality Rights*

Deacon R, Lipton N & Pinker R *Privacy and Personality Rights – Commercial Exploitation and Protection (*Jordans 2010)

De Antrade "The right to privacy"

De Antrade NNG "The right to privacy and right to identity in the age of ubiquitous computing: friends or foes? A proposal towards a legal articulation" in Akrivopoulou CM *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices: Technologies and Practices* (IGI Global 2010)

De Vos, Freedman & Brand *Constitutional law*

De Vos P, Freedman W & Brand D *South African Constitutional Law in Context* (Oxford University Press Southern Africa 2014)

*Social Media and the Law: A Handbook for UK Companies*

*Social Media and the Law: A Handbook for UK Companies* (Linklaters 2014) available at http://www.linklaters.com/Insights/Social-media-law-A-handbook-UK-companies/Pages/Index.aspx

Dunne *Computers and the Law*

Dunne R *Computers and the Law: An Introduction to Basic Legal Principles and their Application in Cyberspace* (Cambridge University Press 2009)

Doyle *Overview of the ECPA*

Doyle C "Privacy: An Overview of the Electronic Communications Privacy Act" 2012 Congressional Research Service, available at https://www.hsdl.org/?view&did=725508

Edwards & Wealde *Law and the Internet*

Edwards L & Waelde C *Law and the Internet: A Framework for Electronic Commerce* (Hart 2000)

Fridman *Fridman on Torts* 528.

Fridman GHL *Fridman on Torts* (Waterlow Publishers Ltd UK 1990)

Giliker & Beckwith *Tort* 468.

Giliker P & Beckwith S *Tort: Sweet & Maxwell's Textbook Series* 3rd ed (Sweet & Maxwell 2008)

Greenleaf "A world data privacy treaty?"

Greenleaf "A world data privacy treaty? 'Globilisation' and 'modernisation' of Council of Europe Convention 108" in Witzleb N, Lindsay D, Paterson M & Rodrick S *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press 2014)

Grogan *Dismissal*

Grogan J *Dismissal* (Juta & Company Cape Town 2010)

Handa *Fundamentals of Information Technology*

Handa S *Fundamentals of Information Technology* (Lexis Nexis Canada 2004)

Hosten et al *Introduction to South African Law and Legal Theory*

Hosten WJ, Edwards AB, Bosman F, Church J *Introduction to South African Law and Legal Theory* 2nd ed (Butterworths Durban 1997)

Harms *Amler's Precedents of Pleadings* 72.

Harms LTC *Amler's Precedents of Pleadings* 8th ed (LexisNexis South Africa 2016)

Hustinx "The reform of EU data protection"

Hustinx P “The reform of EU data protection: towards more effective and more consistent data protection across the EU” in Witzleb N, Lindsay D, Paterson M & Rodrick S *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press 2014)

Hutchison et al *Law of Contract*

Hutchison D, Pretorius C, Naude T, du Plessis J, Eiselen S, Floyd T & Hawthorne L *The Law of Contract* (Oxford University Press Southern Africa 2013)

Jay *Data Protection*

Jay R *Data Protection Law and Practice* 4th ed (Sweet and Maxwell 2014)

Kanovitz *Constitutional Law*

Kanovitz JR *Constitutional Law* (Routledge 2012)

Kuner *European Data Protection Law*

Kuner C *European Data Protection Law: Corporate Compliance and Regulation* (University Press 2007)

Kuner *Transboder Data Flows and Data Privacy Law* 13.

Kuner C *Transboder Data Flows and Data Privacy Law* (Oxford Scholarship online 2013)

Levmore & Nussbaum *The Offensive Internet*

Levmore S & Nussbaum MC *The Offensive Internet* (Harvard University Press 2012)

Li *Center for Democracy and Technology*

Li JH-S *The Center for Democracy and Technology and Internet Privacy in the US: Lessons of the Last Five Years* (Scarecrow Press 2003)

Lloyd *Cyber Law in the United Kingdom*

Lloyd I *Cyber Law in the United Kingdom* (Kluwer Law International 2010)

Loubser et al *Law of Delict*

Loubser MM, Mukheibir A, Midgley R, Perumal D & Niesing L *The Law of Delict in South Africa* (Oxford University Press Southern Africa 2010)

Lomio & Spang-Hanssen *Legal Research Methods in the US and Europe*

Lomio JP & Spang-Hanssen HS *Legal Research Methods in the US and Europe* (DJØF 2009)

Lytras & Ordoñez de Pablos *Social Web Evolution*

Lytras MD & Ordoñez de Pablos P *Social Web Evolution: Integrating Semantic Applications and Web 2.0 Technologies* (IGI Global 2009)

McQuoid-Mason DM *Law of Prvacy*

McQuoid-Mason DM *Law of Privacy in South Africa* (Juta Cape Town 1978)

