UNIVERSITY OF KWAZULU-NATAL ™

INYUVESI YAKWAZULU-NATALI

COLLEGE OF LAW AND MANAGEMENT STUDIES

SCHOOL OF LAW

MAHLANGANISE, EDMORE

The rise of electronic commerce transactions in South Africa: Legal issues pertaining to privacy

Submitted in Fulfilment of the LLM Degree in Business Law at the University of Kwa-Zulu Natal

Supervisor: Adv. Darren Cavell Subramanien

2017

DECLARATION

I hereby declare that this thesis is my own unaided work, and that all my sources of information have been acknowledged. To my knowledge, neither the substance of this dissertation, nor any part thereof, is being submitted for a degree in any other University.

_____

E. MAHLANGANISE

216076101

NOVEMBER 2017

ACKNOWLEDGEMENTS

I would like to thank God for the year of blessings I received during the study towards my LLM and for the completion of the same.

I would also like to thank Adv. Darren Cavell Subramanien for taking on the challenge of being my supervisor for this research. I appreciate his kindness and tolerance to my incessant impositions. His immense knowledge in law across various jurisdictions proved most beneficial and helpful in my studies. His guidance, intellectual stimulation, pedantic nature, extensive comments which he provided in the drafts that I sent to him and his ability to nudge me in the correct direction proved to be the most critical factors in taking me to this proverbial finishing line.

Dr Rosemary Kuhn, (Pietermaritzburg Campus Law Librarian) I could not have been here without her dedication and love. She opened the doors to her office every time I knocked in need of help. I am eternally grateful. Robynne Louw, (Pietermaritzburg Campus Postgraduate Centre for Legal Studies Administrator) I am thankful for the help I received from her from the time I came to this institution.

I am so grateful to my parents, Joel and Edinah, my siblings Godwin, Lucky, Gift, Tafadzwa and Rumbidzai for all they did to ensure my success in all my endeavours. I am thankful to all my friends and all those who supported and encouraged me in any respect throughout this research. I am forever indebted to them.

Finally, when recounting a series of adventures, Satchel Paige was known to say, "Them were tall times." This phrase aptly expresses the sheer scale of the excitement, satisfaction and rich rewards this research has brought me. Tall times, indeed!!

DEDICATION

This piece of work is dedicated to my brother Lucky. You have been the wind beneath my wings and you have provided me with nurturing, care, support and love. Thank you and God bless you abundantly.

TABLE OF CONTENTS

CHAPTER TWO

CHAPTER THREE

3. Consumer Concerns in Data Transmissions and Principles of Information Protection **40**

CHAPTER FOUR

CHAPTER FIVE

CHAPTER SIX

ABBREVIATIONS

1. ACHR - The American Convention on Human Rights of 1969.
2. ATM - Automated Teller Machine.
3. AUCLCS - African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.
4. BILETA - British and Irish Law Education and Technology Association.
5. B2A - Business to Administration.
6. B2B - Business to Business.
7. B2C - Business to Consumer.
8. C2B - Consumer to Administration.
9. C2C - Consumer to Consumer.
10. C2G - Consumer to Government.
11. CDA - Communications Decency Act of 1996.
12. CFAA - Computer Fraud and Abuse Act of 1994.
13. CoE Convention - The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data.
14. COPPA - Children's Online Privacy Protection Act of 1990.
15. CPA - Consumer Protection Act 68 of 2008.
16. DMV - Department of Motor Vehicles.
17. DPA - Data Protection Act.
18. E-Business - Electronic Business.
19. E-Commerce - Electronic Commerce.
20. E-Signature - Electronic Signature.
21. E-Tailing - Electronic Tailing.
22. ECA - Electronic Communications Act 36 of 2006.

23. EC Directive - Electronic Commerce (EC Directive) Regulations of 2002.
24. ECHR - European Convention on Human Rights of 1953.
25. ECPA - The Electronic Communication Privacy Act of 1986.
26. ECTA - Electronic Communications and Transactions Act 25 of 2002.
27. EDI - Electronic Data Interchange.
28. EFTA - Electronic Fund Transfer Act of 1978.
29. EU - European Union.
30. EU Directive - European Union Directive on Privacy and Data Protection.
31. FACTA - Fair and Accurate Credit Transactions Act of 2003.
32. FCRA - Fair Credit Reporting Act of 1970.
33. FERPA - Family Educational Rights and Privacy Act of 1974.
34. FTC - Federal Trade Commission.
35. GLBA - Gramm-Leach Bliley Act of 1999.
36. HIPAA - The Health Insurance Portability and Accountability Act of 1996.
37. HRA - Human Rights Act 1998.
38. ICASA Act - Independent Communications Authority of South Africa Act 13 of 2000.
39. ICCPR - International Covenant on Civil and Political Rights of 1976.
40. ICT - Information Communications Technology.
41. IT - Information Technology.
42. JSC - Judicial Service Commission.
43. MLEC - United Nations Commission on International Trade Law Model Law on Electronic Commerce of 1996.
44. MLES - The United Nations Commission on International Trade Law Model Law on Electronic Signatures of 2001.

45. NCA - National Credit Act 34 of 2005.
46. OECD - Organization for Economic Cooperation and Development.
47. PAIA - Promotion of Access to Information Act 4 of 2000.
48. PEC Regulations - The Privacy and Electronic Communications (EC Directive) Regulations 2003 Number 2426.
49. POPI - Protection of Personal Information Act 4 of 2013.
50. POS - Point of Sale.
51. PPA - Privacy Protection Act of 1980.
52. RICA - Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.
53. SA - South Africa.
54. SAFE Data Act - Secure and Fortify Electronic Data Act of 2011.
55. SALRC - South African Law Reform Commission.
56. SSL - Secure Socket Layer.
57. SCA - Supreme Court of Appeal.
58. TPP - Trans-Pacific Partnership.
59. UDHR - Universal Declaration of Human Rights 1948.
60. UK - United Kingdom.
61. UNCITRAL - United Nations' Commission on International Trade Law.
62. UNECIC - The United Nations Convention on the Use of Electronic Communications in International Contracts 2005.
63. USA - United States of America.
64. USA FREEDOM Act - Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015.

65. USA PATRIOT Act - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.
66. www - World Wide Web.

ABSTRACT

The internet in South Africa provides significant benefits to users involved in electronic commerce. Manufacturers, wholesalers, retailers and consumers enjoy the great convenience of doing business online. While electronic commerce transactions have great benefits, they also come with great risks and ultimately disadvantages. The increase in e-commerce in South Africa is proportional to the increase in privacy concerns, thus the legislature has passed legislation to deal with these informational security issues. Is the legislation addressing privacy concerns in e-commerce sufficient in dealing with these privacy concerns? What are the legal consequences of doing business online in relation to informational privacy?

KEY WORDS AND PHRASES

1. Computer
2. Data
3. Data Controller
4. Data Protection
5. Data Subject
6. Digital *Loci*
7. E-Business
8. E-commerce
9. E-Tailing
10. Electronic Business
11. Electronic Commerce
12. Electronic Data Interchange
13. Electronic Tailing
14. Information
15. Information Communications Technology
16. Information Protection
17. Information Security
18. Information Technology
19. Internet
20. Legal and Policy Framework
21. Online
22. Personal Identifiable Information
23. Personal Information
24. Privacy

25. Privacy Policy
26. Privacy Protection
27. Sale of goods and Services
28. Spam
29. Technology
30. Torts
31. Transactions

DEFINITION OF KEY TERMS

1. Data – Means electronic representations of information in any form.
2. Data Message – Is data generated, sent, received or stored by electronic means and includes (a) voice, where the voice is used in an automated transaction; and (b) a stored record.
3. Electronic Commerce – Is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet.
4. Legal Framework – A set of documents that include the Constitution, legislation, regulations, and contracts. How these documents relate to one another.
5. Online – Controlled by or connected to the internet through a computer or related device.
6. Tort – A wrongful act (infringement of a right) other than the breach of a contract for which relief may be obtained in the form of damages or an injunction.
7. Transaction – A transaction of a commercial nature and includes the provision of information services.

CHAPTER ONE

1. INTRODUCTION

1.1. Background

According to global standards, electronic commerce (hereafter referred to as e-commerce) is still developing in South Africa.[1] The introduction of e-commerce has by great and wide strides changed the way in which companies, individuals and organizations conduct business.[2] The internet has bequeathed organizations with opportunities to improve their business processes, target and expand new markets, create business strategies and increase customer satisfaction.[3]

The introduction of e-commerce in the Republic of South Africa took place more than a decade ago and to date, due to the increase in online transactions, new legal challenges have arisen.[4] As a result of the increase in online transactions, the Republic of South Africa introduced among other legislation, the Electronic Communications and Transactions Act (hereafter referred to as ECTA).[5] The ECTA came into force on 30 August 2002 to govern electronic transactions.[6]

Although the introduction of e-commerce (also referred to hereinafter as e-business or e-tailing) is an evolution that has been a major step up from the traditional way of doing business, it has also brought about adverse legal consequences on issues of security, confidentiality and consumer trust as well as on privacy protection for consumers in data

[1] South Africa Department of Communications 'Discussion Paper on Electronic Commerce' (1999) 1.
[2] N M Din & M Z Jamaluddin 'Building a trusted environment for e-business: Malaysian perspective' (2003) (1) *Journal of ICT* 34.
[3] B J Corbitt … et al 'Trust and e-commerce: A study of consumer perceptions' (2003) 2 (1) *Electronic Commerce Research and Application* 203. Din & Jamaluddin ibid.
[4] I J Lloyd *Information Technology Law* 7 ed (2014) 11. South Africa Department of Communications 'A Green Paper on Electronic Commerce for South Africa' (2000) 15.
[5] Electronic Communications and Transactions Act 25 of 2002.
[6] ibid.

transmission.[7] E-business information must be protected in storage and in transit over the computer telecommunications networks.[8]

1.2. The Rationale for the Study and Key Questions to be Answered by the Research

The e-commerce industry is rapidly expanding and the technology enabling e-business has matured significantly.[9] The benefits derived from e-commerce are numerous, and some of these include the fact that it is an expedient means of contracting, as it saves time and energy and that it is easily accessible.[10] The proliferation in the number of online retailers is indicative of society's acceptance of e-commerce.[11] Benefits also come with inherent risks such as cybercrimes, revenue loss through tax avoidance.[12] In the end the aim is to transform the way e-business is conducted.[13]

Despite its capacity to transform business operations, e-commerce is still faced with a lot of legal challenges.[14] Security is one of the most challenging problems faced by customers who wish to trade in the e-commerce world.[15] The problem results from the vulnerabilities of the internet upon which e-commerce is based. The vulnerabilities of the internet may inhibit customers from participating in e-commerce if they feel that the level of risk is unacceptable.[16]

The current legal framework does not address all the different legal challenges relating to e-

[7] South Africa Department of Communications 'A Green Paper on Electronic Commerce for South Africa' (2000) 15.
[8] See Note 2 above.
[9] See Note 1 above.
[10] B Suh & I Han 'The impact of customer trust and perception of security control on the acceptance of electronic commerce' (2003) 7 (3) *International Journal of Electronic Commerce* 135.
[11] ibid 136.
[12] ibid.
[13] ibid.
[14] See Note 7 above at 24.
[15] See Note 10 above.
[16] ibid.

commerce transactions.[17] Therefore a need exists to formulate a new legal framework and/or to improve the current legal framework for those business transactions that are concluded electronically.[18]

From a policy perspective such a legal framework would have to address all the different factors and challenges that are associated with using an information and communication technology platform for a business transaction to be legally valid.[19]

The rationale of this dissertation is to assess the legal framework around e-commerce and to see how far it helps in dealing with challenges that arise from that type of transaction. The dissertation will more specifically focus on the legal framework of e-commerce particularly on issues relating to privacy and data protection.

This dissertation will attempt to examine the efforts made by South Africa in dealing with information protection issues. This examination will be done by conducting a critical analysis of South Africa's laws that govern information protection in e-commerce transactions. The dissertation will also seek to identify intermissions in that legislation relating to information protection.

This dissertation will also, to a large extent focus on consumer protection. More emphasis will be given on this in the following chapters. A brief analysis of the ECTA will suffice for one to say that the ECTA has certain provisions that deal specifically with consumer protection in electronic transactions.[20]

[17] ibid.
[18] ibid.
[19] ibid.
[20] See Chapter VII of the Electronic Communications and Transactions Act 25 of 2002.

The question of why privacy is important has been addressed in a number of ways. As a matter of fact, privacy concerns are deeply rooted in history dating as far back as the times of the Roman-Dutch law.[21] Grayling, one of the foremost contemporary philosophers in the United Kingdom has made observations that highlight the human rights background on which privacy is based. According to Grayling:

> "No human rights convention is complete without an article that defends privacy, for the excellent reason that privacy is an indispensable adjunct of the minimum that individuals require for a chance to build good lives. One aspect of its importance is that it gives people a measure of control over the front they offer to others, and the amount of information that others have about them, concerning matters that are personal, intimate, eccentric or constitutive of the individual's inner life…. But the foremost reason for privacy is that it is crucial for personal autonomy and psychological wellbeing. Even lovers require a degree of privacy from each other, for the lack of a reserve selfhood is almost the same as not having a self at all."[22]

Blecher has suggested that the Roman law did not lack the necessary means to protect individual privacy, although it might have lacked the need to do so.[23] The issue of privacy is not only a concern in South Africa. Bygone times explain that the experience of European countries with the threat posed by the large-scale collection of personal information led to their recognition of this phenomenon as a human rights issue.[24]

---

[21] J Neethling … et al *Law of Personality* 2 ed (2005) 42, 45 and 46.
[22] A C Grayling *Liberty in the Age of Terror: A Defence of Civil Liberties and Enlightenment Values* (2009) 110.
[23] ibid
[24] A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2008) 11 (4) *South African Law Journal* 400.

The right to privacy in South Africa was recognized and protected as a personality interest under the common law.[25] The Constituional Court in *Bernstein v Bester* pointed out that there is an interconnection between common law and the right to privacy under the Constitution as the right to privacy is expressly protected as a fundamental right.[26] Furthermore; the Constitutional Court also emphasized the interdependency between the common law and the constitutional right to privacy.[27]

On the grounds that the right to privacy is expressly protected as a fundamental right under the Constitution of the Republic of South Africa, it is imperative to note that section 2 clearly states that the Constitution is the supreme law of South Africa and any law or conduct inconsistent with it is invalid.[28] Additionally, entrenched within the Constitution of the Republic of South Africa is the Bill of Rights chapter 2,[29] which is applicable to all law, including the common law relating to the right to privacy and it binds not only the organs of the state,[30] but also, if applicable, natural and juristic persons.[31]

Another reason for this study emanates from the fact that computers are now able to store vast amounts of information in the form of raw data, relatively easily, cheaply and for almost indefinite period.[32] The development of new telecommunications technology, linking computers in networks, principally the internet, and enabling the transfer of information between computer systems, has lent impetus to the processing of information which is also referred to as data.[33]

---

[25] See Note 21 above.
[26] Bernstein v Bester 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC) at 787. See Section 14 of the Constitution of the Republic of South Africa, 1996.
[27] *Bernstein v Bester* 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC) at 787.
[28] See Section 2 of the Constitution of the Republic of South Africa, 1996.
[29] See Sections 7 to section 39 of the Constitution of the Republic of South Africa, 1996.
[30] See Section 8 (1) of the Constitution of the Republic of South Africa, 1996.
[31] See Section 8 (2) of the Constitution of the Republic of South Africa, 1996.
[32] S Flaherty 'Surveillance societies' (1992) 2 (1) *Hastings Law Journal* 1321.
[33] ibid 1321.

Now, when they buy, consumers always have a certain degree of risk associated with privacy like profiling, traffic data, cookies and spam (unsolicited commercial e-mails). [34] Consequently, one of the most important factors that help with the gaining of confidence and perception of risk for the consumer is the quality of information security.[35] On this note, the consumer's confidence may tend to be more important in e-commerce than in traditional commerce.[36]

1.3. Research Questions

The dissertation will attempt to answer the following questions:

a) Has there been legislation designed or put forward by the South African legislature to address information security concerns in e-commerce transactions?

b) To what extent does the South African e-commerce legislation impact on the legislature's endeavour to curb privacy protection problems in e-commerce transactions?

c) How are South African organizations and companies employing policy and legal prescriptions for the purposes of enhancing identifiable private information through information security?

d) To what extent are companies (both public and private) or organizations (both public and private) in South Africa, integrating e-commerce privacy protection legal requirements in their policy formulation as well as their policy implementation? and lastly

[34] See Note 10 above at 136.
[35] ibid.
[36] ibid.

e) Are there intermissions in those legislation that have been enacted to address information security problems especially privacy concerns in e-commerce?

1.4. Aims and Objectives

The aim of the dissertation is to analyse the ECTA and other relevant legislation dealing with electronic transactions. This dissertation will seek to identify intermissions in the legislation relating to information protection. The legislation relating to information protection include the Broadcasting Act 4 of 1999, Competition Act 89 of 1998, Constitution of the Republic of South Africa, 1996, Consumer Protection Act 68 of 2008, Copyright Act 98 of 1978, Electronic Communications Act 36 of 2006, Employment Equity Act 55 of 1998, Financial Intelligence Centre Act 38 of 2001, Independent Communications Authority of South Africa Act 13 of 2000, Interim Constitution of South Africa Act 200 of 1993, Merchandise Marks Act 17 of 1941, National Credit Act 34 of 2005, Prevention of Organised Crime Act 121 of 1998, Promotion of Access to Information Act 2 of 2000, Protection of Personal Information Act 4 of 2013, Protection of Personal Information Bill B9 of 2009, Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002, Regulation of Interception of Communications and Provision of Communication-related Information Amendment Act 48 of 2008, Statistics Act 66 of 1976 and the Telecommunications Act 103 of 1996.

Therefore, the overall objectives are as follows:

a) To define electronic commerce;
b) To identify legal issues pertaining to privacy in e-commerce;
c) To identify intermissions in legislation relating to data transmission;
d) To investigate, examine and suggest any reforms to be made to the laws relating to information protection in e-commerce transactions;

e) To examine the legal and policy framework of the proposed law reforms;

f) To make recommendations on how to improve the existing legal framework to suit the ever-changing technology in e-business.

1.5. Methodology

The research for this dissertation is going to be a desktop based one. In pursuit of the aforementioned research objectives, this dissertation will take the form of a qualitative research methodology. Under this approach, the thesis will firstly conduct a descriptive analysis of the history of e-commerce and the legal framework around it in South Africa. Reference will be made to primary sources of law such as legislation and case law relevant to the topic. Secondary sources like journals, text books, and internet sources will also be consulted. Furthermore, the situation in other countries will also be analysed and conclusions will be drawn.

E-commerce has so many advantages in our day to day business because it makes everything convenient for people.[37] With all the advantages that e-commerce has for easy business transactions, literature on e-commerce legislation is still scant because it is a relatively a new area and as such there is meagre case law on the subject.[38]

This dissertation will also refer to articles which have documented the rise of e-commerce in South Africa and other developing countries. In addition, this dissertation will refer to published articles by leading South African academics which discuss the measures that have been put in place and analyse whether those measures have been successful in resolving the issues they were designed to deal with.

---

[37] S Shahriari ... et al 'E-commerce and it impacts on global trend and market' (2015) 3 (4) *International Journal of Research - Granthaalayah* 49.

[38] D K Gangeshwer 'E-Commerce or internet marketing: A business review from Indian context' (2013) 6 (6) *International Journal of u- and e- Service, Science and Technology* 188.

Reference will also be made to certain organizations regulating and dealing extensively with e-commerce at both an international and national level. This dissertation is also going to take the form of a comparative study of different countries' e-commerce law and foreign case law in order to get some insight into, and an understanding of the approach used by other countries in formulating a legal framework to cater for and deal with e-commerce transactions.

Lastly an interpretive approach will be conducted to provide a better understanding of the rise of electronic commerce transactions in South Africa and the legal issues involved pertaining privacy.

1.6. Structure of the Dissertation

Chapter one of this dissertation provides the background information relating to e-commerce. In this chapter, the rationale of the dissertation is discussed. All the aims and the objectives of this dissertation are listed. The purpose for the analysis of the topic is set out, indicating the importance of the dissertation. All the main research questions are posed. These questions reveal the approach that the dissertation follows.

Chapter two provides a descriptive background to what e-commerce is. It examines the various definitions of e-commerce that exist in the business world. The synonyms for e-commerce are given. Chapter two of the dissertation sheds light on the types of e-commerce models that are used in South Africa. The South African regulatory legal framework relating to electronic transactions is discussed. All other relevant legislation that contributes to the discussion later on in the other following chapters is cited. Other aspects dealt with in this chapter are the four main issues in law that are related to electronic transactions in business. A discussion on the international legal perspective on e-commerce concludes the chapter.

Chapter three provides a comprehensive discussion on the data protection laws from an international stand point. The chapter critically analyses the European Union directive dealing with e-commerce. The chapter takes the discussion to consumer concerns in data transmissions. In this chapter the recognition of the right to privacy is discussed. The nature and scope of protection of personal information is examined to see how far this protection of personal information goes. What constitutes an infringement of the right to privacy is also considered and the chapter closes by focusing on the applicability of international law in e-commerce formulation and application in South Africa.

Chapter four focuses its attention on the South African law relating to data protection. The chapter specifically, looks at the ECTA. The Constitution of the Republic of South Africa, 1996 is also analysed in light of e-commerce law formulation and privacy. The chapter also discusses consumer privacy in Protection of Personal Information Act 4 of 2013, the Consumer Protection Act 68 of 2008, the Electronic Communications Act 36 of 2006, the National Credit Act 34 of 2005 as well as the Promotion of Access to Information Act 2 of 2000 as they are the major statutes dealing with information and privacy protection.

Chapter five concentrates on e-commerce in the United Kingdom and the influence it has exerted on the development of South African e-commerce law. This chapter seeks to explore e-commerce in South Africa in relation to the European Law which was already in place. An extensive discussion of the various privacy laws in the United Kingdom is undertaken. Various other legislation with privacy aspects in the United Kingdom is also discussed.

Chapter six describes privacy and data protection in the United States of America. The chapter deals in length with laws governing privacy in the United States of America, particularly laws governing privacy and data protection in relation to e-commerce. The

chapter looks at privacy laws in various States of the United States of America as well as the Federal privacy laws.

Chapter seven is the final chapter of the dissertation and it provides the conclusion and recommendations. This chapter is a summary of the information discussed in the previous chapters and it provides the conclusions of the findings made. In this chapter, the questions set out in chapter 1 of this dissertation are answered. The challenges facing the South African legislature are pointed out and the solutions are also proposed. This chapter provides a comparison between e-commerce as well as privacy and data protection laws in South Africa, the United Kingdom and the United States of America. This chapter identifies areas where South Africa is ahead of the United Kingdom and the United States of America in drafting and implementing e-commerce privacy protection laws and it also indicates areas where the South African e-commerce legislation still has to improve. The way forward is tabulated and the discussion on the rise of electronic commerce transactions in South Africa and the legal challenges pertaining to privacy is completed.

CHAPTER TWO

2. THE DESCRIPTION AND BACKGROUND OF ELECTRONIC COMMERCE

2.1. Introduction

The purpose of this chapter is to provide a brief background to what e-commerce is. It is imperative to understand what e-commerce is before getting into the discussion of its regulatory framework. This discussion is not meant to exhaust all the definitions of e-commerce, but inasmuch as e-commerce is not defined in the ECTA,[1] it is essential to give a simple definition in order to understand the legal challenges facing this type of transaction.

2.2. Electronic Commerce Defined

Since e-commerce is not defined by the ECTA, it does not have a well-accepted definition.[2] There are a number of widely accepted definitions that have been proffered by various organizations and international academic research associations.[3] One of the organizations that defined e-commerce is the Organization for Economic Cooperation and Development which is also known as the OECD.[4] The OECD is a unique forum where the governments of 34 democracies with market economies work with each other, as well as with more than 70 non-member economies to promote economic growth, prosperity, and sustainable development.[5]

[1] S Papadopoulos 'Online consumer protection' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 65.
[2] ibid.
[3] ibid.
[4] ibid 64.
[5] OECD 'What is the OECD? About the OECD' available at https://usoecd.usmission.gov/mission/overview.html, accessed on 28 December 2016.