Moore *Privacy Rights*

Moore AD *Privacy Rights: Moral and Legal Foundations* (Penn State Press 2010)

Neethling "Personality infringement"

Neethling J "Personality infringement" in Joubert & Faris (eds) 1999 *LAWSA*

Neethling & Potgieter *Law of Delict*

Neethling J & Potgieter J *Neethling, Potgieter & Visser Law of Delict* 7th ed (Durban LexisNexis 2015)

Neethling, Potgieter & Visser *Law of Personality*

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

Potgieter, Steynberg & Floyd *Law of Damages*

Potgieter JM, Steynberg L & Floyd TB *Visser & Potgieter's Law of Damages* 3rd ed (Juta and Company Ltd) 2012

Roos "Data Privacy Law"

Van der Merwe D, Roos A, Pistorious T & Eiselen S *Information and Communications Technology Law (*LexisNexis Durban 2008)

Roos *Data (Privacy) Protection*

Roos A The law of data (privacy) protection: A comparative and theoretical study (LLD thesis, University of South Africa 2003)

Rotenberg *Privacy Law Sourcebook*

Rotenberg M *Privacy Law Sourcebook 2004: United States Law, International Law, and Recent Developments* (Epic 2005)

Samuel *Introduction to Comparative Law*

Samuel G *An Introduction to Comparative Law Theory and Method* (Bloomsbury Publishing 2014)

Savin *EU Internet Law*

Savin A *EU Internet Law* (Edward Edgar Publishing 2013)

Snyman *Criminal Law*

Snyman CR Criminal Law 6th ed (LexisNexis South Africa 2014)

Solove, Rotenberg & Schwartz *Privacy, Information, and Technology*

Solove DJ, Rotenberg M & Schwartz PM *Privacy, Information, and Technology* (Aspen Publishers 2006)

Solove & Rotenberg *Information Privacy Law*

Solove DJ & Rotenberg M *Information Privacy Law* (Aspen Publishers 2003)

Solove & Schwartz *Privacy Law Fundamentals*

Solove DJ & Schwartz PM *Privacy Law Fundamentals* (International Association of Privacy Professionals 2015)

Smith *Internet Law and Regulation*

Smith JH Graham *Internet Law and Regulation* 3rd ed (Sweet & Maxwell 2007)

Street & Grant *Law of the Internet*

Street F Lawrence & Grant MP *Law of the Internet* (Lexis Law Publishing Charlottesville Virginia 2000)

Turkington & Allen *Privacy Law: Cases and Materials*

Turkington RC & Allen AL *Privacy Law: Cases and Materials* (West Group 2002)

Tzanou "Data Protection in EU Law"

Tzanou "Data Protection in EU Law: An analysis of the EU Legal Framework and the ECJ jurisprudence" in Akrivopoulou CM *Personal Data Privacy and Protection in A Surveillance Era* (IGI Global 2010)

Van Dam *European Tort Law*

Van Dam CC *European Tort Law* (Oxford University Press 2006)

Van der Merwe & Olivier *Onregmatige Daad*

Van der Merwe NJ & Olivier PJJ *Die Onregmatige Daad in die Suid-Afrikaanse Reg* 4th ed (JP van der Walt 1980)

Warby, Moreham & Christie *Privacy and the Media*

Warby M, Moreham N & Christie I *Tugendhat & Christie: The Law of Privacy and the Media* (Oxford University Press 2016)

Weaver & Morrison *Social Networking*

Weaver AC & Morrison BB *Social Networking: The Mass Adoption of Social Networking Websites Points to an Evolution in Human Social Interaction* (University of Virginia 2008)

Zimmerman & Visser *Civil Law and Common Law*

Zimmerman R & Visser D *Civil Law and Common Law in South Africa* (Clarendon Press Oxford 1996)

**JOURNALS**

Abril 2007 *Northwestern Journal of Technology and Intellectual Property*

Abril PS 2007 "A (My)Space of one's own: On privacy and online social networks" 2007 *Northwestern Journal of Technology and Intellectual Property* 73-88

Allen 2012 *Journal of Constitutional law*

Allen AL "First amendment privacy and the battle for progressively liberal social change" 2012 *Journal of Constitutional law* 885-927

Allen 2012 *Fordham L Rev*

Allen AL "The natural law origins of the American right to privacy natural law, slavery, and the right to privacy tort" 2012 *Fordham Law Review* 1187-1215

Armstrong 2006 *Computers and Law*

Armstrong N "Defamation and the internet" (2006) Aug/Sept *Computers and Law* 19-21

Bartholomew 2011 *Connecticut Law Review*

Bartholomew M "A right is born: Celebrity, property, and postmodern lawmaking" 2011 *Connecticut Law Review* 301-68

Bennett & Raab 1997 *Inf Soc*

Bennett Colin J & Raab Charles D "The adequacy of privacy: The European Union Data Protection Directive and the North American response" 1997 *Information Society* 245–63

Blume 2012 *IDPL*

Blume P "Will it be a better world? The proposed EU Data Protection Regulation" 2012 *IDPL* available at http://idpl.oxfordjournals.org/

Bratman 2001-2002 *Tennessee Law Review*

Bratman B "Brandeis and Warren's the right to privacy and the birth of the right to privacy" 2001-2002 *Tennessee Law Review* 623-51

Boyd & Ellison 2007 *J Computer-Mediated Comm*

Boyd DM & Ellison NB "Social Network Sites: Definition, history, and scholarship" 2007 *Journal of Computer-Mediated Communication* 210-30

Burchell 2009 *EJ Comp L* 3

Burchell J "The legal protection of privacy in South Africa: A transplantable hybrid electronic" (2009) 13 *Journal of Comparative Law* available at http://www.ejcl.org/131/art131-2.pdf

Calhoun 2015 *Campbell Law Review* 439

Calhoun W "A remedy for online exposure: Recognizing the public-disclosure tort in North Carolina" 2015 *Campbell Law Review* 419-55

Candy 2012 *Drake Law Review*

Cady SS "Reconciling privacy with progress: Fourth amendment protection of e-mail stored with and sent through a third party internet service provider" 2012 *Drake Law Review* 225-50

Caslav 2001 *Victoria University of Wellington Law Review*

Caslav P "Civil law and common law: Two different paths leading to the same goal" (2001) 32 *Victoria University of Wellington Law Review* 817-42

Chigona & Chigona 2008 *Southern African Journal of Information and Communication*

Chigona A & Chigona W "Mxit up in the media: Media discourse analysis on a mobile instant messaging system" 2008 *Southern African Journal of Information and Communication* 42-57

Cohen 2001 *Geo LJ*

Cohen JE "Privacy, ideology, and technology: A response to Jeffrey Rosen" 2001 *The Georgetown Law Journal* 2029-46

Collingwood 2012 *Computer Law & Security Review*

Collingwood L "Privacy, anonymity and liability: Will anonymous communicators have the last laugh?" 2012 *Computer Law & Security Review* 328-34

Connie 2011 *Pace Law Review*

Connie DP "You already have zero privacy. Get over it! Would Warren and Brandeis argue for privacy for social networking" 2011 *Pace Law Review* 146-81

Crean 2009 *Computers and Law*

Crean T "A host of problems: Defamation liability of Irish ISPs" (2009) 20/4 *Computers and Law* 34

Ganguly 2008-2009 *Wis Int LJ*

Ganguly M "Private pictures, public exposure: Papparazzi, compromising images, and privacy law on the Internet" 2008-2009 *Wisconsin International Law Journal* 1141-71

Garrie et al 2010 *Int'l L & Mgmt Rev*

Garrie DB, Gillespie R & Wong R "Data protection: The challenges facing social networking" 2010 *Brigham Young University International Law & Management Review* 127-52

Greenleaf 1(995) 2 *Int Priv Bul*

Greenleaf G “The 1995 EU Directive on data protection – An overview” 1995 (2) *International Privacy Bulletin* 1–28

Greenleaf (2008) 94 *Privacy Laws & Business International*

Greenleaf G “Non-European States May Join European Privacy Convention” (2008) 94 *Privacy Laws & Business International Newsletter* 13-14

Grimmelmann 2009 *Iowa Law Review*

Grimmelmann J “Saving Facebook” 2009 *Iowa Law Review* 1137-1206

Hodge 2006 *Southern Illinois University Law Journal*

Hodge MJ “The fourth amendment and privacy issues on the ‘new’ Internet: Facebook.com and myspace.com” 2006 *Southern Illinois University Law Journal* 95-123

Helscher 1994-1995 *Northern Illinois University Law Rev*iew

Helscher D “*Griswold v Connecticut* and the unenumerated right to privacy” 1994-1995 *Northern Illinois. University Law Rev*iew 33-61

Kirby 2011 *International Data Privacy Law*

Kirby M “The history, achievement and future of the 1980 OECD ALI guidelines on privacy” 2011 *International Data Privacy Law* 6-14

Kleinschmidt 2010 *International Journal of Law and Technology*

Kleinschmidt B “An International comparison of ISP’s liabilities for unlawful third party content” 2010 *International Journal of Law and Technology* 332-55

Larson & Godfread 2011 *William Mitchell LR*

Larson RG & Godfread PA “Bringing John Doe to court: Procedural issues in unmasking anonymous internet defendants” 2011 *William Mitchell Law Review* 328-52