According to the OECD, e-commerce is an:

> "…electronic transaction which is the sale of goods or services between businesses, households, individuals, governments and other public or private organizations, conducted over computer mediated networks."[6]

The OCED termed this definition of e-commerce as the broad definition of e-commerce because the transaction can take place over the internet or any other electronic medium which is not necessarily the internet.[7] The OECD also gave a narrow definition when it defined e-commerce as an internet transaction and not an electronic transaction.[8] According to the OECD,

> "…an internet transaction is the sale or purchase of goods or services, whether between businesses, households, individuals, governments, and other public or private organizations, conducted over the internet."[9]

In both the broad and the narrow definitions given by the OECD, the goods and services are ordered over those networks, but the payment and the ultimate delivery of the goods or services may be conducted on or off-line.[10]

E-commerce can also be defined as the

> "…use of internet to facilitate, execute, and process business transactions."[11]

---

[6] Z Qin … et al *E-Commerce Strategy* 2 ed (2014) 2. OECD *OECD Guide to Measuring the Information Society* (2011) 72. OECD *OECD Glossary of Statistical Terms* (2008) 167.
[7] OECD *OECD Glossary of Statistical Terms* (2008) 167.
[8] S Grist 'The definition dilemma of e-commerce' in S A Becker (ed) *Electronic Commerce: Concepts, Methodologies, Tools, and Applications* (2008) 2094-2095.
[9] Grist ibid. M Stewart *Encyclopaedia of Developing Regional Communities with Information and Communication Technology* (2005) 154.
[10] OECD *Measuring the Information Economy* (2002) 89. E J Malecki & B Moriset *The Digital Economy: Business Organization, Production Processes and Regional Developments* (2007) 94.

It denotes the seamless application of information and communication technology from its point of origin to its endpoint along the entire value chain of business processes conducted electronically and designed to enable the accomplishment of business goals. It involves exchanges among customers, business partners, and vendors.[12]

The fundamental role of e-commerce is similar to information technology (IT) in that both are tools for facilitating business transactions and communicating information to decision-makers.[13] However, there are significant differences in terms of technical and managerial issues encountered.[14] Information technology mainly focuses on internal functions such as desktop support, data centre, and network operations.[15] On the other hand, e-commerce systems enable an interface between a firm and its customers, and provide another channel to market products and services.[16]

Chaffey went beyond just defining e-commerce as a transaction which involves buying and selling of goods and services.[17] He did not limit his definition to the buying and selling process, but his definition also entails pre-sale and post-sale activities across the chain.[18]

In this dissertation, it is necessary to have a comprehensive definition of e-commerce. Electronic commerce is about doing business electronically and it is based on the electronic processing and transmission of data, including text, sound and video.[19] It encompasses many diverse activities including electronic trading of goods and services, online delivery of digital content, electronic fund transfers, electronic share trading, electronic bills of lading,

---

[11] F Wijnhoven 'The importance of information goods abstraction levels for information commerce process models' (2002) 3 (2) *Journal of Electronic Commerce Research* 40.
[12] ibid.
[13] H Chong, 'Validity of Delone and Mclean's e-commerce model in B2C student loan industry' (2010) 19 (1) *Journal of International Technology and Information Management* 77.
[14] ibid.
[15] ibid.
[16] ibid.
[17] D Chaffey *E-Business and E-commerce Management: Strategy, Implementation and Practice* 4 ed (2009) 5. See also R Kalakota & A Whinston *Electronic Commerce: A Manager's Guide* 3 ed (1997) 69.
[18] Kalakota & Whinston ibid.
[19] R Chakrabarti *The Asian Manager's Handbook of E-commerce* (2002) 33.

commercial auctions, collaborative design and engineering, online sourcing, public procurement, direct consumer marketing, and pre-sale as well as post-sale service.[20]

According to Manzoor, e-commerce refers to the use of electronic means and technologies to conduct commerce (sale, purchase, transfer, or exchange of products, services, and/or information), including within business, business-to-business, and business-to-consumer interactions.[21] He concludes by also pointing out that delivery of the product or service may occur over or outside the internet.[22]

The customer can sell items directly to other customers (for example, customer to customer like eBay online auction business that allows people to auction items they own to other people directly) or as a customer to business organization where online registrations can be performed for products consumers purchase, or as a customer to government organization where individual voters in the United States can contact their governmental representatives directly over the internet.[23]

The business to customer organizations are now able through online registrations, to keep better track of their customers for purposes of product recalls and updates.[24] The business to business organizations can transact product and material purchases, share design specifications for new products, and perform research and development activities all online.[25]

[20] ibid.
[21] A Manzoor *E-Commerce: An Introduction* (2010) 2.
[22] ibid 2. OECD *Measuring the Information Economy* (2002) 89. Malecki & Moriset *The Digital Economy: Business Organization, Production Processes and Regional Developments* (2007) 94.
[23] M J Schniederjans …et al *E-Commerce Operations Management* 2 ed (2013) 4.
[24] ibid 5.
[25] ibid.

2.3. Different Types of Electronic Commerce

As alluded to above, e-commerce can be categorized into four major models. These categories are used to differentiate one e-commerce class from another.[26] These are the business to business (B2B), business to consumer (B2C), consumer to consumer (C2C) and consumer to business (C2B) models.[27] While there are four major models of e-commerce, there are also other minor models of e-commerce.[28] These are the business to administration (B2A) and the consumer-to-administration (C2A) among many others.[29] This dissertation will seek to discuss only the four major models as it is not the main purpose of this document to discuss e-commerce categories.

2.3.1. Business to Business (B2B)

Business to business e-commerce (B2B) describes commercial transactions between businesses, such as between a manufacturer and a wholesaler, or between a wholesaler and a retailer.[30] Contrasting terms are business to consumer (B2C) and business to government (B2G).[31] The volume of B2B transactions is much higher than the volume of B2C transactions.[32] The primary reason for this is that in a typical supply chain there will be many B2B transactions involving sub components or raw materials, and only one B2C transaction, specifically the sale of the finished product to the end customer.[33]

---

[26] C Schulze 'Electronic commerce and civil jurisdiction, with special reference to consumer contracts' (2006) 18 (1) *SA Mercantile Law Journal* 32.
[27] Z Qin *Introduction to E-commerce* (2010) 24.
[28] ibid.
[29] ibid.
[30] S P van Zyl 'Determining the place of supply or the place of use and consumption of imported services for Value-Added Tax purposes: Some lessons for South Africa from the European Union' (2013) 25 (4) *SA Mercantile Law Journal* 535.
[31] ibid.
[32] R Nemat 'Taking a look at different types of e-commerce' (2011) 1 (2) *World Applied Programming Journal* 100.
[33] van Zyl see note 30 above. Nemat 'Taking a look at different types of e-commerce' (2011) 1 (2) *World Applied Programming Journal* 104.

B2B e-commerce, which links businesses in the value chain to each other, enables all manner of commercial and administrative transactions to be conducted over private telecommunications circuits, or over the public internet, much more cheaply and timeously than before.[34] B2B e-commerce is the widespread realization of Electronic Data Interchange (EDI), an effective application of Information Communications Technology (ICT) that has been in existence for many years, but still restricted to a few large companies because of its cost and proprietary nature.[35]

For example, an automobile manufacturer makes several B2B transactions such as buying tires, glass for windscreens, and rubber hoses for its vehicles. The final transaction, a finished vehicle sold to the consumer, is a single B2C transaction. B2B is also used in the context of communication and collaboration.[36] Many businesses are now using social media to connect with their consumers B2C; however, they are now using similar tools within the business so employees can connect with one another.[37]

When communication is taking place amongst employees, this can be referred to as B2B communication.[38] The term 'business to business,' was originally coined to describe the electronic communications between businesses or enterprises in order to distinguish it from the communications between businesses and consumers.[39] It eventually came to be used in marketing as well, initially describing only industrial or capital goods marketing.[40] Today it is widely used to describe all products and services used by enterprises.[41] Many professional

[34] P Esselaar and J Miller 'Towards electronic commerce in Africa: A perspective from three country studies' (2002) 2 (1) *The Southern African Journal of Information and Communication* 2.
[35] ibid.
[36] See Note 32 above.
[37] See Note 30 above.
[38] Schniederjans … et al *E-Commerce Operations Management* 2 ed (2013) 4.
[39] ibid.
[40] ibid.
[41] ibid.

institutions and the trade publications focus much more on B2C than B2B, although most sales and marketing personnel are in the B2B sector.[42]

2.3.2. Business to Consumer (B2C)

Business to consumer (B2C), sometimes also called 'Business to Customer', describes activities of businesses serving end consumers with products and/or services.[43] An example of a B2C transaction would be a person buying a pair of shoes from a retailer.[44] The transactions that led to the shoes being available for purchase, is the purchase of the leather, laces, rubber, etc.[45] However, the sale of the shoe from the shoemaker to the retailer would be considered a B2B transaction.[46]

While the term e-commerce refers to all online transactions, B2C stands for 'business to consumer' and applies to any business or organization that sells its products or services to consumers over the internet for its own use.[47] When most people think of B2C e-commerce, they think of Amazon, the online bookseller that launched its site in 1995 and quickly took on the nation's major retailers.[48] In addition to online retailers, B2C has grown to include services such as online banking, travel services, online auctions, health information and real estate sites.[49]

[42] ibid. Nemat 'Taking a look at different types of e-commerce' (2011) 1 (2) *World Applied Programming Journal* 104.
[43] T Shumba 'Towards an SADC community sales law: Lessons SADC may learn from the proposal for a Common European Sales Law (CESL)' (2015) 27 (3) *SA Mercantile Law Journal* 488.
[44] ibid.
[45] ibid.
[46] See Note 34 above.
[47] See Note 30 above at 541-542.
[48] See Note 32 above.
[49] L Classen 'E-commerce and value added tax' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 115.

Peer to peer sites such as Craigslist also fall under the B2C category.[50] B2C e-commerce involves direct business transactions between individual consumers and supplying companies, such as the purchase of books, or booking cinema tickets over the internet, whether within an African country, or between countries, or internationally.[51] This is the most well-known type of e-commerce relationship, but nowhere near as economically important as the business to business e-commerce.[52]

2.3.3. Consumer to Consumer (C2C)

Consumer to consumer (C2C) or citizen to citizen electronic commerce involves the electronically-facilitated transactions between consumers through some third party. [53] A common example is the online auction, in which a consumer posts an item for sale and other consumers bid to purchase it; the third party generally charges a flat fee or commission.[54] The sites are only intermediaries, just there to match consumers.[55]

They do not have to check quality of the products being offered. C2C marketing is the creation of a product or service with the specific promotional strategy being for consumers to share that product or service with others as brand advocates based on the value of the product.[56] The investment into conceptualizing and developing a top-of-the-line product or

[50] Esselaar & Miller 'Towards electronic commerce in Africa: A perspective from three country studies' (2002) 2 (1) *The Southern African Journal of Information and Communication* 2. Nemat 'Taking a look at different types of e-commerce' (2011) 1 (2) *World Applied Programming Journal* 103.
[51] Nemat ibid at 104.
[52] ibid.
[53] M Geist 'When dot-coms die: The e-commerce challenge to Canada's bankruptcy law' (2002) 37 (1) *Canadian Business Law Journal* 34. Nemat 'Taking a look at different types of e-commerce' (2011) 1 (2) *World Applied Programming Journal* 103. Esselaar & Miller 'Towards electronic commerce in Africa: A perspective from three country studies' (2002) 2 (1) *The Southern African Journal of Information and Communication* 2.
[54] Geist ibid.
[55] ibid.
[56] ibid.

service that consumers are actively looking for is equal to a B2C pre-launch product awareness marketing spends.[57]

This type of e-commerce is expected to increase in the future because it cuts out the costs of using another company.[58] An example cited in Management Information Systems, is of someone having a garage sale to promote their sale via advertising transmitted to the GPS units of cars in the area.[59] This would potentially reach a larger audience than just posting signs around the neighborhood.[60] Since the economic downturn which commenced in 2008, C2C online commerce levels have increased dramatically.[61]

2.3.4. Consumer to Business (C2B)

Consumer to business (C2B) is an electronic commerce business model in which consumers (individuals/ customers) offer products and services to companies and the companies pay them.[62] This business model is a complete reversal of traditional business models where companies offer goods and services to consumers.[63] We can see this example in blogs or internet forums where the author offers a link back to an online business facilitating the purchase of some product like a book on Amazon.com, and the author might receive affiliate revenue from a successful sale.[64]

2.4. The South African Regulatory Legal Framework

The information and communication applications are of paramount concern to the banks in today's business environment and the internet has become the major platform for all

[57] Nemat see Note 53 above.
[58] Manzoor *E-Commerce: An Introduction* (2010) 2.
[59] ibid.
[60] ibid.
[61] ibid. Nemat 'Taking a look at different types of e-commerce' (2011) 1 (2) *World Applied Programming Journal* 100-104.
[62] See Note 58 above.
[63] ibid 3.
[64] Nemat see Note 61 above at 103.

financial, banking and commercial transactions in the present scenario.[65] Statistics show that Africa is lagging behind in the adoption of e-commerce.[66] However, there is some e-commerce activity in Africa, with South Africa, Egypt, Morocco, and Tunisia taking the lead.[67] Most rural areas in Africa, where the majority of small and medium businesses are concentrated, have no internet facilities and thus are unable to engage in e-commerce activities.[68] Most countries in Africa, except South Africa, have internet infrastructure only in their major cities.[69]

Despite the slow diffusion of e-commerce in some countries because of the lack of internet facilities, these countries in general and South Africa in particular, face a different challenge altogether.[70] The greatest challenge in South Africa's e-commerce is its regulation.[71] Issues emanating from e-commerce transactions include among many others, taxation, intellectual property rights, privacy, security and validity of contracts.[72]

Like many other countries and governments, the South African government recognized the need for the formation of e-commerce policy and saw its role as an enabler, facilitator, educator and law enforcer to prevent internet crimes.[73] It was essential that South Africa should develop a policy that is in harmony with international best practice so that it is not

[65] G Worku 'Electronic-banking in Ethiopia- Practices, opportunities and challenges' (2003) 1 (2) *Journal of Internet Banking and Commerce* 3
[66] ibid.
[67] ibid.
[68] ibid.
[69] ibid.
[70] S Papadopoulos 'An introduction to cyberlaw' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 3. C Cupido 'Electronic communications regulation' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 25-26.
[71] Papadopoulos ibid 3.
[72] Cupido see Note 70 above at 26.
[73] N Zantsi & M Eloff 'Guide to South African law' (2003) available at http://icsa.cs.up.ac.za/issa/2003/Publications/001.doc/, accessed on 20 December 2016.

excluded from trading electronically with the global world.[74] South Africa therefore monitored developments and followed debates that were taking place around the world.[75]

Legislation was then put in place in South Africa to protect consumers.[76] The Consumer Protection Act (CPA) is one of the latest of these pieces of legislation dealing with consumer protection.[77] The CPA provides for an overarching legislative and institutional framework for consumer protection and all other Acts of parliament providing for consumer protection must be read with the CPA to provide a common standard for consumer protection.[78]

Issues of particular concern range from questions regarding consumer's financial security, data protection, protection from unsolicited information, access to adequate information, and availability of effective and affordable redress mechanisms.[79] To specifically address the electronic related commerce, the ECTA was enacted.[80]

The ECTA comprises 14 chapters with 95 sections, which address e-commerce issues such as e-government, consumer protection, privacy, cyber-crime, and liabilities of service providers, to mention a few.[81] The objective of the ECTA is to facilitate electronic transactions by creating legal confidence around such transactions through helping customers to do electronic commerce transactions without any fear of their right to privacy being infringed upon.[82]

---

[74] ibid.
[75] ibid.
[76] See, for instance, the National Credit Act, Act 34 of 2005; the Promotion of Access to Information Act, Act 2 of 2000; the Competition Act, Act 89 of 1998 and the ECTA, 25 of 2002.
[77] Consumer Protection Act 68 of 2008.
[78] Cupido see note 70 above at 27.
[79] J Huffmann 'Consumer protection in e-commerce: An examination and comparison of the regulations in the European Union, Germany and South Africa that have to be met in order to run internet services and in particular online-shops' (unpublished LLM thesis, University of Cape Town, 2004) 4.
[80] See Note 5 above.
[81] ibid.
[82] Deloitte & Touche Legal 'Electronic Communications & Transaction Bill 2002. (South Africa)' (2002) available at http://www.doc.pwv.gov.za/, accessed on 20 December 2016.

The Broadcasting Act 4 of 1999 deals with broadcasting policy and regulation, as well as with the public broadcaster.[83] The Independent Communications Authority of South Africa Act 13 of 2000 (ICASA Act) was created for the purposes of establishing an independent Authority which created a unified regulator for both broadcasting and telecommunications.[84] The ICASA Act and the ECTA both provide primarily for the regulation of the electronic communications sector.[85]

The Regulation of Interception of Communications and Provision of Communication-related Information Amendment Act 48 of 2008 (RICA)[86], deals with the circumstances under which electronic surveillance and interception are permitted, as well as related procedures and responsibilities.[87] In August 2009, the Protection of Personal Information Bill B9 of 2009 (PPI) was published.[88] The PPI is now the Protection of Personal Information Act 4 of 2013 (POPI) which came into force on 11 April 2014. It also promotes the protection of personal information by public and private bodies.[89]

These amongst the other legislative reforms culminated in the enactment of the ECTA, which provides a legal framework for electronic transactions dealing with cryptography, cyber-crime and the protection of privacy.[90]

The ECTA places computer generated documents on the same footing as traditional paper evidence.[91] The ECTA contains minimalist enabling provisions on contract formation and

[83] Broadcasting Act 4 of 1999.
[84] Independent Communications Authority of South Africa Act 13 of 2000.
[85] Cupido see Note 70 above at 27.
[86] Regulation of Interception of Communications and Provision of Communication-related Information Amendment Act 48 of 2008.
[87] Cupido see Note 70 above at 27.
[88] ibid.
[89] Personal Information Act 4 of 2013.
[90] Z N Jobodwana 'E-commerce and mobile commerce in South Africa: Regulatory challenges' (2009) 4 (4) *Journal of International Commercial Law and Technology* 291.
[91] See Section 11 (1) and Section 12 of the Electronic Communications and Transactions Act 25 of 2002.

seeks to remove legal barriers to e-commerce in South Africa, by providing for functionally equivalent rules for electronic contracting.[92]

These legislative reforms resulted in the adoption of the Electronic Communications Act 36 of 2006 (ECA).[93] The ECA is the primary piece of legislation governing the substantive regulation of the electronic communications industry in South Africa.[94] The ECA regulates the convergence of technologies in the ICT sector.[95] The ECA repealed the Telecommunications Act 103 of 1996,[96] as well as some sections of the Broadcasting Act 4 of 1999,[97] excluding sections dealing with the public broadcaster.[98] The ECA seeks to promote convergence in the broadcasting, broadcasting signal distribution and telecommunications sectors, and to provide the legal framework for convergence of these sectors.[99]

Another very important piece of legislation to consider for the purposes of this dissertation is the Constitution of the Republic of South Africa.[100] The Constitution of the Republic of South Africa states that:

> "…this Constitution is the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled."[101]

Accordingly, the electronic communication and e-commerce industries are subject to the provisions of the Constitution. The two important provisions are Section 16 (1)[102] which

[92] See Note 90 above at 292.
[93] Electronic Communications Act 36 of 2006.
[94] See Note 85 above.
[95] ibid.
[96] Telecommunications Act 103 of 1996.
[97] Broadcasting Act 4 of 1999.
[98] Cupido see Note 70 above at 25.
[99] See Note 90 above.
[100] The Constitution of the Republic of South Africa, Act 108 of 1996.
[101] See Section 2 of the Constitution of the Republic of South Africa, 1996.

includes the freedom of expression and section 14 (*d*)[103] which provides for the right to privacy.[104]

Legal impediments to the implementation of electronic commerce have to be removed from legislation.[105] Certainty has to be achieved as to the application of the law to electronic commerce and business and consumer trust has to be enhanced.[106] Costs and legislation need to be minimized. Legislation has to be applied to a wide range of transactions, facilitating both related and unrelated transactions.[107] Regulatory burdens upon government and business must be minimized.[108] Legislation also has to facilitate the cross-border recognition and enforcement of electronic transactions and signatures.[109]

The ECTA addressed four main issues in law that are related to electronic transactions in business and these aspects are:

- Formation and validity of contracts;
- Jurisdictional aspects;
- The role of electronic signatures; and
- Protection of consumers.

These four aspects will be discussed briefly below. For the purposes of this dissertation, only the fourth element will be the point of focus in the following chapters.

2.4.1. Formation and Validity of E-Contracts

An agreement is not without legal force and effect merely because it was concluded partly or

---

[102] See Section 16 (1) of the Constitution of the Republic of South Africa, 1996.
[103] See Section 14 (*d*) of the Constitution of the Republic of South Africa, 1996.
[104] Cupido see Note 70 above at 25.
[105] L R Francois 'E-commerce: the legal framework' (2000) 1 (1) *De Rebus* 25.
[106] ibid.
[107] ibid.
[108] ibid.
[109] ibid 26.

in whole by means of data messages.[110] Section 11 of the ECTA recognizes the legal status of electronic data.[111] Section 13 of the ECTA deals with digital signatures, and specifies that an electronic signature generally satisfies the legal requirement of a contract, unless it is otherwise specified.[112]

The ECTA also further states that an agreement concluded between parties by means of data messages is concluded partly or in whole by means of data messages at the time when and again at the place where the acceptance of the offer was received by the offeror.[113]

There are four different ways of e-contracting.[114] The first and most important method of contracting on the internet is similar to a negotiation of one or more infrequent transactions by exchange of letters and documents.[115] This is known as e-mail contract.[116] In this method, the parties can exchange e-mails and even attachments setting out the terms and conditions of their contract in detail.[117] This is quite similar to offer and acceptance between the parties.[118]

The second method is known as contracting on the World Wide Web (www) and this way is similar to a mail order.[119] In this method, one party maintains the website on which he advertises his goods and services.[120] The prospective buyer accesses the website and then completes an electronic form, whereby he orders goods or services from the seller.[121]

---

[110] See Section 22 of the Electronic Communications and Transactions Act 25 of 2002
[111] See Section 11 (1) of the Electronic Communications and Transactions Act 25 of 2002.
[112] See Section 13 (1)-(5) of the Electronic Communications and Transactions Act 25 of 2002.
[113] See Section 22 (1) and (2) of the Electronic Communications and Transactions Act 25 of 2002. L Snail 'Electronic contracts in South Africa: Comparative analysis' in Kierkegaard (ed) *Business and Law: Theory and Practice* (2008) 307-328. Jobodwana 'E-commerce and mobile commerce in South Africa: Regulatory challenges' (2009) 4 (4) *Journal of International Commercial Law and Technology* 291.
[114] S Snail 'Electronic contracts in South Africa - A comparative analysis' (2008) 2 (1) *Journal of Information, Law & Technology* 4.
[115] ibid.
[116] ibid.
[117] ibid.
[118] ibid.
[119] T Pistorius 'Formation of internet contracts: Contractual and security issues' (1999) 11 (1) *SA Mercantile Law Journal* 281.
[120] ibid.
[121] ibid.