Kosta et al *Transforming Government: People, Process and Policy*

Kosta E, Kalloniatis C, Mitrou L & Gritzalis S "Data protection issues pertaining to social networking under EU law" 2010 *Transforming Government: People, Process and Policy* 193-201

McQuoid-Mason 1973 *SALJ*

McQuoid-Mason DJ "Invasion of potency"1973 *SALJ* 252-CLOSING PGE

McQuiod-Mason 2000 *Acta Juridica*

McQuoid-Mason DJ "Invasion of privacy: Common law *v* Constitutional delict - Does it make a difference?" 2000 *Acta Juridica* 227-261

Neethling 2014 *LitNet Akademies*

Neethling J "Openbare figuur: Laster, belediging en identiteitskending: *Cele v Avusa Media Limited* [2013] 2 All SA 412 (GSJ)" 2014 *LitNet Akademies* 116-24

Neethling 2005 *CILSA*

Neethling J "Personality rights: A comparative overview" 2005 *CILSA* 210-45

Nel 2007 *CILSA*

Nel S "Online defamation: The problem of unmasking anonymous online critics" 2007 *CILSA* 193-214

Newell 2010-2011 *Rich JL & Tech*

Newell B "Rethinking reasonable expectations of privacy in online social networks" 2010-2011 *Rich JL & Tech* 1-62

Osorio 2010 *NYU Annual Survey*

Osorio A "Twilight: The fading of false light invasion of privacy" 2010 *NYU Annual Survey of American law* 173-209

Pabarcus 2011 *William Mitchell Law Review*

Pabarcus A “Are ‘private’ spaces on social networking websites truly private? The extension of intrusion upon seclusion” 2011 *William Mitchell Law Review* 397-432

Papadopoulos 2009 *Obiter*

Papadopoulos S “Revisiting the public disclosure of private facts in cyberworld” 2009 *Obiter* 30-43

Parent 1983 *American Philosophy Quarterly*

Parent WA “Recent work on the concept of privacy” 1983 *American Philosophy Quarterly* 341-55

Powell 2011 *Pace Law Review*

Powell CD “You already have zero privacy. Get over it! Would Warren and Brandeis Argue for Privacy for Social Networking?” 2011 *Pace Law Review* 146-81

Prosser 1960 *Cal L Rev*

Prosser WL “Privacy” 1960 *California Law Review* 383-423

Rautenbach 2009 *TSAR*

Rautenbach IM “Privacy taxonomies*”* 2009 *TSAR* 548-54

Rautenbach 2001 *TSAR*

Rautenbach IM "The Limitation of rights in terms of provisions of the Bill of Rights other than the general limitation clause: A few examples" 2001 TSAR 617-41

Rautenbach 2001 *TSAR*

Rautenbach IM “The conduct and interests protected by the right to privacy in section 14 of the Constitution” 2001 *TSAR* 115-23

Reding 2012 *IDPL*

Reding V “The European data protection framework for the twenty-first century” (2012) *IDPL* available at http://idpl.oxfordjournals.org/

Richards & Solove 2010 *Cal L Rev*

Richards NM & Solove DJ “Prosser's privacy law: A mixed legacy” 2010 *California Law Review* 1887-1924

Roline & Skalberg *ALSD Journal of Employment Law and Labor Law*

Roline AC & Skalberg K “*Lake v Wal-mart*: The law of privacy revealed” 2004 *ALSD Journal of Employment Law and Labor Law* 77-83

Roos 2012 *SALJ*

Roos A “Privacy in the Facebook era: A South African legal perspective” 2012 *South African Law Journal* 375-402

Roos 2007 *SALJ*

Roos A "Data protection: Explaining the international backdrop and evaluating the current South African position" 2007 *SALJ* 400-33

Roos 2008 *PER*

Roos A “Personal data protection in New Zealand: Lessons for South Africa?” 2008 *PER* 62-109

Rosenblum 2007 *IEEE Security & Privacy*

Rosenblum D “What anyone can know: The privacy risks of social networking sites” 2007 *IEEE Security and Privacy* 40-49

Sewsunker (2013) July *De Rebus*

Sewsunker S “Inexpensive civil remedy for harassment: The Protection from Harassment Act (2013) July *De Rebus* 34-6

Sobel 2000 *VA JL & Tech*

Sobel DL “The process that ‘John Doe’ is due: Addressing the legal challenge to internet anonymity” 2000 *VA JL & Tech* 1522-1687

Stefanone, Lackaff & Rosen 2010 *Journal of Broadcasting and Electronic Media*

Stefanone MA, Lackaff D & Rosen D “The relationship between traditional mass media and ‘social media’: Reality television as a model for social network site behaviour” 2010 *Journal of Broadcasting and Electronic Media* 508-525

Valentine 2000 *Computer & High Technology Law Journal*

Valentine DA “Privacy on the internet: The evolving legal landscape” 2000 *Computer & High Technology Law Journal* 401-417