The third way is where the parties trade under the framework of an Electronic Data Interchange Agreement. The EDI can be defined as computer to computer transmission of data in a standardized format. The EDI enables businesses to exchange documents over either the internet or their private networks.[122] Private networks EDI is used by large businesses when buying goods but smaller businesses and individuals prefer to use the EDI as it reduces costs.[123] This is the primary electronic commerce medium; it is only applicable and valid between the contracting businesses that have assented to it.[124]

Despite the recognition of different forms of expressing one's intent to be contractually bound by electronic means, uncertainty still exists as to whether a click on an icon on the website of a vendor would constitute a legally recognizable act signifying ones intent to be contractually bound as such where terms were unilaterally imposed.[125]

2.4.2. Jurisdictional Aspects

Online transactions may routinely involve several jurisdictions. For example, a person in state A may make a communication through a computer located in state B, received by a person in state C through a server located in state D, owned and operated by a company headquartered in state E, that results in shipment of physical goods from a source located in state F.[126] The jurisdictional aspect covered by the ECTA is also not that unproblematic. Section 22 (2)[127] of the ECTA provides that the place of the contract is the place where the acceptance of the offer is received. Section 23 (*c*)[128] of the ECTA also states that a data message must be regarded as having been received at the addressee's usual place of business or residence. In

[122] J Shim … et al *The International Handbook of Electronic Commerce* 3 ed (2000) 141.
[123] S G Nagalingam 'The enforceability of computer contracts' (unpublished LLB thesis, University of Pretoria, 2000) 6.
[124] See Note 114 above.
[125] See Note 119 above at 293.
[126] J Rothchild 'Protecting the digital consumer: the limits of cyberspace utopianism' (1999) 74 *Indiana Law Journal* 893–989.
[127] See section 22 (2) of the Electronic Communications and Transactions Act 25 of 2002.
[128] See section 23 (*c*) of the Electronic Communications and Transactions Act 25 of 2002.

an on-line contract then, through a computer network it will mean that an acceptance by a customer where the data message is sent to the dealer (assuming that he is the offeror), the place of the contract will be where the dealer is deemed to have received the message which, in terms of the ECTA is dealer's usual business address.[129]

In e-commerce, e-mail use has become prevalent. The ECTA now clarifies the position. The place of a contract will be where the contract was concluded by means of email, which is, the dealer's (offeror's) usual place of business.[130] Where an offer is in writing and the acceptance is by means of email one can also assume that the place of the contract will be the usual place of business or residence of the offeror.[131]

With mobile phones being web enabled, the World Wide Web can be reached by the users anywhere and at any time.[132] Instead of the web page being viewed on the regular desktop, the WAP cell-phone can facilitate one surfing the web in the palm of his or her hand with facilities of telephone conferences, e-mail messaging and the convenience of conducting business in any country. The ECTA does not provide for this type of situation.[133]

Furthermore, the basic principles of jurisdiction are essentially geography-based. As a result, jurisdictional principles are difficult to apply to the internet, which is a largely boundless medium.[134] A website may be viewed from anywhere in the world; the actual location of computers is irrelevant to either the providers or recipients of the information; and there is no necessary connection between the internet address and a physical location.[135]

In other words, legislation has not kept pace with the new technology and its

[129] See Note 90 above at 293.
[130] See Chapter III of the Electronic Communications and Transactions Act 25 of 2002.
[131] ibid.
[132] See Note 90 above at 293.
[133] ibid.
[134] ibid.
[135] A Aladwan 'A cyber-consumer protection framework for prevention of online deceptive advertising' (unpublished LLM thesis, Curtin University 2012) 53.

consequences.[136] The controlling minds behind these events, however, necessarily remain at specific points in real space, a fact no doubt behind the European Union's (EU) position that,

> "The Convention focuses on the substance of transactions, as opposed to their form".[137]

The conclusion drawn from this observation is that:

> "…the rules of jurisdiction pre-date the personal computer age courts and regulators. The internet is a serious issue because the internet of today is a glimmer of what lies ahead".[138]

2.4.3. The Role of Electronic Signatures

The movement from a traditional way of doing business to a one that is technology based also brought about some significant changes relating to how contracts will be signed. The ECTA has a provision for how an electronic contract should be signed.[139] An "electronic signature" is defined as

> "…data attached to, incorporated in or logically associated with other data which is intended by the user to serve as a signature."[140] "…an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form"[141]

There exists a range of electronic authentication methods, of varying degrees of security and reliability, for a person to authenticate an electronic communication.[142] The ECTA states that where the signature of a person is required by law and such law does not specify the type of

[136] ibid.
[137] J Dickie *Internet and Electronic Commerce Law in the European Union* (1999) 32.
[138] Aladwan see Note 135 above.
[139] See section 13 of the Electronic Communications and Transactions Act 25 of 2002.
[140] See section 13 (2) of the Electronic Communications and Transactions Act 25 of 2002.
[141] See section 1 of the Electronic Communications and Transactions Act 25 of 2002.
[142] See Note 90 above at 293.

signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.[143]

The Act further states that an electronic signature is not without legal force and effect. A contract is not rendered invalid merely on the grounds that the signature in it is in its electronic form.[144] These points were raised in *Spring Forest Trading v Wilberry (Pty) Ltd t/a Ecowash & Another*.[145]

The Supreme Court of Appeal (SCA) stated that, an electronic signature as contemplated in section 13 (3), was defined in ECTA 'as data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature'.[146] Put simply, so long as the data in an email was intended by the user to serve as a signature and was logically connected with other data in the email, the requirement for an electronic signature was satisfied.[147]

2.4.4. Protection of Consumers

Providers of goods and services are obliged to make certain information available to consumers on websites where such goods or services are offered.[148] The particular information required includes: the merchant's full name and legal status; physical address and telephone number; security procedures, policies and any code of conduct that the merchant subscribes to; and the manner of payment and the full price of goods or services, including transport costs, taxes and any other fees or costs.[149]

[143] See section 13 (1) of the Electronic Communications and Transactions Act 25 of 2002.
[144] See section 13 (2) of the Electronic Communications and Transactions Act 25 of 2002.
[145] *Spring Forest Trading v Wilberry (Pty) Ltd t/a Ecowash* 2015 (2) SA 118 (SCA) at paras 26-28.
[146] ibid.
[147] ibid.
[148] See Note 90 above at 294.
[149] ibid.

The facelessness and anonymity of contracting parties and concerns about confidentiality and security of electronic transactions are some of the factors that prevent consumers from fully trusting and fully using e-commerce over the internet.[150]

There are certain transactions that are excluded from the ambit of the legislation. Included in the list of excluded electronic transactions are: financial services, insurance and reinsurance operations, banking services and operations relating to dealings in securities; auctions; the supply of foodstuffs, beverages or other goods intended for everyday consumption; and; transactions where the price for the supply of goods or services is dependent upon fluctuations in the financial markets and which cannot be controlled by the supplier.[151]

There has been a rapid increase in the use of e-commerce in South Africa; hence the need to develop legislation that would provide security to internet consumers and merchants.[152] South African common law was not sufficiently addressing issues related to the security of electronic transactions.[153] It is for the purpose of consumer protection then that the ECTA was drafted and adopted.[154]

E-commerce has placed a greater focus on the consumer since the most important factor when conducting business is to satisfy the customer's needs.[155] Well-developed e-commerce websites offer an array of information on products and services.[156] They allow customers to access any information any time and from anywhere.[157] The most important features of an e-

[150] C Ulrich 'Consumer protection in e-commerce: Germany and the United States' (2000) 4 (5) *Journal of Internet* 6.
[151] See Note 90 above at 294.
[152] D Goodburn & M Ngoye 'Privacy and the internet' in R Buys & F Cronje (eds) *Cyberlaw: The Law of the Internet in South Africa* 3 ed (2004) 97
[153] ibid.
[154] ibid.
[155] N J Lightner 'What users want in e-commerce design: Effects of age, education and income' (2003) 46 (1) *Ergonomics* 158-159.
[156] ibid.
[157] ibid 160.

commerce experience for customers are security, information quality, and information quantity.[158]

2.5. The International Legal Perspective on E-Commerce

Paper documents have been the basis for rules on form and evidence of legal acts in most countries.[159] As electronic records promise to displace most of the paper currently being used, lawmakers around the world are moving to adapt legal rules to modern technologies. These measures require adequate international harmonization to avoid the creation of barriers to international e-commerce through conflicting domestic standards.[160]

Initially in the new age of technology and globalisation, there was legal uncertainty worldwide as to how or whether or not contracts concluded by electronic means could or should be recognized as valid and enforceable agreements.[161] As a global organization, the United Nations Commission on International Trade Law (hereafter UNCITRAL) was chosen to propose uniform private law standards for e-commerce.[162] Several factors suggested that what were required were international solutions, rather than individual State initiatives.[163]

Those factors included the transnational nature of e-commerce, and its disregard for traditional jurisdictional borders, together with the lack of domestic laws dealing with e-commerce.[164] The conclusion in favour of international harmonization was the logical

[158] ibid.
[159] J A E Faria 'E-commerce and International Legal Harmonization: Time to go beyond functional equivalence?' (2004) 16 *SA Mercantile Law Journal* 529.
[160] ibid.
[161] Snail 'Electronic contracting in South Africa (e-contracting)' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 41.
[162] ibid.
[163] ibid.
[164] See Note 159 above.

approach for dealing with the legal implications of technological developments as a result of which, as it has been said, 'markets are migrating from geographic space to cyberspace.'[165]

The UNCITRAL was established by the General Assembly of the United Nations in 1966 with the general mandate to promote harmonization and unification of international trade law. In 1996 the United Nations created the model law on e-commerce which is known as the UNICTRAL Model Law on E-commerce.[166] In 2001, the United Nations also created the UNICTRAL Model Law on E-Signatures.[167] The UNICTRAL currently has 60 Member States elected by the General Assembly.[168] Membership is structured so as to be representative of the world's various geographic regions and its principal economic and legal systems.[169]

Members of the Commission are elected for terms of six years, the terms of half the members expiring every three years.[170] In addition to Member States, all other states and invited international organizations may participate as observers in the work of the Commission.[171] The UNCITRAL has implemented its mandate by developing texts on a number of topics including sale of goods, arbitration and conciliation, carriage of goods by sea, banking and finance law, procurement, cross-border insolvency, and e-commerce.[172]

2.5.1. The UNCITRAL Model Law: Background

The decision by the UNCITRAL to formulate model legislation on electronic commerce was taken in response to the fact that in a number of countries the existing legislation governing

[165] ibid.
[166] United Nations Commission on International Trade Law 'UNICITRAL Model Law on Electronic Signatures' available at http://www.uncitral.org/uncitral/en/commission/sessions/29th.html, accessed on 19 January 2017.
[167] ibid.
[168] United Nations Commission on International Trade Law 'About UNICITRAL' available at www.uncitral.org/uncitral/en/about_us.html, accessed on 19 January 2017.
[169] ibid.
[170] ibid.
[171] ibid.
[172] ibid.

communication and storage of information is inadequate or out-dated because it does not contemplate the use of electronic commerce.[173] The lack of legislation in many countries in dealing with E-commerce as a whole results in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper document.[174]

Inadequate legislation at the national level will inevitably create obstacles to international trade.[175] The purpose of Model law was to offer national legislators a set of internationally accepted rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for what has become known as electronic commerce.[176]

The UNCITRAL model law seeks to permit States to adapt their domestic legislation to developments in communications technology applicable to trade law without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements.[177] The Model law thus relies on a new approach known as the 'functional equivalent' approach which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view of determining how those purposes or functions could be fulfilled through electronic commerce techniques.[178]

2.5.2. Global E-Commerce and Standardisation Issues

Standardization is commonly defined in the literature as a strategy wherein marketers assume global homogeneous markets and in response offer standardized products and services using

[173] Abhilash 'E-Commerce Law in developing countries: An Indian perspective' (2002) 11 (3) *Information & Communication Technology Law* 269.
[174] ibid.
[175] ibid.
[176] ibid 270.
[177] Abhilash see Note 173 above. See also Snail 'Electronic contracting in South Africa (e-contracting)' in S Papadopoulos & S Snail (eds) Cyberlaw *@ SA III: The Law of the Internet in South Africa* 3 ed (2012) 42.
[178] See Note 173 above.

a standardized marketing.[179] Scholars in favour of the standardization approach argue that as technology develops and is globally dispersed, cultural distance is minimized, leading to convergence of national cultures into a homogenous global culture. Hence, there is little need to adopt a locally adaptive approach to the marketing.[180] This is what led to the formation of the e-commerce model law.

The advantages that are associated with standardization have been addressed in the existing literature from various perspectives.[181] Most authors argue that the forces of technology and globalization are creating homogenized consumer markets and marketers should use standardized marketing to attract these global consumers. Additionally, standardization seems to be an economical strategy for marketers as it leads to leveraging the same template/product or service marketing mix configuration globally. This leads to economies of scale. By leveraging their home country site for all countries; multinational firms can significantly reduce localization expenses.[182]

Standardization can also lead to the development of a single and unified brand and corporate identity worldwide. This can lead to better global recognition and can provide global competitive advantage. Standardization can lead to having a rationalized product line which comprises only a few core global brands instead of multiple localized brands and brand extensions in numerous countries.[183]

This could potentially lead to better allocation of resources, higher efficiencies, homogenized marketing and higher profits. Hence, in the context of e-commerce, the cost and effort of

[179] H S Alhorr …et al 'E-Commerce on the global platform: Strategic insights on the localization-standardization perspective' (2010) 11 (1) *Journal of Electronic Commerce Research* 7.
[180] ibid.
[181] ibid.
[182] ibid.
[183] ibid.

maintaining a single global website can be significantly less than maintaining several different multilingual sites due to lower resource allocation and marketing requirements.[184]

Due to these standardization ideas, choice of a model law on e-commerce was the ultimate global agreement.[185] The UNCITRAL focused its work on promoting the modernization of statutory requirements that existed under domestic law.[186] The United Nations sought to harmonise all the e-commerce laws that existed at that time into one giant law that would drive e-commerce on a global scale.[187]

2.5.3. Influence of the UNCITRAL Model Law

When it was completed, the Model Law was a unique instrument in a legal landscape where there was no existing body of law, whether uniform international law or national law that comprehensively addressed the issues raised by e-commerce.[188] As such, the UNCITRAL Model Law could be described as an instrument of 'preventive' or 'pre-emptive' harmonization: it led the process of development of law by providing universally acceptable solutions to the issues likely to arise, rather than being negotiated after practices and usage had already resulted in disparate laws and regulations.[189]

The UNICITRAL Model Law is very much in use in the South African Courts. In *Jafta v Ezemvelo KZN Wildlife*[190] in which Jafta responded to an advert using a Short Message Service (SMS) and Electronic mail (e-mail), the court used the UNICITRAL Model Law to

[184] ibid.
[185] ibid.
[186] ibid.
[187] ibid.
[188] See Note 159 above at 531.
[189] ibid.
[190] *Jafta v Ezemvelo KZN Wildlife* (2009) 30 *ILJ* 131 (LC) at para 30.

determine if Jafta's communications constituted a valid acceptance of the offer or not and if an SMS is an appropriate mode of concluding a contract.[191]

The court held that both Jafta's SMS and e-mail were valid acceptances.[192] First, the acceptances in both modes were clear, unequivocal and unambiguous as stated in *Boerne v Harris*[193] and second, both acceptances corresponded with the offer.[194]

The challenge was to bring together countries of divergent economic capabilities, legal heritage, and telecommunications infrastructures to develop common analyses of, and approaches to, new legal problems.[195] That the challenge was successfully met can be gauged from the influence of the UNCITRAL Model Law on e-commerce legislation already adopted, or being developed, around the world.[196]

2.6. To What Extent Can Foreign Law Assist South Africa's Regulation of Online Electronic Transactions?

E-commerce in South Africa is growing at a rate matched only by the growth experienced in the United States of America (USA) and the United Kingdom (UK).[197] To ensure global compatibility with other international markets, the South African legislature largely modelled the South African data protection legislation on the comparative legislation enacted by these two nations (that is, the USA and the UK).[198]

---

[191] P Stoop 'SMS and e-mail contracts: Jafta v Ezemvelo KZN Wildlife' (2009) 21 (1) *SA Mercantile Law Journal* 110. *Jafta v Ezemvelo KZN Wildlife* (2009) 30 *ILJ* 131 (LC) at para 30.
[192] Buys & F Cronje (eds) *Cyberlaw @ SA II: The Law of the Internet in South Africa* 2 ed (2004) 104. *Jafta v Ezemvelo KZN Wildlife* (2009) 30 *ILJ* 131 (LC) at para 113.
[193] *Boerne v Harris* 1949 (1) SA 793 (A) at 799.
[194] Stoop see Note 192 at 116.
[195] See Note 159 above at 531.
[196] ibid.
[197] J Jansen 'A new era for e-commerce in South Africa' (2002) 416 *De Rebus* 17.
[198] ibid.

The right to privacy is expressly guaranteed in a number of international and regional conventions.[199] Although the African Charter on Human and Peoples' Rights does not expressly recognize the right to privacy, it does however give reference to dignity.[200]

The Universal Declaration of Human Rights 1948 (UDHR),[201] the American Convention on Human Rights 1969 (ACHR),[202] the International Covenant on Civil and Political Rights 1976 (ICCPR)[203] as well as many other international and regional treaties regard privacy as a fundamental human right.[204] In most countries in the world, the right to privacy is also recognized and in nearly every country's Constitution it is entrenched.[205] In some countries where this right is not entrenched in the Constitution, it is found in other pieces of legislation of that country or the International Covenant on Civil and Political Rights 1976 (ICCPR) or the European Convention on Human Rights 1953 (ECHR)[206] and it is adopted as binding law.[207]

This dissertation will therefore (in chapter 5 and chapter 6) seek to identify points on which the foreign law dealing with the regulation of online electronic transactions came short in achieving the same, so that South Africa can avoid the same shortfalls. The comparison of the South African regulation of online electronic transactions with those of foreign countries will

[199] D Banisar & S Davies 'Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments' (1999) 18 (1) *Journal of Computer & Information Law* 3.
[200] See Article 5 of the African Charter on Human and Peoples' Rights 1998.
[201] See Article 12 of the Universal Declaration of Human Rights 1948. The Universal Declaration of Human Rights (UDHR) is a declaration adopted by the United Nations General Assembly on 10 December 1948 at the Palais de Chaillot in Paris, France.
[202] See Article 9 of the American Convention on Human Rights 1969.
[203] See Article 17 of the International Covenant on Civil and Political Rights 1976. The International Covenant on Civil and Political Rights (ICCPR) a multilateral treaty adopted by the United Nations General Assembly on 16 December 1966, and in force since 23 March 1976.
[204] See Note 199 above.
[205] ibid.
[206] See Article 8 of The European Convention on Human Rights 1953. The European Convention on Human Rights (ECHR) (formally the Convention for the Protection of Human Rights and Fundamental Freedoms) drafted by the Council of Europe in 1950 and adopted in 1953.
[207] See Note 199 above.

also help South Africa adopt useful regulations that have worked well in foreign jurisdictions and leave out those that didn't. To this end, two foreign jurisdictions will be analysed.

2.7. Conclusion

This chapter defined e-commerce in its broader definition as not just the buying, selling of goods & services but also servicing customers, collaborating with business partners, conducting e-learning & processing electronic transactions. It also pointed out the different types of e-commerce that exists in South Africa. This was a critical discussion because regulation set to deal with e-commerce must not just be sector specific, but must also address the very type of e-commerce being used by and business at any point.

CHAPTER THREE

3. CONSUMER CONCERNS IN DATA TRANSMISSIONS AND PRINCIPLES OF INFORMATION PROTECTION

3.1. Introduction

In the early days of e-commerce in the developed economies, there was much commentary about supplier reliability (the major e-malls and brand names prevailed), privacy of information (credit card fraud was the topic of the day), and the "World Wide Web" as a result of slow telecommunication links.[1] Those concerns have greatly diminished and e-commerce has matured in the major developed nations, but this is far from the case in the developing world and especially Africa.[2]

More specifically, due to the increase in electronic commerce and other electronic transactions, the information society has created and facilitated e-commerce whereby businesses and consumers conduct the majority of their everyday transactions via the internet.[3] These transactions via the internet have data which must be protected.[4]

Data protection is an aspect of safeguarding a person's right to privacy. It provides for the legal protection of a person (the data subject) in instances where such a person's personal particulars (i.e. information) are being processed by another person or institution (the data user).[5] Processing of information generally refers to the collecting, storing, using and communicating of information.[6]

---

[1] Esselaar and Miller 'Towards electronic commerce in Africa: A perspective from three country studies' (2002) 2 (1) *The Southern African Journal of Information and Communication* 2.
[2] ibid.
[3] B Fitzgerald … et al *Internet and e-Commerce Law: Technology, Law and Policy* (2007) 13. S Papadopoulos 'An introduction to cyberlaw' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 1.
[4] Fitzgerald … et al ibid at 13.
[5] The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 9.
[6] ibid 2.

In *Helen Suzman Foundation v Judicial Service Commission*, the main issue was whether the confidentiality considerations insulated the Judicial Service Commission's deliberations in which the court stated that confidentiality does not by itself confer privilege against disclosure.[7] The main issues were that the Judicial Service Commission (JSC) was stifling the candour and rigour of the deliberations, deterring potential applicants, harming the dignity and privacy of candidates who applied with the expectation of confidentiality of the deliberations that would generally hamper effective judicial selection.[8]

3.2. The Importance of the Right to Privacy in E-commerce

Today's transactions in e-commerce typically require the divulgence of large amounts of personal information and this necessary information includes credit card information and delivery details.[9] The possession of such information gives e-business the opportunity to analyze it, discovering trends and increasing the efficiency of their business dealings.[10]

There is a growing consensus that if the jumble of statutes, consumer pressure, and self-help is to be unified into meaningful privacy protection in the digital age, then we will have to do more than pass a law.[11] The law in general and each of us in particular, will have to make some fundamental changes in the way we think of personal information and electronic communication.[12]

Consumers typically had no idea as to the range of possible uses that possession of this information allowed for, and thus had no idea as to the possible violation of their privacy that could occur. However, in the last decade, consumer awareness of privacy is increasing,

---

[7] *Helen Suzman Foundation v Judicial Service Commission* 2017 (1) SA 367 (SCA) at para 39.
[8] ibid.
[9] M Guo 'A comparative study on consumer right to privacy in e-commerce' (2012) 3 (1) *Modern Economy* 403.
[10] ibid.
[11] E Aldermann & C Kennedy *The Right to Privacy* (1997) 332.
[12] ibid.

particularly among the internet users.[13] They are beginning to demand that their privacy be respected by electronic commerce, which requires the legislation of e-commerce consumer rights protection.[14]

The concept of privacy is highly interesting.[15] Perhaps its most striking feature is the fact that there is no agreement upon what it actually is.[16] A suitable definition of privacy has always been the topic of much debate in scholarly literature.[17] Neethling describes privacy as a personality interest and in turn a personality interest as a non-patrimonial interest that cannot exist separately from the individual.[18]

The right of privacy[19] in South Africa is protected by the Constitution.[20] The recognition and protection of the right to privacy as a fundamental human right in the Constitution provides an indication of its importance.[21] Privacy is a valuable and advanced aspect of personality and sociologists and psychologists agree that a person has a fundamental need for privacy.[22]

In *Financial Mail (Pty) Ltd v Sage Holdings Ltd*[23] and *Janit v Motor Industry Fund Administrators (Pty)* Ltd,[24] it was shown that over the years, the remedy for invasion of privacy in South Africa has even been extended to protect a juristic person's confidential sphere. Section 8(4) of the Constitution states that a juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of the juristic person.[25] In *Hyundai Motor Distributors (Pty) Ltd v Smit*,[26] it was also pointed out

[13] ibid.
[14] ibid.
[15] ibid.
[16] ibid.
[17] J Neethling … et al *Neethling's Law of Personality* 2 ed (2005) 18.
[18] ibid 14.
[19] See Section 14 of the Constitution of the Republic of South Africa, 1996.
[20] The Constitution of the Republic of South Africa 108 of 1996.
[21] See Note 17 above at 219-220.
[22] ibid 29.
[23] *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) at 460G-I and 461-2.
[24] *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 (4) SA 293 (A) at 60.
[25] See Section 8 (4) of the Constitution of the Republic of South Africa, 1996.

that because juristic persons are not bearers of human dignity, their privacy rights may be attenuated.[27]

The recognition of the right to privacy is deeply rooted in history.[28] Psychological and anthropological evidence suggest that every society, even the most primitive, adopts mechanisms and structures that allow individuals to resist encroachment from other individuals or groups.[29] Since the right to privacy is deeply rooted in our history, it is also part of our common law.[30] Neethling also pointed out that the right to privacy is also entrenched in our common law.[31] In *Bernstein v Bester*, as pointed out in chapter one of this dissertation, the Constitutional Court emphasized the interdependency between the common law and constitutional right to privacy.[32]

In terms of the common law every person has personality rights such as the right to privacy, dignity, good name and bodily integrity as stated in *Stoffberg v Elliot;*[33] *Lymbery v Jefferies*;[34] *Lampert v Hefer*[35] and in *Esterhuizen v Administrator, Transvaal*.[36]

Worldwide the internet has become a key instrument for communication and for exercising the right to freedom of expression in the form of writing, audio and video.[37] The right to freedom of expression which is entrenched in section 16 of the Constitution[38] includes not

---

[26] *Hyundai Motor Distributors (Pty) Ltd v Smit* 2001 (1) SA 545 (CC) at para18.
[27] J Burchell 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* 8.
[28] A Roos 'The law of data (privacy) protection: A comparative and theoretical study' (unpublished LLD dissertation, University of South Africa 2003) 545.
[29] ibid 545. The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 3.
[30] The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 3.
[31] Neethling … et al *Neethling's Law of Personality* 2 ed (2005) 51. The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 3.
[32] *Bernstein v Bester* 1996 (2) SA 751 (CC) at 787.
[33] *Stoffberg v Elliot* 1923 CPD 148 at 149-150.
[34] *Lymbery v Jefferies* 1925 AD 236 at 240.
[35] *Lampert v Hefer* 1955 (2) SA 507 (A) at 508.
[36] *Esterhuizen v Administrator, Transvaal* 1957 (3) SA 710 (T) at 718-722.
[37] S Nel 'Freedom of expression, anonymity and the internet' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 251.
[38] See section 16 of the Constitution of the Republic of South Africa, 1996.

only the right to freedom of speech but also the right to receive information.[39]

In *National Media Ltd. v Bogoshi*, it was stated that the freedom of expression is also encumbered with restrictions.[40] In this case involving the publication of a series of allegedly defamatory articles in a newspaper, the City Press, the court decided that although the publisher had freedom of speech, the freedom was not absolute as it also came with some responsibilities.[41] The court stated that there should be a balance between the freedom of expression and the right of dignity[42] as also entrenched in the Constitution.[43] This balance was also pointed out in *Khumalo v Holomisa* to be the right to privacy.[44]

Put in another way, Neethling said, the constitutional right to privacy is like its common law contemporary, not an absolute right but may be limited in terms of our law of general application[45] and has to be balanced with other rights entrenched in the Constitution and the task of balancing these opposing interests is a delicate one.[46]

Section 14 of the Constitution reads 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."[47]

[39] See Note 37 above.
[40] *National Media Ltd. v Bogoshi* 1998 (4) SA 1196 (SCA) at para 24.
[41] ibid.
[42] See section 10 of the Constitution of the Republic of South Africa, 1996.
[43] The Constitution of the Republic of South Africa, 1996.
[44] *Khumalo v Holomisa* 2002 (8) BCLR 771 at para 26.
[45] See section 36 of the Constitution of the Republic of South Africa, 1996.
[46] The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 3. Neethling … et al *Neethling's Law of Personality* 2 ed (2005) 273.
[47] See section 14 of the Constitution of the Republic of South Africa, 1996.

This list, given in section 14[48] is not exhaustive and may be extended to other methods of obtaining information or to making unauthorized disclosures.[49]

According to Neethling, a person's right to privacy includes a person having control over his or her personal affairs and being reasonably free from unsolicited intrusions.[50] This right should be respected because consumer activities and the internet user's personal information is readily available and visible on the internet and this type of information is a valuable commodity especially for people who market goods.[51] This information is collected by way of technology such as cookies that track and collect relevant personal information as well as data.[52]

Privacy is most often seen as a fundamental personality right deserving protection either as part of human dignity or, if not subsumed under dignity, nevertheless warranting independent, but similar, protection to other facets of personality rights like dignity or reputation.[53] The argument for recognizing privacy as an independent right really only acquires significance where the concept of impairment of dignity is given a narrow focus, linked to insulting behavior.[54]

If however, dignity is given its true human rights sweep, ranging beyond mere prevention of insulting conduct, then privacy can rightly find its place as part of the fundamental right to human dignity.[55] Aspects of individual autonomy are more appropriately located within this

---

[48] ibid.
[49] Roos 'The law of data (privacy) protection: A comparative and theoretical study' (unpublished LLD dissertation, University of South Africa 2003) 563-564.
[50] Neethling … et al *Neethling's Law of Personality* 2 ed (2005) 31. Snail & Papadopoulos 'Privacy and data protection' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 276.
[51] R Buys & F Cronje (eds) Cyberlaw *@ SA II: The Law of the Internet in South Africa* 2 ed (2004) 171.
[52] ibid.
[53] Burchell 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* 3. Neethling … et al see Note 49 above at18.
[54] Burchell ibid.
[55] ibid.

broad concept of 'dignity' than under an artificially extended concept of 'privacy', as in the United States of America.[56]

The view that privacy is an independent right was, however, not always held so and in a number of early South African criminal cases regarding the protection of privacy, the idea that *dignitas*, and consequently privacy, should be limited to dignity and accordingly that insult forms an element of this *iniuria*, was stated.[57] Even private law decisions after *O'Keeffe v Argus Printing and Publishing Co Ltd* [58] took a similar approach to the recognition of a right to privacy.[59]

In *Bernstein v Bester*,[60] the conclusion was therefore that, despite the decisions equating privacy with dignity (or honor), it can safely be accepted that the right to privacy is recognized by the common law as an independent right of personality and that it has been delimited as such within the *dignitas* concept.[61]

The Constitution expressly recognizes right to privacy in sec 14,[62] independent of the right to dignity in sec 10,[63] furthermore confirming the independent existence of the right to privacy.[64]

In *National Media Ltd v Jooste*, the court said privacy is an individual condition of life characterized by exclusion from the public and publicity.[65] The court went on to point out that this condition embraces all those personal facts which the person concerned has determined to be excluded from the knowledge of outsiders and in respect of which he has

---

[56] ibid.
[57] The South African Law Reform 'Commission Discussion Paper: Privacy and Protection' (2006) 8.
[58] *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 (2) SA 244 (C) at 248.
[59] See Note 57 above.
[60] *Bernstein v Bester* 1996 (4) BCLR 449 (CC) at 789.
[61] The South African Law Reform 'Commission Discussion Paper: Privacy and Protection' (2006) 9.
[62] See section 14 of the Constitution of the Republic of South Africa, 1996.
[63] See section 10 of the Constitution of the Republic of South Africa, 1996.
[64] See Note 57 above at 9.
[65] *National Media Ltd v Jooste* 1994 (2) SA 634 (C) at 271.

the will that they be kept private.[66]

Important to note is that in accordance with this definition, a legal subject personally determines the private nature of facts.[67] In addition, he must exhibit the will or desire that facts should be kept private.[68] If such a will for privacy is absent, then a person usually has no interest in the legal protection of his privacy.[69]

The need to protect privacy in South Africa emerged in the early 1950s in a case whose facts are similar to those of the classic English defamation case of *Tolley v Fry & Sons Ltd*.[70] In the South African version case of *O'Keeffe v Argus Printing and Publishing Co Ltd*,[71] the plaintiff who was a well-known radio personality had consented to the publication of her photograph, taken at a pistol range, being used for the purpose of a newspaper article.[72]

The photograph was, however, used in the press for advertising purposes. Watermeyer AJ in the Cape Supreme Court turned immediately to Voet's 'Commentary on the Digest' for guidance and found examples of what could be classified as invasions of privacy or *iniuriae*.[73]

The right to privacy is not absolute.[74] As a common law right of personality it is necessarily limited by the legitimate interests of others and the public interest.[75] As a fundamental right it can be limited in accordance with the limitation clause of the Bill of Rights, that is, by a law of general application which includes other fundamental rights.[76] In each case a careful

---

[66] ibid.
[67] The South African Law Reform 'Commission Discussion Paper: Privacy and Protection' (2006) 11.
[68] ibid.
[69] ibid.
[70] *Tolley v J.S. Fry & Sons Ltd* [1931] AC 333. Burchell 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* 6.
[71] *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 (2) SA 244 (C) at 248.
[72] See Note 70 above.
[73] ibid.
[74] Neethling … et al *Neethling's Law of Personality* 2 ed (2005) 240.
[75] ibid.
[76] See section 36 of the Constitution of the Republic of South Africa, 1996.

weighing up of the right to privacy and the opposing interests or rights will have to take place.[77]

In *Helen Suzman Foundation v Judicial Service Commission*[78] the court referred to the case of *Comair Ltd v Minister for Public Enterprises*[79] in which the court reiterated the trite principle that confidentiality does not by itself confer privilege against disclosure.[80]

3.3. South African Common Law and the Right to Privacy

The common law provides for personality rights such as physical integrity, freedom, reputation, dignity and privacy.[81] The common law emphasises privacy as part of a person's inviolate personality and as such enjoys protection while the Constitution provides for privacy as a constitutional right [82] as stated in section 14.[83]

In certain common law rulings, the dignity of an individual was widely interpreted, and included a host of personality rights including privacy and thus, privacy has advanced from the common law as being part of the list of personality rights of an individual up to becoming a constitutional right in the final Constitution[84] of South Africa.[85]

Thus within the ambit of the common law, an invasion of an individual's privacy would be interpreted as an impairment of a person's personality.[86]

---

[77] Neethling … et al see note 74 above.
[78] *Helen Suzman Foundation v Judicial Service Commission* 2017 (1) SA 367 (SCA) at para 16.
[79] *Comair Ltd v Minister for Public Enterprises* 2014 (5) SA 608 (GP) at para 39.
[80] See Note 78 above.
[81] D Goodburn & M Ngoye 'Privacy and the internet' in R Buys & F Cronje (eds) *Cyberlaw @ SA II: The Law of the Internet in South Africa* 2 ed (2004) 172. Burchell 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* 2. H N Olinger … et al 'Western privacy and/or ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007) 39 (1) *The International Information & Library Review* 38.
[82] Olinger … et al ibid.
[83] See section 14 of the Constitution of the Republic of South Africa, 1996.
[84] The Constitution of the Republic of South Africa 108 of 1996.
[85] Olinger … et al see note 81 above.
[86] ibid.

Before the enactment of the ECTA,[87] common law could be stretched as far as possible to cater for the arrest of online offenders.[88] In *S v Van den Berg*, the court applied common law to convict Van den Berg for cyber fraud.[89] In *S v Harper*[90] and *S v Manuel*,[91] the court applied common law and came to the conclusion that stealing money online amounted to online forgery.

Another common law position was also applied in *S v Howard*.[92] The court considered that hacking, cracking and the production and distribution of malicious codes known as viruses, worms and Trojan horses amount to the crime of malicious damage to property in common law.[93]

The court had no doubt whether the crime of malicious damage to property could apply to causing an entire information system to breakdown.[94] The court noted that the crime no longer needed to be committed to 'physical property' but could also apply to data messages of data information.[95]

Although it was the common law which gave rise to the protection of privacy concept in most legislation, Lord Hoffmann in *Campbell v Mirror Group Newspapers Ltd* stated that, the protection of confidential personal information was not being based upon the duty of good faith.[96] In *Murray v Big Pictures (UK) Ltd*, it was pointed out that everyone has a right to

[87] Electronic Communications and Transactions Act 25 of 2002.
[88] S Snail 'Cyber crime in South Africa - Hacking, cracking, and other unlawful online activities' (2009) 1 *Journal of Information, Law and Technology* 2.
[89] ibid 2. *S v Van den Berg* 1991 (1) SACR 104 (T) at 106.
[90] *S v Harper* 1981 (2) SA 638 (D) at 655 D-E.
[91] *S v Manuel* 1953 (4) SA 523 (A) at 526.
[92] *S v Howard* (unreported Case no. 41/ 258 / 02, Johannesburg regional magistrate's court).
[93] Snail see Note 88 above at 3.
[94] ibid.
[95] ibid.
[96] *Campbell v Mirror Group Newspapers Ltd* [2004] 2 All ER 995 (HL) at para 51.

privacy, including celebrities, although they voluntarily circumscribe their own sphere of privacy for financial benefits.[97]

3.4. Infringement of the Constitutional Right to Privacy

No human rights convention is complete without an article that defends privacy, for the fundamental reason that privacy is an indispensable adjunct of the minimum that individuals require for a chance to build good lives.[98]

The elements of liability for an action based on an infringement of a person's privacy are in principle the same as any other injury to the personality, namely an unlawful and intentional interference with a legally protected personality interest - here the right to privacy.[99]

In *Harksen v Lane*, the constitutional court pointed out that, to determine whether a constitutional right to privacy has been infringed, there has to be a two-stage process.[100] The first stage would be to assess if there has been an infringement of a right and the second stage would be to ascertain if such an infringement can be justified.[101] Woolman expressed the same point but differently by stating that in the case of a constitutional invasion of privacy the following questions need to be answered: (a) has the invasive law or conduct infringed the right to privacy in the Constitution?[102] (b) If so, is such an infringement justifiable in terms of the requirements laid down in the limitation clause (sec 36)[103] of the Constitution?

[97] *Murray v Big Pictures (UK) Ltd* [2008] EWCA at 446.
[98] A C Grayling *Liberty in the Age of Terror: A Defence of Civil Liberties and Enlightenment Values* (2009) 110.
[99] The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 17.
[100] Neethling … et al *Neethling's Law of Personality* 2 ed (2005) 6. *Harksen v Lane* 1998 (1) SA 300 (CC) at para 53
[101] Neethling ibid.
[102] S Woolman 'Coetzee: The limitations of Justice Sach's concurrence' (1996) 12 (1) *SA Journal on Human Rights* 99-124.
[103] See section 36 of the Constitution of the Republic of South Africa, 1996.

This was also stated in the case of *S v Makwanyane* otherwise known as the Makwanyane case.[104]

In *Bernstein v Bester*[105] the court stated that to establish infringement of the constitutional right to privacy, South African law applies a two-part test that requires a person to have a subjective expectation of privacy that society has recognized as objectively reasonable.[106] This is similar to the common law understanding of a wrongful infringement of the right of privacy, that is, a person subjectively determines the extent of his or her right of privacy and that the *boni mores* considers this determination to be reasonable.[107]

The subjective expectation of privacy is more than whatever feels private, while objectively this has to be reasonable within the context to qualify for protection.[108] The subjective component of this test determines that a person cannot complain about the invasion of privacy if he or she has consented to it.[109] The individual himself or herself determines which information is private, coupled with the will or desires to keep the particular information facts private.[110] If the will to keep the facts private is lacking, the individual's interest in privacy is also lacking.[111]

Applying these principles, the South African Constitutional court in *Bernstein v Bester*[112] followed the foreign judgement in *Katz v United States*[113] and it stated that, firstly that person

[104] *S v Makwanyane* 1995 (3) SA 391 (CC); 1995 BCLR 665 (CC) at 100.
[105] *Bernstein v Bester* 1996 (4) BCLR 449 (CC) at para 65.
[106] S Snail & S Papadopoulos 'Privacy and data protection' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 278.
[107] Roos 'The law of data (privacy) protection: A comparative and theoretical Study' (unpublished LLD dissertation, University of South Africa 2003) 574 & 577. Neethling … et al *Neethling's Law of Personality* 2 ed (2005) 221.
[108] I Currie & J De Waal *The Bill of Rights Handbook* 5 ed (2005) 318-319.
[109] ibid.
[110] Roos see Note 107 above at 574 & 556.
[111] ibid 556.
[112] See Note 104 at paras 65, 67 and 68.
[113] *Katz v United States* 389 U.S. 347 (1967) at 350-353.

must have exhibited an actual expectation of privacy and secondly that the expectation be one that society is prepared to recognize as reasonable.[114]

The same court made a strong illustration by saying, thus a man's home is, for the most purpose, a place where he expects privacy, but objects, activities, or statements that he exposes to the plain view of outsiders are not protected because no intention to keep them has been exhibited.[115] On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[116]

A violation of privacy by means of an act of intrusion takes place where an outsider himself acquires knowledge of private and personal facts relating to the plaintiff, contrary to the plaintiff's determination and wishes.[117] This is also applicable to the collection and storage of personal information. When information relating to a person is collected, the total picture represented by the record of the facts is usually of such a nature that the person in question would like to restrict others from having knowledge thereof despite the fact that some of the information, viewed in isolation, is not "private" in the above sense.[118] Thus in principle the compiling of an information record and obtaining knowledge thereof constitutes an intrusion into privacy.[119]

3.5. Data Protection: An International Phenomenon

Technological innovation in ages past always challenged the traditional means of conducting trade and commerce, while at the same time facilitating trade and commerce by providing faster and easier means of communication and access to a wider range of business

[114] Snail see note 106 above at 277.
[115] ibid.
[116] ibid 278.
[117] Neethling … et al *Neethling's Law of Personality* 2 ed (2005) 222.
[118] The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 21.
[119] ibid. Neethling … et al see Note 117 above at 225-226.

opportunities, as well as goods and services.[120]

Technological change has always presented a significant challenge to existing regulatory structures, and although sometimes it has been regarded as initially having a negative effect upon accepted rules and practices, businesses, parliaments, and courts have gradually developed legislation with rules and practices that take account of the change.[121]

This development necessarily requires re-evaluation of existing rules and regulations and their interrelationship within national legal systems, as well as their relationship to international law and practice.[122]

This is so particularly where technological change facilitates increased interaction between parties in the international commercial sphere to an extent that activities that were once largely local now have a global effect.[123] One of the characteristics of the internet is that it supports greater participation by consumers in what are, essentially, international transactions.[124]

With all the technological changes taking place, it was soon recognized that privacy protection was not only a domestic problem, and due to this discovery, two crucial international instruments evolved.[125] These were the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention); and the OECD Guidelines Governing the Protection of Privacy and Trans Border Data Flows of Personal Data (OECD Guidelines).[126]

---

[120] R Sorieul … et al 'Establishing a legal framework for electronic commerce: The work of the United Nations Commission on International Trade Law (UNCITRAL)' (2001) 35 (1) *The International Lawyer* 107.
[121] ibid.
[122] ibid at 108.
[123] ibid.
[124] ibid.
[125] The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 2.
[126] ibid.

These two agreements have had a profound effect on the enactment of laws around the world with nearly thirty countries signing the CoE Convention and the OECD guidelines having also been widely used in national legislation, even outside the OECD member countries.[127]

In late 1980, the OECD issued a set of guidelines concerning the privacy of personal records.[128] Although broad, the OECD Guidelines set up important standards for future governmental privacy rules and these guidelines underpin the most current international agreements, national laws, and self-regulatory policies.[129] Although the guidelines were voluntary, roughly half of the OECD member-states had already passed or proposed privacy protecting legislation by the end of 1980.[130] By 1983, 182 American companies claimed to have adopted the guidelines, although very few ever implemented practices that directly matched the standards.[131]

The OECD Guidelines have been highly influential in the enactment and content of information protection legislation in non-European jurisdictions, particularly Japan, Australia, New Zealand and Hong Kong.[132] In North America the OECD Guidelines have been formally endorsed by numerous companies and trade associations.[133] These OECD Guidelines have additionally constituted the basis for the first comprehensive set of information protection standards to be developed by a national standards association: the Model Code for the Protection of Personal Information (MCPPI), adopted by the Canadian Standards Association (CSA) in March 1996.[134]

---

[127] ibid.
[128] ibid.
[129] ibid.
[130] ibid.
[131] ibid.
[132] Victoria Law Reform Commission 'Discussion Paper: Privacy Law: Options for Reform' (2001) 23.
[133] ibid.
[134] ibid.

3.5.1. United Nations Commission on International Trade Law (UNCITRAL)

It is certain that in an increasingly economically interdependent world, the importance of an improved legal framework for the facilitation of international trade and investment is widely acknowledged and plays an important role in developing that framework.[135] This framework was developed with a mandate to further the progressive harmonization and modernization of the law of international trade by preparing and promoting the use and adoption of legislative and non-legislative instruments in a number of key areas of commercial law.[136]

As a response to some gaps (lacuna) in legislation governing electronic commerce around the globe, the UNCITRAL and governments of various countries called for the drafting of internationally recognized uniform electronic transactions legislation.[137] The UNCITRAL developed these model laws as an early response to the legal uncertainties pertaining to e-commerce around the world at that time, especially with the quick growth of the internet.[138] In this dissertation, for all intents and purposes, a model law is a legislative text that is recommended to States for enactment as part of their national law.[139]

In 1985, the UNCITRAL drafted and adopted the 'Recommendation on the Legal Value of Computer Records' which at the time of its drafting, was seen as a document, but since the development of the UNCITRAL Model Law one would rather call it the 'policy document'

[135] UNCITRAL 'A Guide to UNCITRAL: Basic facts about the United Nations Commission on International Trade Law' (2013) 1 and 14, available at http://www.uncitral.org/pdf/english/texts/general/12-57491-Guide-to-UNCITRAL-e.pdf, accessed on 03 February 2017.
[136] ibid.
[137] S Pitiyasak 'Electronic contracts: Contract law of Thailand, England and UNCITRAL compared' (2003) 9 (1) *Computer and Telecommunications Law Review* 16.
[138] S Eiselen 'Fiddling with the ECT Act - Electronic signatures' (2014) 17 (6) *Potchefstroom Electronic Law Journal* 2807.
[139] See Note 135 above.

which laid the basis for the harmonization of electronic communications laws on an international level.[140]

Inadequate legislation at the national level will inevitably create obstacles to international trade.[141] The purpose of the UNCITRAL Model Law was to offer national legislators a set of internationally acceptable rules for the enhancement of legal certainty.[142] The principles expressed in the UNCITRAL Model Law were also intended to be of use to individual users of electronic commerce in drafting solutions for contracts that are concluded electronically.[143]

One must mention the interesting fact that the UNCITRAL Model Law on E-Commerce, 1996 (MLEC), the UNCITRAL Model Law on E-Signatures, 2001 (MLES) as well as the United Nations Convention on the use of Electronic Communications in International Contracts (UNECIC) are not legally binding upon South Africa although the first two instruments have been influential in the drafting of the ECTA and have formed the legal basis for this Act.[144]

The UNCITRAL Model Law has served both to educate lawmakers about the legal ramifications of electronic transactions and to provide a framework for any country wishing to draft electronic commerce legislation and although South Africa is not a member state, it has drawn some inspiration from it in drafting its own legislation.[145]

---

[140] S Snail 'Electronic contracts in South Africa - A comparative analysis' (2008) 2 (1) *Journal of Information, Law & Technology* 2-3. Sorieul … et al 'Establishing a legal framework for electronic commerce: The work of the United Nations Commission on International Trade Law (UNCITRAL)' (2001) 35 (1) *The International Lawyer* 107.

[141] Abhilash 'E-commerce law in developing countries: An Indian perspective' (2002) 11 (3) *Information & Communication Technology Law* 269.

[142] United Nations Commission on International Trade Law 'UNICITRAL Model Law on Electronic Signatures' available at http://www.uncitral.org/uncitral/en/commission/sessions/29th.html, accessed on 30 January 2017.

[143] S L S Mtuze 'A comparative review of legislative reform of electronic contract formation in South Africa' (unpublished LLM thesis, University of South Africa, 2015) 21.

[144] ibid.

[145] ibid.

In South Africa or any other country, the UNCITRAL Model Law can only have effect if and only if it is enacted into national law by the country in question.[146] It is also imperative to recognize that the UNCITRAL Model Law provisions specifying standards do not specify technology to be adopted or used by any country which becomes a member state.[147]

In South Africa, chapter III of the ECTA is based on the UNCITRAL Model Law on E-Commerce, 1996 and the UNCITRAL Model Law on E-Signatures, 2001.[148] The UNCITRAL developed these model laws as an early response to the legal uncertainties pertaining to e-commerce around the world at that time, especially the quick growth of the internet.[149]

The decision by the UNCITRAL to formulate model legislation on electronic commerce was also taken in response to the fact that in a number of countries the existing legislation governing communication and storage of information is inadequate or outdated because it does not contemplate the use of electronic commerce.[150] The lack of legislation in many countries in dealing with e-commerce as a whole results in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper document.[151]

The UNCITRAL Model Law on E-Commerce, 1996 is a more conceptual text.[152] The legislation that has been based on this model law largely reflects the principles of the

[146] C Satapathy 'Legal framework for e-commerce' (1998) 33 (29) *Economic and Political Weekly Journal* 1906.
[147] ibid.
[148] Eiselen 'Fiddling with the ECT Act - Electronic signatures' (2014) 17 (6) *Potchefstroom Electronic Law Journal* 2807.
[149] ibid.
[150] Abhilash 'e-commerce law in developing countries: An Indian perspective' (2002) 11 (3) *Information & Communication Technology Law* 269.
[151] ibid.
[152] 'A Guide to UNCITRAL: Basic facts about the United Nations Commission on International Trade Law' (2013) 1 available at http://www.uncitral.org/pdf/english/texts/general/12-57491-Guide-to-UNCITRAL-e.pdf, accessed on 03 February 2017.

text, although there are some departures from it in terms of not only drafting, but also in the combination of provisions adopted.[153]

3.5.2. United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, 1996 Revised 1998 (MLEC)

To assist countries in drafting and enacting laws to give legal recognition to electronic contracts, in 1996, the United Nations adopted the UNCITRAL Model Law on E–Commerce.[154] The UNCITRAL Model Law on E-Commerce, 1996 was adopted on 12 June 1996 and aimed to create a more certain legal environment for what had become known as 'electronic commerce' by providing a tool for States to enhance their legislation of paperless communication and storage of information.[155]

The UNCITRAL Model Law on E-Commerce, 1996, purports to enable and facilitate commerce conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce.[156] In particular, it was intended to overcome obstacles arising from statutory provisions that could not be varied contractually by providing equal treatment to paper-based and electronic information.[157] Such equal treatment was essential for

---

[153] ibid.

[154] United Nations Commission on International Trade Law 'UNICITRAL Model Law on Electronic Commerce' available at http://www.uncitral.org/uncitral/en/commission/sessions/29th.html, accessed on 30 January 2017. See also Sorieul … et al 'Establishing a legal framework for electronic commerce: The work of the United Nations Commission on International Trade Law (UNCITRAL)' (2001) 35 (1) *The International Lawyer* 108.

[155] T Pistorius 'Contract formation: A comparative study of legislative initiatives on select aspects of electronic commerce' (2002) 25 (1) *Comparative & International Law of South Africa* 130. United Nations Commission on International Trade Law 'UNICITRAL Model Law on Electronic Signatures' available at http://www.uncitral.org/uncitral/en/commission/sessions/29th.html, accessed on 30 January 2017.