Warren & Brandeis 1890 *Harv L Rev*

Warren SD & Brandeis LD “The right to privacy” 1890 *Harvard Law Review* 193-220

Westin 2003 *Journal of Social Issues*

Westin AF “Social and political dimensions of privacy” 2003 *Journal of Social Issues* 431-53

Williams 2013 *Qualitative Market Research: An International Journal*

Williams AWD "Why people use social media: A uses and gratifications approach" (2013) 16/4 *Qualitative Market Research: An International Journal* 362 - 9

Wong 2009 *Communication Law*

Wong “Social Networking: A conceptual analysis of a data controller” (2009) 14/5 *Communication Law* 142-9

**JUDICIAL DECISIONS**

**Australia**

*Gutnick v Dow Jones* 2002 HCA 56

**South Africa**

*African Life Assurance Society Ltd v Phelan* (1908) 25 SC 743

*Bernstein and others v Bester NO* 1996 (2) SA 751 (CC)

*C v Minister of Correctional Services* 1996 (4) SA 292 (T)
*CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* 2012 (5) SA 604 (KZD)
*Case v Minister of Safety and Security* 1996 (3) SA 617 (CC)
*Crawford v Albu* 1917 AD 102

*De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, and Others* 2004 (1) SA 406
*Dutch Reformed Church Vergesig Johannesburg Congregation and Another v Rayan Soknunan t/a GloryDivinee World Ministries* 2012 (6) SA 201 (GSJ); [2012] 3 All SA 322 (GSJ)

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

*GA Fichardt Ltd v The Friend Newspaper Ltd* 1916 AD 1
*Greeff v Protection 4U h/a Protect International* 2012 (6) SA 393 (GNP)
*Grütter v Lombard* 2007 (4) SA 89 (SCA)

*H v W* 2013 (2) SA 530 (GSJ); 2013 (5) BCLR 554 (GSJ); [2013] 2 All SA 218 (GSJ)
*Harvey v Niland and Others* 2016 (2) SA 436 (ECG)
*Heroldt v Wills* 2013 (2) SA 530

*Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 (1) SA 545 (CC) 557
*Isparta v Richter and Another* 2013 (6) SA 529 (GNP)

*Janit and Another v Motor Industry Fund Administrators (Pty) Ltd and Another* 1995 (4) SA 293 (A)
*Jansen van Vuuren and Another NNO v Kruger* 1993 (4) SA 842 (A)
*Jooste v National Media Ltd* 1994 (2) SA 634 (C)
*Jordan v State* 2002 (6) SA 642 (CC)

*Kidson v SA National Associated Newspapers Ltd* 1957 (3) SA 461 (W)
*Kumalo v Cycle Lab (Pty) Ltd* [2011] ZAGP JHC 56 (17 June 2011)

*Laugh it Off Promotions CC v South African Breweries International (Finance) BV t/a* 2005 (8) BCLR 743 (CC); 2006 (1) SA 144 (CC)
*Le Grange v Schoeman* 1980 (1) SA 885 (E)

*M v B* 2015 (1) SA 270 (KZP)
*Makhanya v Vodacom* 2010 (3) SA 79 (GNP)
*Malan v Bulbring NO and Others* 2004 (25) *ILJ* 1737 (LC)
*Malema v Rampedi and Others* 2011 (5) SA 631 (GSJ)
*Marais v Richard* 1981 (1) SA 1157 (A)
*Media Workers Association of SA on behalf of Mvemve and Kathorus Community Radio* 2010 (31) ILJ 2217 (CCMA)
*Mhlongo v Bailey* 1958 (1) SA 370 (W)
*Mistry v Interim National Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC)
*Motor Industry Fund Administrators (Pty) Ltd v Janit* 1994 3 SA 56 (W) 60-61

*NM and Others v Smith and Others (Freedom of Expression Institute as* Amicus Curiae*)* 2007 (5) SA 250 (CC)
*National Coalition for Gay and Lesbian Equality v Minister of Justice* 1998 (12) BCLR (CC)
*National Media Ltd v Bogoshi* 1998 (4) SA 1196 (SCA)
*National Media Ltd and Another v Jooste* 1996 (3) SA 262 (A)

*O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 3 SA 224 (C)

*Priday v Thos Cook & Son (SA) Ltd* 1952 (4) SA 761 (C)

*R v Holliday* 1927 CPD 395
*Rhodesian Printing and Publishing Co Ltd v Duggan* 1975 (1) SA 590 (RA)