[156] 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998' available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html, accessed on 03 February 2017.

[157] ibid.

enabling the use of paperless communication, thus fostering efficiency in international trade.[158]

The use of e-mails and EDI has increased rapidly and due to the use of modern means of communication for the conduct of international trade, transactions have been increasing rapidly and are expected to develop further as technical support becomes more widely accessible.[159] For this reason, the United Nations developed the UNCITRAL Model Law on E-Commerce, 1996 because the communication of legally significant information in the form of paperless messages was being hindered by legal obstacles to the use of such messages, or by uncertainty as to their legal effect or validity.[160]

It is against this background of increasing legal uncertainty and the exponential increase in international e-commerce (e-trade) that the UNCITRAL established a working group to draft legal rules on e-commerce.[161]

The UNCITRAL Model Law on E-Commerce, 1996 states that the adoption of the UNCITRAL Model Law on Electronic Commerce by the UNCITRAL Commission will significantly assist all States in enhancing their legislation governing the use of alternatives to paper-based methods of communication and storage of information and in formulating such legislation where none currently exists.[162] Now through the application of the principle of functional equivalence, the UNCITRAL Model Law advocated, as a first step, the adaptation of existing legal principles to the e-commerce environment.[163]

---

[158] ibid.
[159] United Nations 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998' (1999) 16.
[160] ibid 16.
[161] C Glatt 'Comparative issues in the formation of electronic contracts' (1998) 1 (1) *International Journal of Law and Information Technology* 57.
[162] UNCITRAL Model Law on Electronic Commerce (1996) Resolution 51&162.
[163] Mtuze 'A comparative review of legislative reform of electronic contract formation in South Africa' (unpublished LLM thesis, University of South Africa, 2015) 26.

The UNCITRAL Model Law on E-Commerce, 1996 is divided into two parts namely, Part 1, that deals with the general electronic commerce provisions and Part 2, that deals with e-commerce in specific areas and it has an open-ended structure to allow for future additions.[164]

It is also worth mentioning that the UNCITRAL Model Law on E-Commerce, 1996 itself lists five non-exhaustive main objectives.[165] First, to facilitate electronic commerce among and within nations; secondly, to validate transactions that have been concluded by new means of technology; third, to promote new technology and encourage the implementation of such technology in trade transactions by facilitating and enabling them; fourth, to create and promote uniformity and support e-commerce practices.[166] Fifth, Article 5 sets out the fundamental principle that electronic communications should not be discriminated against or denied legal effect simply because they are in electronic form and Article 6 sets the basic standard for an electronic document where it is a legal requirement that a document be in writing.[167] Thus the UNCITRAL Model Law on E-Commerce, 1996 points out its intended purposes.[168]

With Article 7 of the UNCITRAL Model Law on E-Commerce, 1996 acknowledging that a signature is used in the real world to indicate one‘s approval or verify the contents of the document, it gives an electronic signature the same legal effect as an ink signature even if it was not authenticated in a manner peculiar to a paper document.[169]

---

[164] See Note 161 above at 58.
[165] See Note 163 above at 29.
[166] ibid.
[167] ibid.
[168] ‘UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998’ available at http://www.uncitral.org/uncitral/en/ uncitral_texts/ electronic_commerce/1996Model.html, accessed on 05 February 2017.
[169] ibid.

3.5.3. United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures, 2001 (MLES)

In 2001 UNCITRAL published the UNCITRAL Model Law on Electronic Signatures which is usually referred to as UNCITRAL Model Law on Electronic Signatures, 2001 as an addition to the 1996 Model Law on Electronic Commerce.[170] This was for the purpose of offering practical standards against which the technical reliability of electronic signatures may be measured, adding substantially to the UNCITRAL Model Law on E-Commerce, 1996.[171] The UNCITRAL Model Law on Electronic Signatures would help by adopting an approach under which the legal effectiveness of a given electronic signature technique may be predetermined or assessed prior to being actually used.[172]

The UNCITRAL Model Law on Electronic Signatures, 2001 makes it clear that the sufficiency of an electronic signature is first and foremost determined by the parties themselves unless there is a peremptory law requiring a signature.[173] The UNCITRAL Model Law on Electronic Signatures, 2001 unlike the UNCITRAL Model Law on E-Commerce, 1996 actually contains the definition of 'electronic signature'.[174]

It defines electronic signature as

> "data in electronic form, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message."[175]

---

[170] Eiselen 'Fiddling with the ECT Act - Electronic signatures' (2014) 17 (6) *Potchefstroom Electronic Law Journal* 2807-2808. UNCITRAL Model Law on Electronic Signatures (2001) para 4.
[171] ibid.
[172] ibid.
[173] ibid.
[174] ibid.
[175] UNCITRAL Model Law on Electronic Signatures (2001) Article 2.

The UNCITRAL Model Law on Electronic Signatures, 2001 also states that requirements for electronic signatures should not require a higher level of security or difficulty than their physical counterparts to comply with the principles of media neutrality and functional equivalence underlying the Model Law.[176]

UNCITRAL came to the conclusion that a paper based handwritten signature has a number of functions such as identifying a person, providing certainty as to the personal involvement of that person in the act of signing, and associating the person with the contents of the document.[177] According to the UNCITRAL Model Law on E-Commerce, 1996, in many legal systems certain processes such as stamping, printing and even letterheads are accorded recognition as signatures depending on the level of certainty required.[178]

The UNCITRAL Model Law on Electronic Signatures, 2001 provides a link between technical reliability and legal effectiveness of an electronic signature by adopting an approach according to which the legal effectiveness of an electronic signature is predetermined.[179] It sets out the presumption that where electronic signatures meet certain criteria of technical reliability, they should be treated as equivalent to hand-written signatures.[180]

Wang explains that there are three different approaches when dealing with the various electronic signature legislation that have been enacted world-wide, namely the 'minimalist approach', the 'prescriptive approach' (also known as the technology-specific approach) and the 'two-tiered approach'.[181]

---

[176] UNCITRAL Model Law on Electronic Commerce (1996) para 15. D P Van de Merwe *Information and Communications Technology Law* (2008) 146.
[177] F F Wang *Law of Electronic Commercial Transactions - Contemporary issues in the EU, US and China* (2010) 83-85.
[178] UNCITRAL Model Law on Electronic Commerce (1996) paras 53-54.
[179] Mtuze 'A comparative review of legislative reform of electronic contract formation in South Africa' (unpublished LLM thesis, University of South Africa, 2015) 54.
[180] ibid.
[181] M Wang 'Review of the signature regulations: Do they facilitate or impede intentional electronic commerce?' (2006) 14 (1) *Association for Computing Machinery* 549.

Some jurisdictions that follow a technological neutrality approach recognize all technologies for electronic signatures. This approach is called the minimalist approach as it is non-prescriptive.[182]

The technological approach is seen as a light approach as it recognizes all forms of electronic signatures as functional equivalents of handwritten signatures provided that they fulfil certain specified functions and meet the technology-neutral reliability requirement.[183]

3.5.4. United Nations Convention on the Use of Electronic Communications in International Contracts, 2005 (UNECIC)

When the United Nations created the Model Laws on E-commerce in 1996 and E-signatures in 2001, it became apparent that issues relating to the formation of international contracts required further redress.[184] On 23 November 2005, the United Nations (UN) General Assembly adopted the new United Nations Convention on the Use of Electronic Communications in International Contracts (the Convention).[185]

With the UNCITRAL Model Law on E-Commerce, 1996 in place, different countries implemented this model differently, resulting in significant variations in electronic commerce legislation even amongst countries that had adopted the UNCITRAL Model Law on E-Commerce, 1996.[186] In 2000, the EU promulgated the Directive 2000/31/EC which differed

[182] Mtuze see Note 179 above at 56.
[183] UNCITRAL 'Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods' (2009) 36, available at http://www.uncitral.org/uncitral, accessed on 06 February 2017.
[184] See Note 179 above at 63.
[185] UNCITRAL conventions available at http://www.uncitral.org/uncitral/en/uncitral-texts/electronic-commerce/2005Con vention.html, accessed on 06 February 2017.
[186] W K Chong & J C Suling 'United Nations convention on the use of electronic communications in International contracts-A new global standard' (2006) 18 (1) *Singapore Academy of Law Journal* 117.

significantly in scope and content from the UNCITRAL Model Law on E-Commerce, 1996.[187]

There was therefore a serious lack of uniformity and harmonization amongst national e-commerce legislation around the world and this lack of uniformity and harmonization was perceived as a barrier to international trade by electronic means.[188]

The Convention builds upon the UNCITRAL Model Law on E-Commerce, 1996 and the UNCITRAL Model Law on Electronic Signatures, 2001, but its provisions have been improved and updated to take into account technological developments since 1996, most notably, the growth of the internet and as an interpretative legal instrument with minimum substantive provisions.[189] It facilitates the use of electronic communications in international contracting by providing for the functional equivalence of electronic communications, while preserving the principle of technological neutrality.[190]

Taking the form of a convention, it is a landmark legal instrument that promises to harmonize basic electronic commerce legislation amongst contracting states, hence removing legal barriers to cross-border e-commerce.[191] The Convention is also intended to remove obstacles to the use of electronic communications that might arise under existing international trade law instruments, most of which were negotiated long before the development of new technology, such as e-mail, Electronic Data Interchange and the internet.[192]

The Convention does not have autonomous application, and applies only when the law of a Contracting State governs the transaction between the parties.[193]

---

[187] ibid.
[188] ibid 117-118.
[189] ibid 119.
[190] ibid.
[191] ibid.
[192] ibid.
[193] UNCITRAL Article 60/17, at para 22.

3.5.5. Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (AUCLCS)

The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (AUCLCS) was created following the 14th AU summit in 2010 which explored the theme 'Information and Communication Technologies in Africa: Challenges and Prospect for Development'.[194] This was subsequently confirmed by the 'Abuja Declaration', and brought into law by the African Union in June 2014.[195]

The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa gives effect to a resolution of the last session of the Assembly of Heads of State of Governments of the African Union and seeks to harmonize African cyber legislation on e-commerce, personal data protection, cyber-security promotion and cyber-crime control. [196]

It is clear, however, that its focus is more on cyber-security and cyber-crimes than provisions on enablement and regulation of e-commerce in Africa and interestingly, unlike the MLEC, the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa has omitted definitions such as 'data', 'data messages', 'writing', 'electronic signature' and 'original' but includes wide definitions for terms such as 'electronic commerce', 'electronic mail' and 'information'.[197]

Although the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa re-states that electronic commerce is an economic activity by which a person offers or provides goods and services by electronic means, it goes

[194] Mtuze & Matanzima 'Without prejudice - cyber security in Africa: Cyber law' (2014) 14 (9) *Electronic Journal of Commerce* 88.
[195] ibid.
[196] ibid.
[197] ibid.

on to define the field of electronic commerce as also comprising of services such as those providing information on-line, commercial communications, research tools, access, data retrieval and access to communication or information hosting network, even where such services are not remunerated by the recipients.[198]

Murungi, in "Comments on the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (2011)", argues that the definition only includes the seller's economic activity by which a person offers or provides goods and services by electronic means.[199] He states that a better attempt at such provision would have been to use words such as person who offer or receives offers, by electronic means.[200]

3.5.6. Influence of the UNCITRAL Model Law on International Law

The UNCITRAL Model Law could be described as an instrument of 'preventive' or 'pre-emptive' harmonization: it led to the process of development of law by providing universally acceptable solutions to the issues likely to arise, rather than being negotiated after practices and usage had already resulted in disparate laws and regulations. [201]

However, notwithstanding the fact that many countries widely accepted the principles contained in the UNCITRAL Model Law, it could not simply be assumed that its principles achieved the goal of world-wide harmonization.[202] The provisions of the UNCITRAL Model Law soon proved inadequate to deal with all the issues raised by the creation and use of electronic signatures.[203]

---

[198] ibid.
[199] ibid.
[200] ibid.
[201] J A E Faria 'E-commerce and international legal harmonisation: Time to go beyond the functional equivalence?' (2004) 16 (1) *SA Mercantile Law Journal* 533.
[202] ibid. Mtuze 'A comparative review of legislative reform of electronic contract formation in South Africa' (unpublished LLM thesis, University of South Africa, 2015) 53.
[203] Mtuze see note 202 above.

Already at the time of the drafting of the UNCITRAL Model Law on Electronic Signatures, 2001, there were calls for another round of legislation, an international convention on e-commerce, to achieve further harmonization of national laws.[204] Despite the wide acceptance of the UNCITRAL Model Law on E-Commerce, 1996, it cannot simply be assumed that its principles have already achieved universal application through domestic legislation.[205]

The UNCITRAL Model Law on E-Commerce, 1996 does not address aspects of contract formation and performance that may be affected by the ways in which electronic transactions are currently structured and by the ways in which those structures are being changed to facilitate e-commerce.[206]

That the challenge was successfully met can be gauged from the influence of the Model Law on e-commerce legislation already adopted, or being developed, around the world.[207]

3.6. The European Union Directive on Privacy and Data Protection

On October 24, 1995 the European Union (hereafter EU) enacted the European Union Directive on Privacy and Data Protection 95/46/EC (for the purposes of this dissertation this will be cited in full to avoid confusion) in order to harmonize member states' laws in providing consistent levels of protections for citizens and ensuring the free flow of personal data within the EU.[208]

Formally adopted in 1995, the European Union Directive on Privacy and Data Protection 95/46/EC arose from the sense that European citizens were losing control over their personal information and that they had a fundamental right to privacy.[209]

---

[204] See Note 201 above.
[205] ibid 533-534.
[206] ibid 533.
[207] ibid.
[208] The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 7.
[209] ibid.

On September 12, 1996, the EU Council adopted the Electronic Communication Data Protection Directive, a supplement to the European Union Directive on Privacy and Data Protection 95/46/EC.[210] In October 1998, the EU enacted the Personal Data Protection Act, which was also revised from the European Union Directive on Privacy and Data Protection 95/46/EC and in early 1999; the European Commission issued the General Principles on Personal Data Privacy Protection on the internet, and then promulgated the Advices on sightless and automatic personal data processing carried by software and hardware in internet.[211]

Although the European Union Directive on Privacy and Data Protection 95/46/EC directive was designed for the EU with only 15 member states in it, non-member states are affected because the Directive provides high standards of data protection and attempts to eliminate data transmission barriers in 15 member states.[212] In the meanwhile, in order to transmit data between the member states and a country outside the EU, the European Union Directive on Privacy and Data Protection 95/46/EC stipulates that the country must adopt the same protection standards as the EU countries.[213]

The EU member states are not allowed to transfer their personal data to any non-member state, until it ensures adequate protection.[214] This measure ensures that personal data is protected and it prevents accidental data loss, data transform, unauthorized data access or exposure, as well as other forms of illegal operation.[215]

[210] Guo 'A comparative study on consumer right to privacy in e-commerce' (2012) 3 (1) *Modern Economy* 403.
[211] ibid.
[212] ibid.
[213] ibid.
[214] ibid.
[215] ibid 404.

The need for a legislative data protection framework in South Africa is largely a trade and development issue.[216] After the EU introduced the European Union Directive on Privacy and Data Protection 95/46/EC, it was deemed necessary by the South African government to place the issue of data protection on the agenda.[217] Both the European Union and South Africa tend to share an overall similarity when it comes to being apprehensive about doing business online.[218] The concern of users was that their private data/information will not be sufficiently protected, thus allowing for others to gain access and carry out illegal practices, and hence the "call" from users for the implementation of protective measures to ensure their personal data is protected.[219]

The EU has two main directives regarding the processing of data which are: the Data Protection Directive which applies to general aspects of data processing and the Privacy and Electronic Communications Directive.[220] The European Union Directive on Privacy and Data Protection 2002/58/EC (hereafter EU Directive) replaced the Telecommunications Data Protection Directive (97/66/EC).[221] Due to the rule of *lex specialis* the EU Directive has priority over the European Union Directive on Privacy and Data Protection 95/46/EC on issues covered by both directives.[222]

3.7. Applicability of International Law in South Africa

As stated in the previous chapter, when it was completed, the UNCITRAL Model Law was a unique instrument in a legal landscape where there was no existing body of law, whether

[216] P Pluckhahn '(E-commerce) data protection in the European Union and South Africa. A comparative study' (unpublished LLM thesis, Aarhus University, 2010) 43.
[217] ibid.
[218] ibid.
[219] ibid.
[220] E Cleff 'Mobile advertising: A comparative regulatory overview' (unpublished LLM thesis, Aarhus University, 2005) 28.
[221] ibid.
[222] ibid.

uniform international law or national law that comprehensively addressed the issues raised by e-commerce.[223]

As such, the UNCITRAL Model Law could be described as an instrument of 'preventive' or 'pre-emptive' harmonization: it led the process of development of law by providing universally acceptable solutions to the issues likely to arise, rather than being negotiated after practices and usage had already resulted in disparate laws and regulations.[224]

The UNICITRAL Model Law is very much in use in the South African courts. In *Jafta v Ezemvelo KZN Wildlife*[225] dealing with Short Message Service (SMS) and Electronic mail (e-mail) contracts, the court used the UNICITRAL Model Law to determine if Jafta's communications constituted a valid acceptance of the offer or not and if an SMS is an appropriate mode of concluding a contract.[226]

The court held that both *Jafta's* SMS and e-mail were valid acceptances.[227] First, the acceptances in both modes were clear, unequivocal and unambiguous as stated in *Boerne v Harris*[228] and second, both acceptances corresponded with the offer.[229]

In South Africa, chapter III of the ECTA[230] is based on the UNCITRAL Model Law on E-Commerce, 1996 and the UNCITRAL Model Law on Electronic Signatures, 2001.[231]

---

[223] H S Alhorr …et al 'E-Commerce on the global platform: Strategic insights on the localization-standardization perspective' (2010) 11 (1) *Journal of Electronic Commerce Research* 7.
[224] Faria 'E-commerce and international legal harmonization: Time to go beyond functional equivalence?' (2004) 16 *SA Mercantile Law Journal* 531.
[225] *Jafta v Ezemvelo KZN Wildlife* (2009) 30 *ILJ* 131 (LC) at paras 39, 45, 109 and 113.
[226] P Stoop 'SMS and e-mail contracts: Jafta v Ezemvelo KZN Wildlife' (2009) 21 (1) *SA Mercantile Law Journal* 110.
[227] R Buys & F Cronje (eds) *Cyberlaw @ SA II: The Law of the Internet in South Africa* 2 ed (2004) 104. *Jafta v Ezemvelo KZN Wildlife* (2009) 30 *ILJ* 131 (LC) at paras 112 and 113.
[228] *Boerne v Harris* 1949 (1) SA 793 (A) at 799.
[229] Stoop see Note 226 above.
[230] Electronic Communications and Transactions Act 25 of 2002.
[231] Eiselen 'Fiddling with the ECT Act - Electronic signatures' (2014) 17 (6) *Potchefstroom Electronic Law Journal* 2807.

As stated earlier on in this chapter, it is worth noting that although the UNCITRAL Model Law serves both to educate lawmakers about the legal ramifications of electronic transactions and to provide a framework for any country wishing to draft electronic commerce legislation, South Africa is not a member state and is not bound by this UNCITRAL Model Law.[232]

Another aspect worth noting is the fact that the UNCITRAL Model Law on e-commerce and the model law on electronic signatures are not conventions and as such are not directly binding on the South African legal system.[233] However, as previously mentioned, they have had an influence in the drafting of the ECTA and have formed a clear basis for this legislation.[234] The ECTA[235] has some remarkable consistencies with what is proposed in the above model laws; however it also represents a uniquely South African response to the challenges of e-commerce.[236] The challenges of e-commerce as stated in chapter one of this dissertation include but not is not limited to a threat to security, confidentiality and consumer trust as well as privacy protection for consumers in data transmission.

Although our courts are not bound to the provisions of the UNCITRAL Model Law, by virtue of the Constitution[237] they are entitled to interpret legislation in a manner that is consistent with section 233[238] and are bound by it.[239]

According to Van der Merwe, it is not just the international law that has had an influence on the South African e-commerce laws.[240] Van der Merwe stated that during the drafting of the ECTA, a wide range of foreign legislation was consulted, apart from UNCITRAL Model

---

[232] Mtuze 'A comparative review of legislative reform of electronic contract formation in South Africa' (unpublished LLM thesis, University of South Africa, 2015) 21.
[233] Snail 'Electronic contracting in South Africa (e-contracts)' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 42.
[234] ibid.
[235] See Note 230 above.
[236] Snail see note 233 above.
[237] See Section 232 of The Constitution of the Republic of South Africa, 1996.
[238] See Section 233 of The Constitution of the Republic of South Africa, 1996.
[239] D P Van der Merwe *Information and Communications Technology Law* (2008) 146.
[240] ibid.

Law.[241] This included legislation from Australia, Bermuda, Canada, Germany, India, Ireland, New Zealand, the Philippines, Singapore and the United Kingdom.[242]

The principle of functional equivalence is reflected in the ECTA[243], as are the principles of the 'party autonomy' and 'technology neutrality'.[244]

3.7.1. Case Law: Cases Relating to the UNCITRAL Model Law

To prove the relevance of the UNCITRAL Model Law in the South African legislation and its application in the courts of law, the dissertation now turns to the South African court decisions and arbitral awards relating to the UNCITRAL Model Law.

3.7.1.1. *Sihlali v South African Broadcasting Corporation Ltd* (J700/08) [2010] ZALC 1; (2010) 31 ILJ 1477 (LC); [2010] 5 BLLR 542 (LC) (14 January 2010)

In *Sihlali v South African Broadcasting Corporation Ltd*,[245] the court dealt with a notice of termination of employment contract by sending an SMS.[246]

The applicant and the respondent, a South African corporation, entered into a fixed term employment contract, under which the former was employed as a legal adviser and after learning from the press about allegations of impropriety, and pending an audit on those allegations, the applicant informed the respondent of his decision to quit his job with immediate effect by sending an SMS.[247] The respondent replied with a letter accepting the resignation.[248] Six weeks after sending the SMS, the applicant sent an email asserting that the employment contract was still valid and the respondent replied by indicating that the notice of

[241] ibid.
[242] ibid.
[243] Electronic Communications and Transactions Act 25 of 2002.
[244] See Note 239 above.
[245] (J700/08) [2010] ZALC 1; (2010) 31 ILJ 1477 (LC); [2010] 5 BLLR 542 (LC) (14 January 2010) at para1.
[246] ibid at para 1. 'CLOUT case 1230 – UNCITRAL' available at https://www.uncitral.org/clout/clout/data/zaf/clout_case_1230_leg-2892.html, accessed on 06 February 2017.
[247] ibid.
[248] ibid.

resignation sent by SMS was valid, and that therefore the employment contract had been terminated.[249]

The preliminary issue raised was whether an SMS sent by the applicant constituted a valid notice of resignation.[250] Pursuant to South African labor law, a valid notice of termination of an employment contract must be given in writing (unless the employee is illiterate).[251] The court held that a communication by SMS is a communication in writing, by referring to the Section 1 and Section 12 of the ECTA, which are based on articles 2 and 6 (1) UNCITRAL Model Law on E-Commerce, 1996.[252] The court thus confirmed that the applicant's notice by SMS was a valid written form of notice of resignation.[253]

3.7.1.2. *Phoenix Shipping Corporation v DHL Global Forwarding SA (Pty) Ltd* (AC70/2011) [2012] ZAWCHC 11; 2012 (3) SA 381 (WCC) (24 February 2012)

In *Phoenix Shipping Corporation v DHL Global Forwarding SA (Pty) Ltd*,[254] the Western Cape High Court also used the UNCITRAL Model Law to decide on an arbitration matter.[255]

3.7.1.3. Spring Forest Trading v Wilberry [2014] ZASCA 178; 2015 (2) SA 118 (SCA), 725/13

The case of *Spring Forest Trading v Wilberry*,[256] dealt with the validity of a cancellation agreement using e-mail communications in light of a no-oral modification clause providing for the cancellation to be in writing and signed by the parties.[257]

---

[249] ibid.
[250] J Hofman 'The Moving Finger: sms, on-line communication and on-line disinhibition' (2011) 8 (1) *Digital Evidence and Electronic Signature Law Review* 180.
[251] See Section 37 (4) (*a*) of the Basic Conditions of Employment Act 75 of 1997.
[252] Hofman see Note 250 above at 183.
[253] ibid.
[254] (AC70/2011) [2012] ZAWCHC 11; 2012 (3) SA 381 (WCC) (24 February 2012) at paras 36 and 62.
[255] 'CLOUT case 1397 – UNCITRAL' available at https://www.uncitral.org/clout/clout/data/zaf/clout_case_1397_leg-2892.html, accessed on 06 February 2017.
[256] [2014] ZASCA 178; 2015 (2) SA 118 (SCA), 725/13 at para 17.
[257] See Note 255 above.