*S v A* 1971 (2) SA 293 (T).
*S v Madiba* 1988 (1) SA BCLR 38 (D)
*Sabmark International* 2005 (8) BCLR 743 (CC); 2006 (1) SA 144 (CC)
*Santam Insurance v Vorster* 1973 (4) SA 764 (A) 779
*Sedick & Another and Krisray (Pty) Ltd* (2011) 32 ILJ 752 (CCMA)
*Setlogelo v Setlogelo* 1914 AD 221 227
*Smith v Partners in Sexual Health (non-profit)* (2011) 32 IJL 1470 (CCMA)
*Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 4 SA 549 (T)
*Swanepoel v National Media Ltd v Jooste* 1996 (3) SA 262 (A); 1996 (2) SA 751 (CC)

*Tshabalala-Msimang and Others v Makhanya and Others* 2008 (6) SA 102 (W)
*Tsichlas v Touch Line Media (Pty) Ltd* 2004 (2) SA 112 (W)

*Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T)
*Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1979 (1) SA 441 (A)

*Walsh v Botha* 1960 (2) SA 323 (O)
*Witwatersrand Native Labour Association Ltd v Robinson* 1907 TS 264

**United Kingdom**

*Bunt v Tilley 2006* EWHC 407 QB

*Campbell v MGN Limited* [2004] UKHL 22

*Duchess of Argyll v Duke of Argyll* 1967 Ch 302

*Godfrey v Demon Internet Ltd* 2001 QB 201

*Harrington v Polytechnic of North London* [1984] 1 WLR 1293
*Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804

*McKennit v Ash* [2006] EWCA Civ 1714

*Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] AC 133

*Prince Albert v Strange* (1849) ER 1171

*R (B) v MOJ* [2009] EWHC 2220 (Admin)
*R (Purdy) v DPP* [2009] UKHL 45; [2009] 3 WLR 403

*Telnikoff v Matusevitch* [1991] 4 All ER 817 826
*Totalise plc v The Motley Fool* [2001] EWCA Civ 1897

**United States of America**

*American Civil Liberties Union v Reno* 31 F Supp 2d 473 US Dist Lexis (ED Pa 1999)

*Boyd v United States* 116 US616 (1886)

*Cecilia L Barnes v Yahoo Inc, A Delaware Corporation* (District of Oregon) US Court of Appeal 9th Cir 2005

*Chaplinsky v New Hampshire* 315 US 568 (1942)

*Columbia Insurance Co v Seescandy.com* 185 FRD 573 (ND Cal 1999)

*Cubby Inc v CompuServe Inc* 776 F Supp 135 (SD NY 1991)

*Doe v Kohn Nast & Graf PC* 866 F Supp 190 (ED Pa 1994).

*Faconnable v Does* 2011 WL 2173736 (US District Court D Colorado Jun 2 2011)

*Fischer v Hooper* 732 A 2d 396 (1999)

*Hill v NCAA* 865 P2dn638 (Cal 1994)

*In re Subpoena* Duces Tecum *to American Online Inc* 52 Va Cir 26 (2000)

*Jim Henson Productions Inc v John T Brady & Associates Inc* 687 F Supp 185 (SDNY 1994)

*Lake v Wal-Mart* 582 NW 2d 231 (Minn 1998)

*Miller v California* 413 US 15 (1973)

*Miller v Motorola Inc* 560 NE 2d 900 (Ill App 1990)

*Monroe v Darr* 221 Kan 281, 559 P 2d 322 (1977)

*Moreno v Hanford Sentinel Inc* 91 Cal Rptr (Cal Ct App 2009)

*New York v Ferber* 458 US 747 (1982)

*Noel v Hall* 568 F 3d 743 (9th Cir 2009)

*Pavesich v New England Life Insurance Co* 122 Ga 190, 50 SE 68 (1905)
*People v Christian* Sacramento County Superior Court case number 08F09791
*Pritchett v Board of Com'rs of Knox Country* 85 NE 32 (ND Ga 1951)

*Roe* v *Wade* 410 US 113 (1973)
*Rogers v Loews L'Enfant Plaza Hotel* 526 F Supp 523 (DDC 1981)

*Schmerber v California* 384 US 757 (1966)
*Shepard's Pharmacy Inc v Stop & Shop Companies Inc* 37 Mass App Ct 516; 640 NE 2d 1112 (Ct App 1994)
*Stratton Oakmont Inc v Prodigy Services Company* 1995 NY US

*United States v Szymuszkiewicz* 622 F 3d 701 (7th Cir 2010).

*Watts v United States* 394 US 705, 89 S Ct 1399, 22 L Ed 2d 664 (1969)

*Zeran v America Online Inc* 129 F 3d 327 (4th Cir 1997)

**Regional**

*Amann v Switzerland* Case no 27798/95 ECHR [GC]

*Bărbulescu v Romania* Case no 61496/08 ECHR 61
*Bodil Lindqvist v Åklagarkammaren i Jönköping* ECLI:EU:C:2003:596

*Copland v UK* Case no 62617/00 § 41 ECHR 2007- I
Costello-Roberts *v UK* 1995 (19 EHRR) 112

*Dudgeon v UK* [1983] ECHR 2, 7525/76, (1983) 5 EHRR 573

*EB v France* [GC] (2008) 47 EHRR 21
*Eifert v Land Hessen* ECLI:EU:C:2010:662

*Fernández Martínez v Spain* [GC] no 56030/07 § 126; 2014 ECHR
*František Ryneš v Úřad pro ochranu osobních údajů* ECLI:EU:C:2014:2428

*Gaskin v UK* (1989) 12 EHRR 36
*Goodwin v UK* (2002) 35 EHRR 18

*Halford v The United Kingdom* (1997) 24 EHRR 523.

Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Laskey v UK* (1997) 24 EHRR 39

*Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650, 06/10/2015
*McFeeley v UK* (1981) 3 EHRR 161
*McCotter v UK* (1993) 15 EHRR CD98
*MS v Sweden* 20837/92 [1997] ECHR 49

*Niemietz v Germany* [1992] 16 EHRR 97
*Norris v Ireland* (1991) 13 EHRR 186

*Peck v UK* (2003) 36 EHRR 719
*Pretty v UK* (2002) 35 EHRR 1
*Pretty v UK* (2001) 35 EHRR 1
*Raninen v Finland* (1998) 26 EHRR 563

*Shelley v UK* (2008) 46 EHRR SE16
*Slivenko v Latvia* (2004) 39 EHRR 24
*Stjerna v Finland* (1997) 24 EHRR 195

*Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* ECLI:EU:C:2008:727

*Von Hannover v Germany* (2005) 40 EHRR

## LEGISLATION

### South Africa

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Correctional Services Act 111 of 1998

Criminal Procedure Act 51 of 1977

Electronic Communication and Transactions Act 25 of 2002

Films and Publications Act 65 of 1996

Films and Publications Amendment Bill [B 37—2015]

Magistrates' Courts Act 32 of 1944

National Credit Act 34 of 2005

National Health Act 61 of 2003

Promotion of Access to Information Act 2 of 2000

Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000

Protected Disclosures Act 26 of 2000

Protection from Harassment Act 17 of 2011

Protection of Personal Information Act 4 of 2013

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

Supreme Court Act 59 of 1959

### Sweden

Personuppgiftslag (SFS 1998:204) (Swedish Data Protection Act 1998)

### United Kingdom

Data Protection Act, 1998

Defamation Act, 1996

Defamation Act, 2013

Freedom of Information Act, 2000

Human Rights Act, 1998

Regulation of Investigatory Powers Act, 2000

**United States of America**

Bank Secrecy Act of 1970

Cable Communications Policy Act of 1984

CAN-SPAM Act of 2001

Children's Online Privacy Protection Act of 1998

Communications Assistance for Law Enforcement Act of 1994

Communications Decency Act of 1996

Computer Matching and Privacy Protection Act of 1988

Department of Homeland Security Act of 2002

Driver's Privacy Protection Act of 1994

Electronic Communications Privacy Act of 1986

Employee Polygraph Protection Act of 1988

Fair Credit Reporting Act of 1970

Family Educational Rights and Privacy Act of 1974

Foreign Intelligence Surveillance Act of 1978

Foreign Intelligence Surveillance Act 1978 Amendment Act of 2008

Gramm-Leach-Bliley Act of 1999

Health Insurance Portability and Accountability Act of 1996

Identity Theft Assumption and Deterrence Act of 1998

Intelligence Authorization Act for Fiscal Year 2001

Omnibus Crime Control and Safety Street Act of 1968 Title III

Personal Responsibility and Work Opportunity Reconciliation Act of 1996

Privacy Act of 1974

Privacy Protection Act of 1980

Rights to Financial Privacy Act of 1978

Telephone Consumer Protection Act of 1991

USA-PATRIOT Act of 2000

USA PATRIOT Act of 2001

USA PATRIOT Improvement and Reauthorization Act of 2006

Video Privacy Protection Act of 1988

Video Voyeurism Prevention Act of 2004

21st century Department of Justice Appropriations Authorization Act of 2002

## INTERNATIONAL & REGIONAL INSTRUMENTS

### African Union

African Charter on Human and Peoples' Rights ('Banjul Charter') 27 June 1981 CAB/LEG/67/3 rev 5, (1982) 21 *ILM* 58

African Charter on the Rights and Welfare of the Child 11 July 1990 CAB/LEG/24.9/49 (1990)

Convention on Cyber Security and Personal Data Protection 27 June 2014 EX CL/846(XXV) (2012)

### United Nations

Charter of the United Nations 24 October 1945 1 UNTS XVI

Guidelines for the Regulation of Computerized Personal Files UNGA res 45/95 14 December 1990