The Supreme Court of Appeal (SCA) held that an e-mail, being a data message, satisfied a legal requirement for an agreement to be in writing set forth in Section 12 of the ECTA whose enactment was influenced by Article 6 (1) of the UNCITRAL Model Law on E-Commerce, 1996.[258]

In discussing the case, the Supreme Court also considered whether the names of the parties at the foot of their e-mail constituted signatures as contemplated in Section 13 (1) of the Act which provides that:

> "…where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used".[259]

Section 13 (3) of the ECTA whose enactment was influenced by Article 7 (1) of UNCITRAL Model Law on E-Commerce, 1996 provides that:

> "where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if (a) a method is used to identify the person and to indicate the person's approval of the information communicated;[260] and (b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated".[261]

[258] ibid.
[259] ibid.
[260] See Section 13 (3) (*a*) of the Electronic Communications and Transactions Act 25 of 2002.
[261] ibid.

Section 1 of the ECTA defines an electronic signature as

> "…data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature"[262]

This is similar to Article 2 (*a*) of the UNCITRAL Model Law on Electronic Signatures, 2001.[263] Using this definition of a signature, the Supreme Court dismissed the respondent's argument that no reliable method was used with respect to the e-mails, since the reliability of the e-mails, the accuracy of the information communicated and the identities of the authors were undisputable.[264]

3.7.1.4. *Jafta v Ezemvelo KZN Wildlife* (2009) 30 *ILJ* 131 (LC)

As stated earlier in this chapter, the case of *Jafta v Ezemvelo KZN Wildlife* deals with the conclusion of a labor contract in connection with the use of electronic communications (email and SMS). [265]

After a successful selection process, the respondent, Ezemvelo, sent by e-mail an employment offer to the applicant, Jafta, who tentatively accepted.[266] The respondent sent a second e-mail, prompting a final decision, to which the applicant replied by accepting the offer without conditions.[267] Although the applicant's information system indicated that the acceptance e-mail had been successfully sent, it never reached the respondent's system.[268] Later, one of the respondent's employees sent a final reminder of the pending offer by Short

[262] See Section 1 of the Electronic Communications and Transactions Act 25 of 2002.
[263] 'CLOUT case 1397 – UNCITRAL' available at https://www.uncitral.org/clout/clout/data/zaf/clout_case_1397_leg-2892.html, accessed on 06 February 2017.
[264] ibid.
[265] (2009) 30 *ILJ* 131 (LC) at para 1.
[266] Stoop 'SMS and e-mail contracts: Jafta v Ezemvelo KZN Wildlife' (2009) 21 (1) *SA Mercantile Law Journal* 110.
[267] ibid.
[268] Buys & F Cronje (eds) *Cyberlaw @ SA II: The Law of the Internet in South Africa* 2 ed (2004) 104.

Message System (SMS), to which the applicant replied promptly confirming his acceptance.[269]

The Court considered the conclusion of the labor contract by e-mail and SMS in the context of the ECTA which is based, in the relevant parts, on the UNCITRAL Model Law on E-Commerce, 1996.[270] In particular, the Court noted the necessity to interpret the ECTA in light of its uniform origin and of the inherent transnational nature of the law of electronic communications; it therefore made reference to the UNCITRAL Model Law on E-Commerce, 1996, to other enactments of the UNCITRAL Model Law on E-Commerce, 1996 as well as to relevant case law from foreign jurisdictions.[271]

Moreover, the Court noted that certain principles of the law of electronic communications are widely accepted worldwide and enacted in South African law.[272] Such principles include: non-discrimination of electronic communications (section 11 ECTA; article 5 of the UNCITRAL Model Law on E-Commerce, 1996); due evidential weight of data messages (section 15 ECTA; article 9 of the UNCITRAL Model Law on E-Commerce, 1996); and freedom of the parties to vary statutory provisions by agreement (section 21 ECTA; article 4 of the UNCITRAL Model Law on E-Commerce, 1996).[273]

With respect to the formation of the contract, the Court noted that there was no evidence that the e-mail reply by the applicant containing unconditional acceptance of the offer had entered the information system under the control of the intended recipient, and that therefore the contract could not be considered concluded at that moment (see section 23 (*b*) ECTA, inspired by article 15 (2) (*a*) (*i*) of the UNCITRAL Model Law on E-Commerce, 1996, but

[269] ibid.
[270] 'CLOUT case 1397 – UNCITRAL' available at https://www.uncitral.org/clout/clout/data/zaf/clout_case_1397_leg-2892.html, accessed on 06 February 2017.
[271] ibid.
[272] ibid.
[273] ibid.

adding the requirement that the message should be capable of being retrieved and processed by the addressee).[274]

The Court then stated that a message sent by SMS meets the notion of electronic communication set in the ETCA, with particular regard to the definitions of 'electronic communication' and 'data message' (drafted after Article 2 (*a*) of the UNCITRAL Model Law on E-Commerce, 1996) contained therein, and that therefore the acceptance expressed by SMS constitutes a valid method of communicating the acceptance of an offer (section 22 ECTA; see also Article 11 of the UNCITRAL Model Law on E-Commerce, 1996).[275]

3.8. Conclusion

This chapter dealt with the right to privacy and other principles of information protection. In e-commerce rightly regulated, everyone has the right to the protection of personal data concerning him or her. 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.

Due to globalization and standardization, there is a great need for South Africa to design electronic commerce regulatory framework that is in line with international standards by harmonizing its e-commerce laws with the international legal perspective on e-commerce. These international standards are not just those set by first world countries in their e-commerce regulatory framework, but includes among others e-commerce regulation adopted by international organisations to which South Africa subscribes.

[274] ibid.
[275] See Note 268 above.

CHAPTER FOUR

4. SOUTH AFRICA'S DATA PROTECTION LAWS

4.1. Introduction

Due to the consumer's online shopping activities or business transactions, consumers either advertently or inadvertently disclose personal information to other people.[1] Because of these new threats to consumers, the need for the protection of the right to privacy has led to protection of personal information becoming a basic necessity.[2] Data protection legislation is becoming more common and electronic information has become a vital corporate asset.[3]

Business practices are moving from traditional paper-based business practices that involve personal contact with clients, towards e-commerce.[4] E-commerce certainly brings new benefits to consumers and businesses alike but consumer protection remains crucial and a top priority since there is uncertainty in e-business privacy.[5]

It is just in this past century that the internet has developed so much and over the last few years the internet has developed from a glorified catalogue with companies advertising their products on a passive website, into a real marketplace with interactive websites offering a wide range of products and services, which can be ordered, paid for and sometimes even delivered on-line.[6]

---

[1] D Goodburn & M Ngoye 'Privacy and the internet' in R Buys & F Cronje (eds) Cyberlaw @ SA II: The Law of the Internet in South Africa 2 ed (2004) 171.
[2] L Swales 'Protection of personal information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' (2016) 28 (1) *SA Mercantile Law Journal* 49.
[3] ibid.
[4] R F Henschel & E B Cleff 'Information requirements and consumer protection in future m-commerce: Textual information overload or alternative regulation and communication?' (2007) 1 (1) *International Journal of Intercultural Information Management* 59.
[5] ibid.
[6] F Le Roux 'E-commerce: The legal framework' (2000) 392 *De Rebus* 25.

Because of such a development in electronic transactions, in *Heroldt v Wills*, Judge Willis commented:

> "The pace of the march of technological progress has quickened to the extent that the social changes that result therefrom require high levels of skill not only from the courts, which must respond appropriately, but also from the lawyers...."[7]

Many scholars have argued that the lack of adequate privacy protection may slow economic growth or hinder economic development because of the lack of foreign markets and consumers which is a direct result of hesitancy by consumers to transact online.[8] According to Justice Sachs in *National Coalition for Gay and Lesbian Equality v Minister of Justice*, privacy recognizes that we all have a right to a sphere of private intimacy and autonomy without interference from the outside community.[9]

When it comes to e-commerce legislation, it is true that governments, businesses and internet users in general are confronted with a range of legal issues, complicated by the unique nature of electronic communication, a medium for which existing legal rules do not always provide satisfactory answers.[10]

South Africa has no 'Data Privacy Act' yet which deals solely with data privacy matters, but certain important provisions and references to the need for personal privacy have been mentioned in several legal instruments.[11] It is the rise of electronic commerce transactions in South Africa that has led to this study of the legal issues pertaining to privacy.

---

[7] *Heroldt v Wills* 2013 (2) SA 530 (GSJ) at para 8.
[8] See Note 1 above.
[9] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 (CC) at para 32.
[10] Roux see Note 6 above.
[11] H N Olinger … et al 'Western privacy and/or ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007) 39 (1) *The International Information & Library Review* 38.

Again, it is vital to note that in South Africa, as in most countries, a plethora of national legislation has been enacted seeking to regulate various aspects of electronic communications as well as to promote data protection and hence this chapter will analyse those legislation and discuss the references made to privacy.[12]

4.2. Fiduciary Regulation of E-commerce (Privacy, Trust and Confidence)

Due to the physical location of the buyer being separate from that of the seller, as well as the physical location of the buyer and that of the merchandise, privacy, trust and confidence become a major concern in e-commerce.[13] Privacy is an issue in a virtual world where online consumers use computer systems and it plays a primary role in e-commerce.[14]

The existence of terms like 'TRUST', 'WebTrust', and 'WebAssure' is a prime indication of the expressions of privacy or trust and the importance of confidence to e-commerce.[15]

Businesses involved in e-commerce transactions ensure trust by protection of consumer's personal information (data) and thereby establishing user confidence.[16] TRUST which is one of the web seal providers has a statement on their website which reads:

> "One of the best ways to make consumers feel comfortable providing personal information and conducting transactions on the internet is to use a third-party oversight program such as TRUST's. Our oversight procedures go a long way to ease consumers' privacy concerns and to establish website credibility in the minds of your online customers and visitors."[17]

---

[12] ibid.
[13] B C Ho & K B Oh 'An empirical study of the use of e-security seals in e-commerce' (2009) 33 (4) *Online Information Review* 658.
[14] ibid.
[15] L I Rotman 'The fiduciary regulation of e-commerce' (2004) 29 *Queen's Law Journal* 739.
[16] ibid 740.
[17] "TRUSTe Oversight" available at http://www.truste.com, accessed on 16 February 2017.

Ernst & Young an accounting firm also advertised their approach on user trust when they advertised their firm in the Wired Magazine:

> "Protect your customers' privacy and transactions or you may be the one who gets burned.... If your internet customers feel exposed they'll quickly take their business elsewhere. The cyber process certification solutions that we offer, including WebTrust, help you build and maintain their trust. So you can grow your customer base and establish a competitive advantage."[18]

It is the lack of trust that is identified as the major obstacle to consumer acceptance of e-commerce.[19] With the growth of the internet and e-commerce, cyber-trust has become critical to the success of e-business and privacy protection determines the user confidence of the internet in e-commerce.[20]

Therefore it is for fiduciary trust that a reason has been created to regulate e-commerce in South Africa to establish user trust as well as user confidence.

4.3. Functions of E-commerce Legislation

Proper and functional e-commerce legislation has to serve various purposes.[21] Legal impediments to the implementation of e-commerce should be removed, certainty must be achieved as to the application of the law to e-commerce and business and consumer trust has to be enhanced.[22] Costs need to be minimized; legislation has to be applied to a wide range of transactions, facilitating both related and unrelated transactions.[23] Legislation also has to

[18] Rotman see Note 15 above at 741.
[19] T Sun 'The roles of trust and experience in consumer confidence in conducting e-commerce: A cross-cultural comparison between France and Germany' (2011) 35 (3) *International Journal of Consumer Studies* 330.
[20] ibid. See also Goodburn & Ngoye see Note 1 above.
[21] Roux see Note 6 above.
[22] ibid 26.
[23] ibid.

facilitate the cross-border recognition and the enforcement of electronic transactions and signatures with regulatory burdens minimized upon government and businesses.[24]

Leonard I Rotman stated that:

> "Although e-commerce is a relatively new phenomenon, it has quickly entrenched itself in the contemporary commercial psyche. Its rapid expansion has created new challenges for those seeking to ensure its continued vitality while simultaneously protecting the interests of its users. The trans-jurisdictional nature of e-commerce increases these challenges. For the most part, e-commerce regulation has looked to traditional methods, such as legislation, international agreements, and voluntary self-regulation (including website privacy policies and third-party webseals or trust marks).
>
> These methods do not always pay sufficient attention to the interactive nature of e-commerce transactions, and to the fact that the central issue in e-commerce regulation is fostering user confidence in the system. The fiduciary concept is concerned with maintaining the integrity of certain important relationships in a contemporary society. By focusing on the often neglected but essential human interaction component of e-commerce, the fiduciary concept could provide a valuable means of coming to grips with the problem of user confidence."[25]

It is important for South Africa to examine its existing legal rules, and amend those rules if necessary, so as to facilitate the development of e-commerce in this country, for it seems that

[24] ibid.
[25] Rotman see Note 15 above.

the UNCITRAL Model Law, as an influential example of the minimalist approach to legislation, is no longer a suitable point of departure for purposes of such an exercise.[26]

4.4. South African Legislation

E-consumer law is a branch of the *lex informatica*, otherwise referred to as cyber-law, which is not a traditional source of law but rather a new hybrid-law encompassing various pieces of telecommunications legislation as well as the common law.[27] One must also note the supremacy of the Constitution of the Republic of South Africa 1996.[28] In addition, the Constitution states that international law must be considered and foreign law may be considered in the interpretation of South African law.[29]

As was stated earlier in chapter two of this dissertation, the greatest challenge in South Africa's e-commerce is its regulation. Legislation has been put in place in South Africa as consumer-centric in order to protect consumers.

Like many other countries, the South African government recognized the need for the formation of electronic commerce policy and saw its role as an enabler, facilitator, educator and law enforcer to prevent internet crimes.[30] It was crucial that South Africa should develop a policy that is in harmony with international best practice so that it is not excluded from trading electronically with the global world.[31] South Africa therefore monitored developments and followed debates that were taking place around the world.[32]

---

[26] Roux see Note 6 above.
[27] Snail 'South African e-consumer law in the context of the ECT Act (part 1)' (2007) 15 (1) *The Quarterly Law Review for People in Business* 40.
[28] ibid 40. See section 2 of the Constitution of the Republic of South Africa, 1996.
[29] Snail 'Electronic contracts in South Africa - A comparative analysis' (2008) 2 (1) *Journal of Information, Law & Technology* 2. See section 39 of the Constitution of the Republic of South Africa, 1996.
[30] N Zantsi & M Eloff 'Guide to South African law' (2003) available at http://icsa.cs.up.ac.za/issa/2003/Publications/001.doc/, accessed on 13 February 2017.
[31] ibid.
[32] ibid.

On 4 and 5 April 2013 the *Lex Informatica* 2013: Cyber Law, ICT Law and Information Ethics Conference was held in Pretoria.[33] Andries Nel, the then Deputy Minister of Justice and Constitutional Development cited that the main objective of the convention which was then expected to be in force by 2014, was to harmonize legislation relating to electronic transactions, development of personal data protection, cyber security promotion and the fight against cyber-crime.[34]

In that same conference, Lenja Dahms-Jansen from the law firm Bowman Gilfillan encouraged employers to be aware of the following legislation: the Protection of Personal Information Bill[35], which would later become the Protection of Personal Information Act[36] on 11 April 2014, the Regulation of Interception of Communications and Provision of Communication-related Information Act[37], the Electronic Communications and Transactions Act[38], and Section 6 of the Employment Equity Act[39]. Lenja Dahms-Jansen also spoke about social media and misconduct. [40]

The famous author on cyber laws and electronic transactions, Sylvia Papadopoulos from the University of Pretoria's law faculty also spoke on the changing face of spam regulation in South Africa and stated that having different pieces of legislation dealing with spam was problematic.[41]

Another famous author on electronic transaction laws, Sizwe Snail, the director of Snail Attorneys also spoke on cyber-crime in South Africa and various sections of the ECTA

[33] K O'Reilly 'South African law coming to grips with cyber-crime: News' 2013 (530) *De Rebus* 14.
[34] ibid.
[35] Protection of Personal Information Bill B9B of 2009.
[36] Protection of Personal Information Act 4 of 2013.
[37] Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.
[38] The Electronic Communications and Transactions Act 25 of 2002.
[39] Employment Equity Act 55 of 1998.
[40] See Note 33 above.
[41] ibid.

dealing with different types of cyber-crime.[42] He also noted that there were other statutory remedies that could apply to cyber-crime.[43] These remedies included the Prevention of Organised Crime Act (POCA)[44] and the Financial Intelligence Centre Act (FICA)[45].

To conclude the above discussion, it is also worth noting that the South African data protection legislation must comply with the international data protection law standards. A case in point was when Nedbank Ltd. responded to the South African Law Reform Commission's (SALRC) issue paper in which Nedbank stated the impact of the lack of adequate data protection in South Africa on its business:

> "Nedbank has been forced, in the absence of data protection legislation locally which would have facilitated the bank processing information within South Africa, at great extra cost, to set up processing centres in Europe, in order to meet European information protection legislative requirements."[46]

In interpreting the legislation providing for the protection of data by privatising personal information, the South African case law has accepted Neethling's definition of privacy.[47] Neethling defined privacy as

> "…individual condition of life characterized by exclusion from publicity, which condition includes all those personal facts which the person himself or herself at the relevant time determines to be excluded from the

[42] ibid 14-15.
[43] ibid 15.
[44] Prevention of Organised Crime Act 121 of 1998.
[45] Financial Intelligence Centre Act 38 of 2001.
[46] South African Law Reform Commission 'Privacy and Data Protection Project 124 Discussion Paper 109' (2005).
[47] See for example *National Media Ltd v Jooste* 1996 (3) SA 262 (A) at 271; *Jooste v National Media Ltd* 1994 (2) SA 634 (C) at 645; *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T) at 384; *Bernstein v Bester* 1996 (2) SA 751 (CC) at 789; *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 (4) SA 549 (T) at 553.

knowledge of outsiders and in respect of which he or she evidences a will for privacy."[48]

4.4.1. Constitution of the Republic of South Africa, 1996

In *Heroldt v Wills* 2013,[49] the court stated that prior to South Africa's constitutional dispensation, privacy protection was entrenched by virtue of ancient common law rights. This common law right which protected the right to privacy in ancient times is known as the *actio iniuriarum*, as it protected privacy by affording a general delictual remedy for wrongs to an individual's personality.[50] This was first accepted in *O'Keeffe v Argus Printing and Publishing Co Ltd & Another*.[51]

The right to privacy is enshrined in the Constitution of the Republic of South Africa.[52] The Constitution is the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled.[53] Accordingly, the electronic communication and e-commerce industries are subject to the provisions of the Constitution.[54] This is because the right to privacy is found in the Bill of Rights of which section 8 of the Constitution states that its provisions bind the judiciary,[55] the natural persons as well as the juristic persons.[56] Although juristic persons also enjoy the rights in the Bill of Rights as stipulated by section 8,[57] in *Hyundai Motor Distributors (Pty) Ltd v Smit*, the court pointed

[48] J Neethling … et al *Neethling's Law of Personality* 2 ed (2005) 14 and 32.
[49] *Heroldt v Wills* 2013 (2) SA 530 (GSJ) at para 7.
[50] J Burchell 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* 6.
[51] *O'Keeffe v Argus Printing and Publishing Co Ltd & Another* 1954 (3) SA 244 (C) at paras 247H–249E.
[52] H N Olinger … et al 'Western privacy and/or ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007) 39 (1) *The International Information & Library Review* 38. Snail 'Electronic contracts in South Africa - A comparative analysis' (2008) 2 (1) *Journal of Information, Law & Technology* 2. See Section 14 of the Constitution of the Republic of South Africa, 1996.
[53] See section 2 of the Constitution of the Republic of South Africa, 1996. J De Waal & I Currie *The Bill of Rights Handbook* (1998) 7.
[54] C Cupido 'Electronic communications regulation' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 25.
[55] See section 8 (1) of the Constitution of the Republic of South Africa, 1996.
[56] See section 8 (2) of the Constitution of the Republic of South Africa, 1996.
[57] ibid.

out that juristic persons are not bearers of human dignity and as such, their privacy rights may be attenuated.[58]

The Constitution also gives an injunction for courts to interpret any provision or to develop common and customary law by promoting the spirit, purport, and objects of the Bill of Rights.[59] In a matter concerning the private law governing invasion of privacy in *NM v Smith (Freedom of Expression Institute as Amicus Curiae)*[60] the court examined the sweep of the common law of privacy against fundamental concepts of dignity and privacy thereby adhering to section 39 of the Constitution.[61]

In the same case *NM v Smith (Freedom of Expression Institute as Amicus Curiae)* the court stated that privacy encompasses the right of a person to live his or her life as he or she pleases.[62] The court also 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.[63]

The two important provisions when dealing with privacy issues are Section 16[64] which includes the freedom of expression and section 14[65] which provides for the right to privacy.[66]

The provisions for privacy in the Constitution place the South African government under obligation to provide the relevant legislation to protect these privacy rights of South African citizens.[67] The term 'possessions' in Section 14(*c*)[68] could be interpreted to range from tangible property through to intangible property such as personal reputation, intellectual

[58] *Hyundai Motor Distributors (Pty) Ltd v Smit* 2001 (1) SA 545 (CC) at para 18.
[59] See section 39 (2) of the Constitution of the Republic of South Africa, 1996.
[60] *NM v Smith (Freedom of Expression Institute as Amicus Curiae)* 2007 (7) BCLR 751 (CC) at para 32.
[61] See section 39 (2) of the Constitution of the Republic of South Africa, 1996.
[62] See Note 60 above at 33.
[63] ibid at 34.
[64] See section 16 (1) of the Constitution of the Republic of South Africa, 1996.
[65] See section 14 (*d*) of the Constitution of the Republic of South Africa, 1996.
[66] See Note 54 above.
[67] Olinger … et al see Note 52 above.
[68] See section 14 (*c*) of the Constitution of the Republic of South Africa, 1996.

property, personal photographs, and personality-related concepts such as personal preferences.[69]

A constitutional right is the highest form of right a citizen or juristic person may enjoy, because it binds all state organs, the judiciary and the executive to ensure these rights are protected and entrenched for citizens.[70] The right to privacy was also enshrined in the Interim Constitution of South Africa[71] Section 13: Privacy:

> "Every person shall have the right to his or her personal privacy, which shall include the right not to be subject to searches of his or her person, home or property, the seizure of private possessions or the violation of private communications."[72]

From the Interim Constitution, the current Constitution also included the right to privacy. Section 14 of the Constitution of the Republic of South Africa[73] dealing with the right to privacy is closely related to the common law right to privacy which is part of a person's *dignitas*.[74] It is the violation of the person's right to privacy and/or the disclosure of their private facts that amounts to the violation of the right to privacy as encapsulated in this section.[75]

In *Bernstein v Bester*[76] and in *National Coalition for Gay and Lesbian Equality v Minister of Justice*,[77] Ackermann J applied the constitutional right to privacy as contained in section 14 and stated that privacy extends beyond the individual's personal realm to cover autonomous

---

[69] Olinger … et al see Note 52 above.
[70] ibid. See section 8 (1) of the Constitution of the Republic of South Africa, 1996.
[71] The Interim Constitution of South Africa Act 200 of 1993.
[72] See section 13 of the Interim Constitution of South Africa Act 200 of 1993.
[73] ibid.
[74] I J Prinsloo 'How safe are South African schools?' (2005) 25 (1) *South African Journal of Education* 8.
[75] ibid 8. *NM v Smith (Freedom of Expression Institute as Amicus Curiae*) 2007 (7) BCLR 751 (CC) at paras 33 and 34.
[76] *Bernstein v Bester* 1996 (2) SA 751 (CC) at para 65 and 59.
[77] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 (CC) at para 32.

identity. In an appeal case of *Douglas v Hello!*[78] Sedley LJ pointed out personal autonomy as the essence of privacy.[79]

O'Regan J in *NM v Smith (Freedom of Expression Institute as Amicus Curiae)* said: the value we place on privacy reflects our constitutional understanding of what it means to be human.[80] Ackermann J in *Bernstein v Bester* also pointed out that the right to privacy is recognized as an independent personality right which the Courts have included within the concept of *dignitas.*[81] O'Regan J in the Constitutional court in *Khumalo v Holomisa* stated that no sharp lines can be drawn between various facets of personality rights in giving effect to the value of human dignity in our Constitution.[82]

With the right to privacy being implanted in the Constitution, it is also important to note that the Constitution also provides for the right of access to personal information.[83] Section 32 of the South African Constitution provides for the right of access to personal information,[84] which might limit the constitutional right to privacy. Although the right to privacy is embedded in the South African Constitution in section 14,[85] in *Khumalo v Holomisa*, the court stated that this right to privacy like any other right is not absolute.[86]

Ackermann J in *Bernstein v Bester* stated that 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.[87] In light of what this

[78] *Douglas v Hello!* [2001] QB 967 at 1001.
[79] Burchell 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* 12.
[80] *NM and v Smith (Freedom of Expression Institute as Amicus Curiae)* 2007 (7) BCLR 751 (CC) at para 131.
[81] *Bernstein v Bester* 1996 (2) SA 751 (CC) at paras 56 and 68.
[82] *Khumalo v Holomisa 2002* (5) SA 401 (CC) at para 27.
[83] See Note 79 above at 12.
[84] See section 32 of the Constitution of the Republic of South Africa, 1996.
[85] See Section 14 of the Constitution of the Republic of South Africa, 1996.
[86] See Note 82 above.
[87] *Bernstein v Bester* 1996 (2) SA 751 (CC) at para 67.

dissertation has shown so far, this statement by Ackermann J may also mean that the right to privacy in e-business also shrinks although he did not state under what circumstances.[88]

This approach is an echo to section 36 of the Constitution which clearly points out that rights in the Bill of Rights may be limited.[89] As noted in the paragraph above, this interpretation by Ackermann J was later reiterated in *Khumalo v Holomisa* when the court stated that this right to privacy like any other rights is not absolute.[90]

Reasonableness can be used as justification for limiting the right to privacy that a person holds.[91] O'Regan in *NM v Smith (Freedom of Expression Institute as Amicus Curiae)* also recognized that privacy must be balanced against the right to freedom of expression.[92] O'Regan also noted that the main defences to an action for invasion of privacy would be that the publication was in the public interest or that informed consent had been given.[93]

In e-commerce, the risk of invasion of the right to privacy happens if the information privacy is not protected since e-business consists mainly of the process of sending information and receiving of the same.

In *Mistry v Interim Medical and Dental Council of South Africa*, the court gave some general guidelines that govern data protection and these are:

a) was the information obtained in an intrusive manner;

b) was the information about intimate aspects of the subject's personal life;

c) was it provided for one purpose but used for another;

---

[88] ibid.
[89] See section 36 of the Constitution of the Republic of South Africa, 1996.
[90] *Khumalo v Holomisa* 2002 (5) SA 401 (CC) at para 27.
[91] Burchell see Note 79 above at 13.
[92] *NM v Smith (Freedom of Expression Institute as Amicus Curiae)* 2007 (7) BCLR 751 (CC) at para 145.
[93] ibid 154. Burchell see Note 79 above at 13.

d) was it disseminated to the press or general public from whom the subject 'could reasonably expect such information would be withheld'?[94]

The Constitution gave way to the development of the Promotion of Access to Information Act [95] which governs the right of access to all other information, the Electronic Communications and Transactions Act[96] which sets out information protection principles and the National Credit Act[97] which regulates credit information and credit bureaux.[98] These and other related legislation will be discussed briefly in light of the right to privacy, access to information and information protection with a detailed discussion of the ECTA and with specific references in some instances to e-commerce.

4.4.2. Promotion of Access to Information Act 2 of 2000

The Promotion of Access to Information Act (PAIA) was enacted to give effect to the right stipulated by section 32 of the Constitution.[99] The PAIA deals with inter alia allowing individuals access to personal information, but it does not regulate who and how that personal information may be collected and controlled by the individual.[100]

As stated in the paragraphs above, the right to privacy was enshrined in section 13 of the Interim Constitution which granted everybody the right to privacy. [101] The Interim Constitution advocated for the right to privacy, however the constitutional court when certifying the final Constitution explicitly demanded transparency.[102] The court also stated

[94] *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC) at para 23.
[95] Promotion of Access to Information Act 4 of 2000.
[96] Electronic Communications and Transactions Act 25 of 2002.
[97] National Credit Act 34 of 2005.
[98] Burchell see Note 79 above at 14.
[99] See section 32 (2) of the Constitution of the Republic of South Africa, 1996.
[100] Olinger … et al 'Western privacy and/or ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007) 39 (1) *The International Information & Library Review* 38.
[101] See section 13 of the Interim Constitution of South Africa, 1993.
[102] *In re: Certification of the Constitution of the Republic of South Africa* 1996, 1996 (10) BCLR 1253 (CC) at para 285.

that the right of access to information generally helps to achieve what is commonly referred to as good governance.[103]

The final Constitution obliged the State in section 32 (2) to enact national legislation to give effect to the right of access to information.[104] Thus by giving the right of access to information, the PAIA regularizes the need for certain justifiable limitations on privacy and/or commercial confidentiality. With the foremost objective of the PAIA being to give effect to section 32 of the Constitution,[105] the court in *S v Makwanyane and Another* stated that the PAIA has to be interpreted purposively.[106]

Although the PAIA facilitates the access to information, chapter 4 sets out some grounds for refusal of access to records.[107] A request for access to a record must be refused if its disclosure would involve the unreasonable disclosure of personal information about a third party, including a deceased individual.[108]

By permitting an individual to have access to both manual and electronic records relating to personal information, the PAIA promotes privacy or data protection.[109]

Privacy is strongly related to how personal information can be controlled by the information owner, and this provision is missing in the PAIA. It is specifically the failure of the PAIA in comprehensively addressing privacy that led to a separate Data Privacy Bill being drafted and legislated.[110]

---

[103] ibid.
[104] See section 32 (2) of the Constitution of the Republic of South Africa, 1996.
[105] ibid.
[106] *S v Makwanyane and Another* 1995 (6) BCLR 665 (CC) at para 9. See section 2(1) of the Promotion of Access to Information Act 2 of 2000.
[107] See section 34 (1) of the Promotion of Access to Information Act 2 of 2000.
[108] ibid.
[109] See sections 3-8 of the Promotion of Access to Information Act 2 of 2000.
[110] ibid.

4.4.3. Electronic Communications and Transactions Act 25 of 2002

The ECTA deals with cryptography, cyber-crime and the protection of personal information or data (privacy).[111] To specifically address electronic related commerce, the ECTA[112] was enacted to focus on establishing a framework within which e-commerce can be regulated.[113] As set out in the preamble, [114] the ECTA was also created to regulate electronic communications and transactions by advancing universal access to electronic communications and transactions.[115]

One of the supporting objectives of the ECTA is to protect individuals engaged in e-commerce and this expresses itself in Chapter 8 as a voluntary regime of data protection principles for personal information. [116] The ECTA creates technological neutrality by developing a safe and secure environment thereby promoting legal certainty and confidence in respect of electronic transactions. [117] Thus the objective of the ECTA is to facilitate electronic transactions by protecting privacy around such transactions.[118]

The ECTA comprises of 14 chapters with 95 sections, which addresses e-commerce issues such as e-government, consumer protection, privacy, cyber-crime, and liabilities of service providers, to mention a few.[119] The ECTA in e-commerce provides some obligations that are incumbent on the e-vendor that prohibit them from disclosing the e-consumer's private

[111] Z N Jobodwana 'E-commerce and mobile commerce in South Africa: Regulatory challenges' (2009) 4 (4) *Journal of International Commercial Law and Technology* 291.
[112] Electronic Communications and Transactions Act 25 of 2002.
[113] See Note 100 above.
[114] See Note 112 above.
[115] Swales 'Protection of personal information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' (2016) 28 (1) *SA Mercantile Law Journal* 68.
[116] ibid 38.
[117] W Jacobs 'The Electronic Communications and Transactions Act: Consumer protection and internet contracts' (2004) 16 (1) *SA Mercantile Law Journal* 557.
[118] Deloitte & Touche 'Legal Electronic Communications & Transaction Bill 2002. (South Africa)' (2002) available at http://www.doc.pwv.gov.za/, accessed on 13 February 2017.
[119] ibid.

information.[120] This is called a non-disclosure obligation which helps in information protection by providing data protection.[121]

The ECTA has an entire chapter that applies only to personal information obtained through electronic transactions.[122] According to section 51 of the ECTA, in order to collect, collate and process or disclose any personal information belonging to a data subject, a data controller must possess express written permission to do so.[123] If required by the law to do so, the information must be necessary for the lawful purpose for which the personal information is required.[124]

According to both the Promotion of Access to Information Act (PAIA)[125] and the ECTA[126], personal information is defined as:

> "(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;
>
> (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved:
>
> (c) any identifying number, symbol, or other particular assigned to the individual;

[120] S Snail 'An overview of South African e-consumer law in the context of the Electronic Communications and Transactions Act (part 2)' (2007) 15 (1) *Journal of Business Law* 54.
[121] ibid 54.
[122] See chapter VIII of the Electronic Communications and Transactions Act 25 of 2002.
[123] See section 51 (1) of the Electronic Communications and Transactions Act 25 of 2002.
[124] See section 51 (1) and 51 (2) of the Electronic Communications and Transactions Act 25 of 2002.
[125] Promotion of Access to Information Act 2 of 2000.
[126] Electronic Communications and Transactions Act 25 of 2002.

(d) the address, fingerprints or blood type of the individual;

(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual:

(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the individual:

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but excludes information about an individual who has been dead for more than 20 years."[127]

As stated in the paragraph above, the ECTA deals with the protection of this personal information in sections 50 and 51.[128] Section 50 gives the scope of protection of personal

[127] See section 1 of the Electronic Communications and Transactions Act 25 of 2002. See section 1 of the Promotion of Access to Information Act 2 of 2000.
[128] See Chapter VIII of the Electronic Communications and Transactions Act 25 of 2002.

information, while section 51 provides for the principles for electronically collecting personal information.[129]

Although the ECTA has been key in data protection, it however does not impose legally binding obligations on data controllers as the data controller may exclude such principles by agreement with a data subject.[130] The danger of such a provision in the ECTA is that disclosure of information is likely going to be an exception rather than the norm.

4.4.3.1. The Shortcomings of the Electronic Communications and Transactions Act 25 of 2002 on Consumer Protection

The ECTA provides for the protection of consumers in chapter 7.[131] Although the ECTA provides for the protection of all consumer electronic transactions, there are some other electronic transactions which are subject to limitations as stated in section 42.[132]

According to the ECTA, a consumer is any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier.[133]

A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction must make certain information such as its full name, physical address and telephone number available to its customers.[134] The information does not need to be

[129] See Chapter VIII Section 50 and 51 of the Electronic Communications and Transactions Act 25 of 2002.
[130] ibid.
[131] See sections 42 to section 49 of the Electronic Communications and Transactions Act 25 of 2002.
[132] See sections 42 (*a*) to 42 (*j*) to section 49 of the Electronic Communications and Transactions Act 25 of 2002.
[133] See section 1 of the Electronic Communications and Transactions Act 25 of 2002.
[134] See section 43 of the Electronic Communications and Transactions Act 25 of 2002. Jacobs 'The Electronic Communications and Transactions Act: Consumer protection and internet contracts' (2004) 16 (1) *SA Mercantile Law Journal* 558.

made available on the website itself.[135] However, the ECTA does not state that the consumer must make his information to the supplier.

Although supplier information must be provided, section 43 (1)[136] only refers to an offer and not online advertisements.[137] Thus if that provision is analysed *stricto sensu* by applying a narrow interpretation, supplier information would not be required for all advertisements where consumers have the option of making offers by placing orders, thereby putting consumers at a risk.[138]

Another challenge that chapter 7 does not deal with pertains to the uncertainty also found in section 43 (1).[139] The ECTA only shows that supplier information should be made available when goods or services are offered for sale, hire, or exchange by way of an electronic transaction.[140] The ECTA does not state if supplier information should be provided or not when goods or services are not offered on the website of the supplier, for example, when an offer and acceptance is made by e-mail.[141]

The exact meaning of goods and services as pointed out in section 43 (1)[142] is not given. There are other financial services which are excluded from the list of goods and services and yet the ECTA does not give a list of these services as is done with other electronic transactions that are listed in section 42.[143] This lack of certainty poses a challenge to the consumers since suppliers won't provide information that consumers need for privacy protection.

---

[135] Jacobs see Note 134 above at 559.
[136] See section 43 (1) of the Electronic Communications and Transactions Act 25 of 2002.
[137] Jacobs see note 134 above at 559.
[138] ibid.
[139] See Note 136 above.
[140] ibid.
[141] Jacobs see note 134 above at 559.
[142] See Note 136 above.
[143] See Note 132 above.

It is also stated in section 50 of the ECTA that a data controller may elect to subscribe to the principles outlined in section 51, which means that subscription to these principles is voluntary as the parties are only governed by the terms of their agreement.[144] This provision implies that the supplier and the consumer do not have to comply with the provisions of section 51 if they do not wish to.

4.4.3.2. The Success of the Electronic Communications and Transactions Act 25 of 2002 in Dealing with Privacy Protection

Parties cannot choose to exclude the provisions of chapter 7 by agreement.[145] Any agreement that the parties will make to exclude the requirements of chapter 7 will be invalid to the point of inconsistency.[146]

One of the legal measures that ensure the protection of data in electronic transactions is found in chapter 10 of the ECTA.[147] The existence of the provision which agitates for the protection of critical data by the establishment of the cryptography providers prevents information technology (IT) related crimes.[148]

Cryptography relates to the hiding of information such that when a message has been encrypted it is impossible for an intruder to read it. The ECTA defines a cryptography product as

> "any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring-that such data can be accessed only by relevant persons."[149]

[144] See section 50 (2) of the Electronic Communications and Transactions Act 25 of 2002.
[145] See section 48 of the Electronic Communications and Transactions Act 25 of 2002.
[146] ibid.
[147] See section 53 of the Electronic Communications and Transactions Act 25 of 2002.
[148] ibid.
[149] See Note 133 above.

The authenticity of the data, the integrity of the data or the source of the data can be correctly ascertained.[150]

In chapter VIII, according to section 51, the data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.[151] The information that is in the control of a data controller may not be disclosed to a third party and must be deleted or destroyed once it has become obsolete.[152] However the data controller can disclose information if required or permitted by law or specifically authorised to do so in writing by the data subject.[153]

The ECTA also provides for the protection of information by providing chapter XIII, which deals with the regulation of cybercrime.[154] Section 86 of the ECTA deals with the unauthorized access to, interception of or interference with data.[155] This chapter also introduces statutory criminal offences relating to information systems.[156] Thus information is protected against unauthorized access and disclosure.

4.4.4. Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002

The Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA)[157], deals with the circumstances under which electronic surveillance and interception are permitted, as well as related procedures and responsibilities.[158]

---

[150] ibid.
[151] See section 51 (4) of the Electronic Communications and Transactions Act 25 of 2002.
[152] See section 51 (6) and section 51 (8) of the Electronic Communications and Transactions Act 25 of 2002.
[153] See section 51 (6) of the Electronic Communications and Transactions Act 25 of 2002.
[154] See section 86 of the Electronic Communications and Transactions Act 25 of 2002.
[155] ibid.
[156] ibid.
[157] Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

The RICA, also known as the 'Surveillance Act,' primarily focuses on the communications aspect of privacy by prohibiting all wiretaps and surveillance of all personal communications.[159] The only exception allowed is either for law enforcement agencies to perform wiretaps during criminal investigations or when special permission has been obtained.[160]

4.4.5. National Credit Act 34 of 2005

The National Credit Act (NCA) was assented to by the president of the Republic of South Africa in March 2006.[161] In the preamble as well as in part B of the NCA, [162] it is clear that the purpose of the enactment of the NCA is to inter alia regulate credit information. Thus the NCA was enacted to promote a fair and non-discriminatory marketplace which improves the standards of consumer information.[163]

Some of the sections of the NCA came into operation in June 2006, others in September 2006 and the rest in June 2007 as the dates were fixed by proclamation by the President in terms of section 173 of the NCA.[164] As this chapter of the dissertation is dealing with personal information it is worth noting that the provisions on issues of confidentiality as well as consumer credit information came into operation on 1 September 2006.

According to part B of the NCA dealing with confidentiality, personal information and consumer credit records, any person who, in terms of this Act, receives, compiles, retains or reports any confidential information pertaining to a consumer, consumers, prospective

---

[158] Cupido 'Electronic Communications regulation' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed (2012) 27.
[159] Olinger … et al 'Western privacy and/or ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007) 39 (1) *The International Information & Library Review* 39.
[160] ibid.
[161] National Credit Act 34 of 2005.
[162] ibid.
[163] See section 3 (*f*) of the National Credit Act 34 of 2005.
[164] See section 173 of the National Credit Act 34 of 2005.

consumer or prospective consumers, must protect the confidentiality of that information.[165] To uphold the right to confidentiality, use of any information should be only for a purpose permitted or required in terms of the NCA, national legislation or provincial legislation.[166]

The use of a consumer's personal information (confidential information) is allowed only when use of the information is permitted by the NCA or any other legislation or when the consumer has consented to having their information processed.[167] Information can also be released to a third party if the release is directed by an order of a court or the Tribunal.[168]

Confidential information is defined by the NCA as any personal information that belongs to a person and is not generally available to other people or known by them.[169] Consumer credit information is also defined by the NCA as information concerning a person's credit, financial, employment, educational, professional, business, or career history.[170] This also includes information relating to identity such as name, date of birth, identity number, marital status, past and current addresses, and contact details.[171]

The challenge with the NCA when it comes to the protection of consumer information is that it does not specifically require that the purpose for which the information is collected should be spelled out before the collection takes place. That is a gap in law that allows for the misuse of information by other credit offering institutions.

Of the statutes dealing with privacy protection, the NCA is probably the most successful in its attempt to introduce data protection provisions. It proposes to deal with the security and

[165] See section 68 (1) of the National Credit Act 34 of 2005.
[166] See section 68 (1) (*a*) of the National Credit Act 34 of 2005.
[167] ibid.
[168] See section 68 (1) (*b*) (ii) of the National Credit Act 34 of 2005.
[169] See section 1 of the National Credit Act 34 of 2005.
[170] See section 70 (1) of the National Credit Act 34 of 2005.
[171] ibid.

confidentiality principle by instructing persons who receive, compile, retain or report confidential information to protect the confidentiality of that information.

4.4.6. Electronic Communications Act 36 of 2006

A number of legislative reforms undertaken since the year 2000 culminated in the adoption of the Electronic Communications Act (ECA) in 2006.[172] The ECA is the primary piece of legislation governing the substantive regulation of the electronic communications industry in South Africa.[173] The ECA regulates the convergence of technologies in the ICT sector.[174]

The ECA repealed the Telecommunications Act,[175] as well as some sections of the Broadcasting Act[176], excluding sections dealing with the public broadcaster.[177] The ECA seeks to promote convergence in the broadcasting, broadcasting signal distribution and telecommunications sectors, and to provide the legal framework for convergence of these sectors.[178]

4.4.7. Consumer Protection Act 68 of 2008

The Consumer Protection Act (CPA)[179] provides an overarching legislative and institutional framework for consumer protection and all other Acts providing for consumer protection must be read with this Act to provide a common standard for consumer protection.[180] According to section 5,[181] the CPA applies to every transaction occurring within the

[172] Electronic Communications Act 36 of 2006.
[173] Cupido 'Electronic Communications regulation' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* (2012) 25.
[174] ibid 25.
[175] Telecommunications Act 103 of 1996.
[176] Broadcasting Act 4 of 1999.
[177] Jobodwana 'E-Commerce and mobile commerce in South Africa: Regulatory challenges' (2009) 4 (4) *Journal of International Commercial Law and Technology* 291.
[178] ibid 291.
[179] Consumer Protection Act 68 of 2008.
[180] Cupido see Note 173 above.
[181] See section 5 (1) (*a*) of the Consumer Protection Act 68 of 2008.

Republic, apart from the exceptions also listed in sections 5.[182] Whether the supplier resides or has its principal office within or outside South Africa is irrelevant and insignificant.[183]

Section 1 broadly defines a transaction to include an agreement between a person acting in the ordinary course of business and another person for the supply of goods or services in exchange for consideration, as well as the supply of goods or the performance of services to a consumer for consideration.[184]

The overarching philosophy of the CPA is to protect consumers from unfair business practices and this includes electronic business or electronic transactions in which consumer information should be protected.[185] Issues of particular concern range from questions regarding consumer's financial security, data protection, protection from unsolicited information, access to adequate information, and availability of effective and affordable redress mechanisms.[186]

Section 11 of the CPA deals with the consumers' right to privacy. It states that:

> "The right of every person to privacy includes the right to -
>
> a. refuse to accept;
> b. require another person to discontinue; or
> c. in the case of an approach other than in person, to pre-emptively block, any approach or communication to that person, if the approach or communication is primarily for the purpose of direct marketing."[187]

[182] See section 5 (2)-(4) of the Consumer Protection Act 68 of 2008.
[183] See section 5 (8) (*a*) of the Consumer Protection Act 68 of 2008.
[184] See section 1 of the Consumer Protection Act 68 of 2008.
[185] Swales 'Protection of personal information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' (2016) 28 (1) *SA Mercantile Law Journal* 66.
[186] J Huffmann 'Consumer Protection in E-Commerce: An examination and comparison of the regulations in the European Union, Germany and South Africa that have to be met in order to run internet services and in particular online-shops' (unpublished LLM thesis, University of Cape Town, 2004) 4.
[187] See section 11 of the Consumer Protection Act 68 of 2008.

Marketers have an obligation to respect consumers by making sure that their personal information is protected.

4.4.8. Protection of Personal Information Act 4 of 2013

The Protection of Personal Information Act (POPI)[188] is the latest of the legislation dealing with consumer protection in South Africa. In August 2009, the Cabinet published the Protection of Personal Information Bill (PPI)[189] which is now the POPI. The POPI came into force on 11 April 2014 and it promotes the protection of personal information by public and private bodies.

In the context of electronic transactions, the promulgation of the POPI[190] follows the recent trend in South Africa of enacting consumer-centric legislation.[191] The other consumer-centric legislation is the Consumer Protection Act and the National Credit Act.[192] The POPI also came as an addition to the Protection of Access to Information Act[193] which deals with the negligent use or disclosure of information.[194]

Sachs J in *National Coalition for Gay and Lesbian Equality v Minister of Justice*[195] in analysing the South African jurisprudence in the area of privacy law explains: Privacy recognizes that we all have a right to a sphere of private intimacy and autonomy without interference from the outside community.[196]

[188] Protection of Personal Information Act 4 of 2013.
[189] Protection of Personal Information Bill B9 of 2009.
[190] See Note 188 above.
[191] See Note 185 above at 49.
[192] ibid.
[193] Promotion of Access to Information Act 2 of 2000.
[194] Olinger … et al 'Western privacy and/or ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007) 39 (1) *The International Information & Library Review* 38.
[195] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 (CC) at para 32.
[196] ibid.

In *Bernstein v Bester*,[197] the court poignantly noted that privacy is not based on a notion of the unencumbered self, but on the notion of what is necessary to have one's own autonomous identity.

Information is sacrosanct and in e-commerce, privacy relates to e-mail addresses, age, gender, sexual orientation, race, spending habits, location, medical information and any other information that will, or has the potential to identify an individual.[198] According to one of the salient provisions of the POPI, it is pointed out that personal information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.[199]

In e-commerce as mentioned in the paragraph above, this personal information may include, but is not limited to race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.[200]

The overarching principle of the POPI is safeguarding personal information of the data subject by giving effect to the constitutional right to privacy, subject to justifiable limitations.[201] Any juristic person or natural person to whom the personal information relates is the data subject.[202]

[197] *Bernstein v Bester* 1996 (2) SA 751 (CC) at para 65.
[198] See Note 185 above at 51.
[199] See section 1 of the Protection of Personal Information Act 4 of 2013.
[200] ibid.
[201] See section 2 of the Protection of Personal Information Act 4 of 2013.
[202] See Note 185 above at 59.