International Covenant on Civil and Political Rights 16 December 1966, 999 UNTS 171 and 1057 UNTS 407 / [1980] ATS 23 / (1967) 6 *ILM* 368

International Covenant on Economic, Social and Cultural Rights 16 December 1966 999 UNTS 171 and 1057 UNTS 407 / [1980] ATS 23 / (1967) 6 *ILM* 368

Universal Declaration of Human Rights UNGA res 217A (III) 10 December 1948

### Organisation for Economic Cooperation and Development

Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data, Paris 23 September 1980

Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy 12 June 2007

### Council of Europe

Convention for the Protection of Human Rights and Fundamental Freedoms ETS 5 4 November 1950

Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data No 108/1981

**European Union**

Charter of Fundamental Rights of the European Union (2010/C 83/02)

Directive 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

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on privacy and electronic communications)

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution

of Criminal Penalties, and on the Free Movement of such Data, and Repealing Council Framework Decision 2008/977/JHA

European Union Referendum Act of 2015

Proposal for a regulation of the European Parliament and of the Council 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) 2012/0011 (COD)

**INTERNET WEBSITES**

http://www.ispa.org.za/code-of-conduct/take-down-procedure
http://www.facebook.com
http://newsroom.fb.com/content/default
www.socialmedialogue.com/facebook-statistics
http://www.comscore.com/About_comScore
www.thepresidency.gov.za/pebble
www.matthewgain.posterous.com
http://mashable.com
http://www.mxit.co.za
www.vjolt.net
www.myspace.com
www.twitter.com
http://site.mxit.com/pages/policies/privacypolicy
http://www.oecd.org
www.echr.coe.int/Documents/
http://www.presscouncil.org.za

**CONFERENCES, PAPERS, REPORTS, SEMINARS**

American Law Institute *Restatement of the Law (Second) Torts 1977* available at https://cyber.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm

Bowen "*Article 8 and 'private life': The protean right"*

Bowen P "*Article 8 and 'private life': The protean right"* Constitutional & Administrative Law Bar Association Seminar, Doughty Street Chambers 2 March 2010

Boyd "*Friendster and publicly"*

Boyd D "*Friendster and publicly articulated social networks*" Conference on Human Factors and Computing Systems (CHI 2004) Vienna: ACM, April 24-29, 2004.124

Dywer, Hiltz & Passerini 2007 *"Trust and privacy concern"*

Dwyer C, Hiltz SR & Passerini *"Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace"* (2007) *Americas Conference on Information Systems Proceedings* 2007

Esselaar "*What ISPs can do about undesirable content"*

Esselaar P "*What ISPs can do about undesirable content"* paper commissioned by the Internet Service Providers' Association (ISPA) 2008 available at !http://www.ispa.org.za

EU Art 29 DP WP "*Data Protection Reform Package Annex 2"*

EU Art 29 Data Protection Working Party *Statement of the Working Party on Current discussions regarding the Data Protection Reform Package Annex 2: Proposals for Amendments regarding Exemption for Personal or Household Activities (*27 February 2013)

EU Art 29 DP WP *Opinion 5/2009 on Online Social Networking* WP 5

EU Art 29 DP WP *Opinion 1/2008 on Data Protection Issues related to Search Engines WP* 8

Greenleaf & Georges "2014 *Privacy Laws & Business International Report"*

Greenleaf G & Georges M "African regional privacy instruments: Harmonising effects" 2014 *Privacy Laws & Business International Report* available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566724 13-17

Gross & Acquisti *"Information revelation"*

Gross R & Acquisti A *"Information revelation and privacy in online social networks"* ACM Workshop on Privacy in the Electronic Society (WPES) 2005 New York available at https://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf

Information Commissioner's Office *Guide to Data Protection* 2010 (UK) available at https://ico.org.uk/for-organisations/guide-to-data-protection/

SALRC "*Privacy and data protection 2005"*

South African Law Reform Commission "*Privacy and data protection 2005"* discussion paper 109 Project 124 October 2005 available at http://www.justice.gov.za/salrc/dpapers/dp109.pdf

Seppa *"The future of social networking"*

Seppa V *"The future of social networking"* paper presented at the Seminar on Internetworking at Helsinki University of Technology Seminar on Internetworking 28 April 2008 available at cse.tkk.fi/en/publications/B/1/papers

UK Equality & HR Commission *"The UK and the European Court of Human Rights"*

UK Equality & Human Rights Commission *"The UK and the European Court of Human Rights"* Research Report 83 (2012) available at www.equalityhumanrights.com/en/publication

Zheleva & Getoor *"To join or not to join"*

Zheleva E & Getoor L *"To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles"* paper presented at the

18th International World Wide Web conference, Madrid Spain April 2009 available at //linqs.cs.umd.edu/basilic/web