4.5. Conclusion

All the legislation discussed above present the myriad of laws that address information security related issues including matters of privacy.[203] These pieces of legislation place similar non-disclosure obligations on the e-vendor as regards specific disclosures.[204]

In all aspects where a person's legitimate expectation of privacy has been infringed by personal information being processed or divulged, he/she can have a remedy by relying on the law of delict, but only once active control of personal information has been established.[205]

This remedy may prevent a person from wrongfully processing or divulging personal data or continuing to divulge personal data, or the *actio iniuriarum* for a *solatium* for non-patrimonial loss in the form of injury to personality (*iniuria*) resulting from the wrongful and intentional processing of personal information, or lastly, compensation under the *actio legis aquiliae* for patrimonial loss (*damnum iniuria datum*) sustained as a result of the wrongful, negligent processing of personal information.[206]

However as stated in earlier paragraphs, the right to privacy is not absolute as was pointed in *S v Bailey*[207] in which a defendant relied on his right to privacy as a defence for not having his status furnished as compulsory information in terms of the Statistics Act.[208] The court held that interference with the plaintiff's right to privacy was lawful, because it was justified by some superior legal right, namely the Statistics Act.[209]

---

[203] R Dagada …et al 'Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant?' available at http://uir.unisa.ac.za/handle/10500/2660, accessed on 17 February 2017.
[204] Snail 'An overview of South African e-consumer law in the context of the Electronic Communications and Transactions Act (part 2)' (2007) 15 (1) *Journal of Business Law* 54.
[205] Neethling … et al *Neethling's Law of Personality* 2 ed (2005) 334ff.
[206] ibid 334 ff.
[207] *S v Bailey* 1981 (4) SA 187 (N) at 6.
[208] Statistics Act 66 of 1976.
[209] ibid.

CHAPTER FIVE

5. E-COMMERCE IN THE UNITED KINGDOM

5.1. Introduction

This chapter seeks to analyze the UK online privacy and data protection laws by discussing the Human Rights Act of 1998[1] as well as both the Data Protection Act of 1984[2] and the Data Protection Act of 1998.[3] To avoid confusion in this discussion, the Data Protection Act of 1984 will be referred to as the (1984 DPA) and the Data Protection Act of 1998 will be referred to as the (1998 DPA). A brief discussion of the Electronic Commerce (EC Directive) Regulations 2002[4] and the Privacy and Electronic Communications Regulations 2003[5] will also ensue.

This chapter will also briefly analyze other UK legislation containing some elements dealing with privacy. These Acts to be discussed are the Consumer Credit Act,[6] Rehabilitation of Offenders Act,[7] Telecommunications Act,[8] Police Act,[9] Broadcasting Act,[10] Protection from Harassment Act,[11] Access to Medical Reports Act,[12] Access to Health Records Act,[13] Health and Social Care Act[14] and the Crime and Disorder Act[15]. Although these statutes were

[1] Human Rights Act 1998, Chapter 42.
[2] Data Protection Act 1984, Chapter 35.
[3] Data Protection Act 1998, Chapter 29.
[4] Electronic Commerce (EC Directive) Regulations 2002, No. 2013.
[5] Privacy and Electronic Communications Regulations 2003, No. 2426.
[6] Consumer Credit Act of 1974, Chapter 39.
[7] Rehabilitation of Offenders Act 1974, Chapter 53.
[8] Telecommunications Act 1984, Chapter 12.
[9] Police Act 1997, Chapter 50.
[10] Broadcasting Act 1996, Chapter 55.
[11] Protection from Harassment Act 1997, Chapter 40.
[12] Access to Medical Reports Act 1988, Chapter 28.
[13] Access to Health Records Act 1990, Chapter 23.
[14] The Health and Social Care Act 2001, Chapter 15.
[15] Crime and Disorder Act 1998, Chapter 37.

enacted and adopted in the UK, some of those enacted before 1998 have now been repealed in part or replaced in full by the 1998 DPA.[16]

5.2. Common Law Protection of Privacy and Data Before the Incorporation of the Human Rights Act 1998, Chapter 42

The Human Rights Act of 1998[17] is an Act of Parliament of the UK which received Royal Assent on 9 November 1998, and mostly came into force on 2 October 2000 in Scotland and in the UK it was fully adopted and came into effect on 1 October 2001.[18]

Before the enactment of the Human Rights Act of 1998,[19] the right to privacy was protected indirectly by the common law which covered issues such as the breach of confidence, conspiracy, copyright, breach of contract, negligence, trespass, private nuisance, defamation, legal professional privilege, and certain statutory remedies.[20] Although the 1998 DPA does not abolish any of the above remedies, the protection they provide to privacy in personal information is direct, but incidental and limited.[21]

In *Malone v Metropolitan Police Commissioner*, Sir Robert Megarry held that English law did not recognize a right to privacy and that the tapping of a telephone conversation by the Post Office could therefore not amount to a breach of such a right because such a right does not exist in common law.[22] In *Attorney General v Guardian Newspapers Ltd*., the court dealt with the common law of confidentiality.[23] Lord Justice Keith pointed out that the right to

---

[16] The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 386. P Reid ''Regulating' online data privacy' (2004) 2 (3) *Script-ed Journal* 489.
[17] Human Rights Act 1998, Chapter 42.
[18] L B Cardonsky 'Towards a meaningful right to privacy in the United Kingdom' (2002) 20 (2) *Boston University International Law Journal* 399.
[19] Human Rights Act 1998, Chapter 42.
[20] L B Cardonsky 'Towards a meaningful right to privacy in the United Kingdom' (2002) 20 (2) Boston University International Law Journal 399.
[21] A Roos 'The law of data (privacy) protection: A comparative and theoretical study' (unpublished LLD dissertation, University of South Africa, 2003) 247.
[22] *Malone v Metropolitan Police Commissioner* (No2) [1979] 2 All ER 620 at para 2.
[23] *Attorney General v Guardian Newspapers Ltd*. No. 2, 1 A.C. 109 (H.L. 1990).

personal privacy must be protected by the law.[24]

The old English case of *Kaye v Robertson* [1991] FSR 62, reiterated the sentiments of *Malone v Metropolitan Police Commissioner*[25] by pointing out that in English law, common law does not recognize a general right to privacy.[26] Glidewell, LJ stated that:

> "It is ... invasion of privacy which underlies the plaintiff's complaint. Yet it alone, however gross, does not entitle him to relief in English law"[27]

Although the UK common law does not protect and does not provide for a specific right to privacy, infringement of privacy could be actionable at common law if a breach of confidence could be proved.[28] In *Terrapin v Builders' Supply Co (Hayes) Ltd*,[29] the court stated that under the rules of 'equity', one who receives information under express or implied conditions of confidence is under a duty not to reveal it without consent.[30]

In two other separate cases, the court also stated that under the rules of 'equity', an action may also be brought for breach of commercial confidence where a person uses another's confidential material for his own commercial gain.[31]

Using the principles set forth in the case of *Morison v Moat*, in *Thomas Marshall (Exporters) Ltd v Guinle*,[32] commercial information such as the names and telex addresses of the company's manufacturers and suppliers and their individual contacts; details of the company's current negotiations; information as to the requirements of the company's customers; the

---

[24] ibid.
[25] *Malone v Metropolitan Police* Commissioner (No2) [1979] 2 All ER 620.
[26] *Kaye v Robertson* [1991] FSR 62, 70.
[27] ibid.
[28] *Saltman Engineering v Campbell Engineering* [1948] 65 RPC 203.
[29] *Terrapin v Builders' Supply Co (Hayes) Ltd* [1967] RPC 375.
[30] See also *Attorney General v Guardian Newspapers* (No 2) [1990] 1 AC 109 at 281.
[31] *Morison v Moat* [1851] 9 Hare 241. See also *Saltman Engineering v Campbell Engineering* [1948] 65 RPC 203.
[32] *Thomas Marshall (Exporters) Ltd v Guinle* [1978] 3 WLR 116.

company's new ranges, actual or proposed, the company's samples and negotiated prices paid to the company by customers were held to be capable of being confidential.[33]

In *Prince Jefri Bolkiah v KPMG*, the duty of confidence was also said to arise from any type of a professional relationship like that between an employer and an employee.[34] In turn, in *Golder v United Kingdom*, the court also stated that a prisoner has a resounding right to communicate with his or her lawyer.[35]

The professional relationship of a lawyer is seen in *Lord Ashburton v Pape*, which established that a solicitor has a duty of confidentiality in respect of any information received directly from a client.[36] In *Hunter v Mann*, the professional relationship of medical practitioner was described as a duty of a doctor not to disclose information obtained in his professional capacity without the affirmed consent of his or her patient.[37] The professional relationship in *Tournier v National Provincial and Union Bank of England* was said to be an implied term in the banker's contract with the customer that the banker shall not disclose the customers' accounts and transactions arising thereto.[38]

In *Francome v Mirror Group Newspapers Ltd*, the defendant eavesdropped on a telephone conversation using a radio-telephone to gain access to a private conversation.[39] The court pointed out that in circumstances where there is no professional relationship existing, the courts will give the duty of confidence if the information is confidential and there is a need to protect the privacy of another person.[40]

---

[33] ibid.
[34] *Prince Jefri Bolkiah v KPMG* [1999] 1 All ER 577.
[35] *Golder v United Kingdom* (1975) 1 EHRR 524.
[36] *Lord Ashburton v Pape* [1913] 2 Ch 469.
[37] *Hunter v Mann* [1974] 1 QB 767.
[38] *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461.
[39] *Francome v Mirror Group Newspapers Ltd* [1984] 1 WLR 892.
[40] ibid.

The English common law recognized the protection of privacy rights that is substantive in protecting the right not to disclose confidential information on family relationships.[41] The case of *Argyll v Argyll,* applied this substantive common law when dealing with the Duchess of Argyll and the Duke of Argyll in a case relating to trust and personal privacy in the marriage.[42] The court gave an injunction preventing one spouse from disclosing to the public any of the intimate details of their marriage.[43] The court in *Moore v East Cleveland* rejected the definition of family unit which limits 'family' to occupancy of a dwelling to members of the same family.[44]

In *A v B,* the UK went on to expand the ground which common law covers in protecting privacy by allowing a professional football player to prohibit a certain newspaper company from publishing information about his extra-marital affair.[45] The court in this and other cases of a similar nature stated that confidences must refer to information which is not in the public domain.[46]

For that information to be disclosed there must be some form of relationship between the discloser of the information (the data controller) and recipient of that information (the data receiver), unless if consent has been given by the interested party (the data subject).[47]

5.3. The Data Protection Act 1984 and The Data Protection Act 1998

To investigate invasions of privacy in the private sector, Sir Kenneth Younger was appointed by the UK government to lead a committee in the late 1960s known as the Privacy Committee

[41] *Argyll v Argyll,* [1965] 2 W.L.R. 790 (Chancery Div.).
[42] ibid.
[43] ibid.
[44] *Moore v East Cleveland* (1977) 431 US 494, 52 LEd 2d 531, 97 SCt 1932.
[45] *A v B* [2001] 1 All ER 449 (QB).
[46] Cardonsky 'Towards a meaningful right to privacy in the United Kingdom' (2002) 20 (2) *Boston University International Law Journal* 400.
[47] ibid.

of the Society of Conservative Lawyers (Conservative Political Centre).[48] Following the committee's report, the government issued two white papers on privacy.[49]

The Privacy Committee of the Society of Conservative Lawyers, when discussing the price of privacy in July 1971, called for legislation from the government which would protect personal information by introducing the right to privacy.[50] The call was made because of the increase of personal information being stored on computers.[51]

It was the USA, California case of *Kerby v Hal Roach Studios* from which the Privacy Committee of the Society of Conservative Lawyers coined their definition of what was to be privacy in the UK.[52]

In *Kerby v Hal Roach Studios*, the court defined the right to privacy by stating that:

> "Privacy is the right to live one's life in seclusion, without being subjected to unwarranted and undesired publicity. In short, it is the right to be left alone."[53]

The UK government also adopted the privacy concept by the European Convention of Human Rights[54] which was also implemented from the Human Rights Act of 1998.[55] Article 8 of the Convention provides:

> (1) "Everyone has the right to respect for his private and family life, his home and his correspondence."[56]

---

[48] V Collins 'Privacy in the United Kingdom: A Right conferred by Europe?' (1994) 1 (3) *International Journal of Law and Information Technology* 291.
[49] See White paper 'Computers and Privacy' (Cmnd 6353), (1975) and the 'Computers: Safeguards for Privacy' (Cmnd 6354), (1975).
[50] See Note 48 above at 292.
[51] At 291-292.
[52] *Kerby v Hal Roach Studios* (1942) 53 Cal App 2d 207.
[53] Supra at 210. See also *Olmstead v United States* 277 US 438 at 478.
[54] See Article 8 of The European Convention on Human Rights 1953.
[55] P Reid ''Regulating' online data privacy' (2004) 2 (3) *Script-ed Journal* 490.

Another committee which was set up by the UK government was the Data Protection Committee chaired by Sir Norman Lindop to safeguard individual privacy and it reported in 1978.[57]

The UK does not have a written Constitution and their common law does not in any way recognize the right to privacy.[58] For this reason, after consulting with all the various committees[59] the UK government, established the Data Protection Act of 1984[60] which was created and adopted for the protection against any misuse of data or information in the automated processing of personal information.[61]

Before the 1984 DPA was enacted, the UK had no legislation giving individuals the right to privacy although it had already been a party to treaties that recognized the right to privacy.[62] In order to protect individual's personal information, the 1984 DPA accorded every person the right to have their data held by another person protected.[63]

In July 1998, the 1998 DPA was approved by parliament and in March 2000 it was signed into law as an update of the 1984 DPA.[64] This was a way of aligning the United Kingdom privacy and data protection laws with the European Union Data Protection Directive (95/46/EC) of 24 October 1995 which deals with basic privacy rights when processing personal data since the 1984 DPA only regulated the use of automated files about

---

[56] See Article 8 of The European Convention on Human Rights 1953.
[57] 'Report of the Committee on Data Protection' (Cmnd 7341), (1978).
[58] The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 385. See also *Kaye v Robertson* [1991] FSR 62, 70 and *Malone v Metropolitan Police Commissioner* (No2) [1979] 2 All ER 620.
[59] See for example, the Younger Committee, the Lindop Committee and the Privacy Committee of the Society of Conservative Lawyers.
[60] Data Protection Act 1984, Chapter 35.
[61] E Taylor 'UK schools, CCTV and the Data Protection Act 1998' (2011) 26 (1) *Journal of Education Policy* 3.
[62] Collins 'Privacy in the United Kingdom: A right conferred by Europe?' (1994) 1 (3) *International Journal of Law and Information Technology* 290.
[63] ibid 290.
[64] The South African Law Reform Commission 'Discussion Paper: Privacy and Protection' (2006) 385. Taylor see note 61 above.

individuals.[65]

This European Union Data Protection Directive (95/46/EC) was supposed to be implemented by member states before 24 October 1998 and it was only Sweden which met the deadline.[66]

The purpose of this dissertation prohibits an exhaustive discussion of the entire 1998 DPA; therefore attention will only be given to sections as well as schedules that are of particular interest in relation to online privacy protection.

5.3.1. Applicability of the Data Protection Act of 1998 in the UK

Unlike the 1984 DPA which only regulated the use of automated files about individuals, the 1988 DPA applies to paper-based records as well as automated or electronic records.[67] However, a number of the basic provisions of the 1984 DPA and the 1998 DPA are similar.

'Data' according to the 1998 DPA means information which:

> "(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;or (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)"[68]

[65] ibid. See also D Beyleveld 'Data protection and genetics: Medical research and the public good' (2007) 18 (1) *King's Law Journal* 276
[66] Reid ''Regulating' online data privacy' (2004) 2 (3) *Script-ed Journal* 492.
[67] See Section 1 (1) of the Data Protection Act 1998, Chapter 29.
[68] ibid.

Data as defined in the 1998 DPA refers to paper-based records as well as automated or electronic records and applies to information that is being processed whether the information is in the process of being recorded or already exists in recorded form.[69]

5.3.2. Personal Data and Sensitive Personal Data

The 1998 DPA [70] distinguishes between personal data and sensitive personal data. [71] Conditions applied to sensitive personal data are much stricter than those applied when processing just personal data.[72] In *Michael John Durant v Financial Services Authority*,[73] the court pointed out that sensitive personal data according to the 1998 DPA is not just data in digital form, but includes manual data that is structured and readily accessible.[74]

According to the 1998 DPA, sensitive personal data is information relating to a data subject's race, ethnicity, political opinions, religious beliefs or information of such a nature and the physical or mental condition of a data subject. [75] It also includes the sexual life and commission or alleged commission of any offence by the data subject.[76]

According to Lorber:

> "The concept of 'personal data' is fundamental to data protection legislation. If data is personal, a data controller has strict duties with which it must comply; if data is not personal, no data protection duties apply and, subject

[69] ibid.
[70] Data Protection Act 1998, Chapter 29.
[71] R Ananthapur 'India's new data protection legislation' (2011) 8 (2) *Script-ed Journal* 195. See Section 1 of the Data Protection Act 1998, Chapter 29.
[72] See Section 1, schedule 2 & schedule 3 of the Data Protection Act 1998, Chapter 29.
[73] *Michael John Durant v Financial Services Authority* [2003] EWCA Civ 1746; [2004] FSR 28.
[74] See Section 1 (*c*) of the Data Protection Act 1998, Chapter 29.
[75] See Part I, Section 2 of the Data Protection Act 1998, Chapter 29.
[76] ibid.

> of course to any other legal constraints, the data controller can do whatever it likes with the data."[77]

If the data in question is not 'personal data', it is considered too wide in scope to protect it as private information and if data is 'personal data' there is a danger of failing to give enough protection since the scope of information protection will be too narrow.[78] The reason why the 1998 DPA[79] distinguishes between sensitive personal data and just personal data results from a judgement handed down in *Michael John Durant v Financial Services Authority*[80] in which the court gave a narrow interpretation of personal data.[81]

The Data Protection Directive (95/46/EC 24 October 1995) from which the 1998 DPA adopted some of its sections on privacy, defined personal data as any information relating to an identified or identifiable natural person (data subject).[82] It also defines an identifiable person as a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[83]

The 1998 DPA also defines personal data as information which relates to a living individual who can be identified from the data and other information which is in the possession of, or is likely to come into the possession of a data controller and includes any expression of opinion about the individual.[84] It is noteworthy that personal data must relate only to a person who is alive.

---

[77] S Allison 'The concept of "personal data" under the data protection regime' (2009) 48 (1) *Edinburgh Student Law Review* 48. S Lorber 'Data protection and subject access requests' (2004) 179 (1) *International Law Journal* 183.
[78] Allison see note 77 above.
[79] See Section 2 of the Data Protection Act 1998, Chapter 29.
[80] *Michael John Durant v Financial Services Authority* [2003] EWCA Civ 1746; [2004] FSR 28.
[81] Allison see note 77 above.
[82] See Chapter 1, Article 2 (a) of the Data Protection Directive (95/46/EC 24 October 1995).
[83] ibid.
[84] See Section 1 (1) of the Data Protection Act 1998, Chapter 29.

It can be noted that the two definitions above are very similar and they mean one and the same thing, although the wording is not alike. However the definition in the 1998 DPA[85] added the phrase 'likely to come into the possession of'.[86] This would mean that, if a data controller possesses an encrypted database but does not possess, or is unlikely to come into possession of, the key for decryption, then the information will not constitute personal information.[87]

The 1998 DPA gives the data subject the right to have access to their data being processed by the data controller or on behalf of that data controller.[88] Although this section presents the presumption that a data subject must be informed about any data involving them, the right to access of information is not absolute due to a number of miscellaneous exemptions set out in schedule 7.[89]

The 1998 DPA also specifies that:

> "Unless the context otherwise requires—
>
> (a) 'obtaining' or 'recording', in relation to personal data, includes obtaining or recording the information to be contained in the data, and
>
> (b) 'using' or 'disclosing', in relation to personal data, includes using or disclosing the information contained in the data."[90]

[85] See Section 1 (1) of the Data Protection Act 1998, Chapter 29.
[86] Allison 'The concept of "personal data" under the data protection regime' (2009) 48 (1) *Edinburgh Student Law Review* 48.
[87] ibid 52.
[88] See Section 7 (1) (*a*) of the Data Protection Act 1998, Chapter 29.
[89] C McDougall 'An introduction to the Data Protection Act 1998 and the Freedom of Information Act 2000: Part I' (2002) 7 (1*) Judicial Review* 204. See also Schedule 7 of the Data Protection Act 1998, Chapter 29.
[90] See Section 1 (2) (*a*) and 1 (2) (*b*) of the Data Protection Act 1998, Chapter 29.

5.3.3. Data subject, Data Controller and Data Processor

The 1998 DPA also defines a "data subject" as an individual who is the subject of personal data.[91] The definition given by the 1998 DPA allows third parties about whom personal information is processed, to be regarded as data subjects.

The 1998 DPA also defines a "data controller"

> "as 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".[92]

A "data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.[93]

5.3.4. E-commerce and Medical Privacy Rights

In *R v Dep't of Health ex parte Source Informatics Ltd.*, the British Appellate court held that, for whatever purpose they wish, pharmacists can use a patient's personal data even without authorization or consent.[94] This includes online information submitted by a patient when making a medical transaction.[95] Data that could be obtained included but is not limited to the physician's name, the date of prescription, the product and the quantity prescribed.[96]

---

[91] See Section 1 (1) of the Data Protection Act 1998, Chapter 29.
[92] ibid.
[93] ibid.
[94] *R v Dep't of Health ex parte Source Informatics Ltd.*, [2000] 1 All E.R. 786 (C.A.), rev'g 4 All E.R. 185 (Q.B. 1999) at 796-97. I Walden 'Anonymising personal data' (2002) 10 (2) *International Journal of Law and Information Technology* 224.
[95] ibid at 797.
[96] Y F Dunkel 'Medical privacy rights in anonymous data: Discussion of rights in the United Kingdom and the United States in light of the source informatics cases' (2001) 23 (41) *The Loyola of Los Angeles International and Comparative Law Review* 42.

This was countered by the British Department of Health which issued a policy prohibiting any pharmacist from selling any patient's information relating to prescription data.[97] The British Department of Health Policy on disclosure of information stated:

> "Under common law... the general rule is that information given in confidence [by a patient] may not be disclosed without the consent of the provider of the information."[98]

This policy document resulted in the doctors and pharmacists refusing to sell prescription drug information to any data collection companies such as (Source Informatics Limited) for fear it would result in the breach of confidence of the patients.[99] The court agreed with the policy document by dismissing an appeal made by Source Informatics Limited and it reiterated the policy document's position by stating that use by the pharmacist of confidential information was a clear breach of confidence.[100]

This position follows the 1998 DPA which stated that information must only be used for the purposes for which it was obtained and any use contrary to this provision amounts to a breach unless if consent was given for another purpose other than the one for which it was originally intended.[101]

---

[97] ibid.
[98] ibid.
[99] ibid.
[100] ibid.
[101] See Schedule 2 and Schedule 3 of the Data Protection Act 1998, Chapter 29.

5.3.5. Lack of a Definition of Consent in the Data Protection Act of 1998 and the Processing of Personal Data for Direct Marketing in E-Commerce

The 1998 DPA and the Privacy and Electronic Communications Regulations 2003[102] only allow the processing of personal information by the data controller if consent has been given by the data subject.[103]

Although the word 'consent' is mentioned in Schedule 2 of the 1998 DPA as a condition for processing personal information, it is however not defined in the same Act.[104] Schedule 1 of the 1998 DPA states that:

> "In determining for the purposes of the first principle [i.e. the fairness principle] whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed."[105]

The lack of the definition of 'consent' in the 1998 DPA does not, however, make the processing of information without consent legal since schedule 1 does state that the personal data must be obtained and processed fairly.[106] The inclusion of this schedule in the 1998 DPA implies that consent of the data subject must be given freely and that the consent must be an informed one before personal data is processed.[107]

---

[102] Privacy and Electronic Communications Regulations 2003, No 2426.
[103] A Mitton 'Data protection and web 2.0: Whose data is it anyway?' (2007) 3 (1) *Convergence* 94. See also Schedule 2 of the Data Protection Act 1998, Chapter 29.
[104] Kosta 'Construing the meaning of "opt-out"- An analysis of the European, U.K. and German data protection legislation' (2015) 1 (1) *European Data Protection Law* 21.
[105] See Schedule 1 of the Data Protection Act 1998, Chapter 29.
[106] See Note 104 above.
[107] ibid.

It therefore follows that any processing of personal data without the consent of the concerned individual amounts to the invasion of privacy.[108] The only exception is if, and only if, this is done following the exemptions stipulated in part four of the 1998 DPA.[109]

5.3.6. Implied Consent in Data Processing

The 1998 DPA prohibits the data controller from processing or from beginning to process personal data belonging to a data subject if that data subject through a notice writes to him or her ordering that he/she stop processing or begin to process the data for direct marketing.[110] According to the 1998 DPA, direct marketing means the communication by whatever means of any advertising or marketing material which is directed to particular individuals.[111]

With the business-oriented approach adopted by the UK construing 'opt-out' as an implied consent in which if the data subject does not take actions (for example, failure to tick a box) consent would be assumed.[112] The 'opt-out consent' as it is known in the UK literature must not be in fine print for it to be accepted as a valid consent since the data subject may not have been able to read the material sentence or may not have seen the box at all.[113]

The UK Information Commissioner stated that organizations should not infer consent if an individual does not respond to an electronic mail communication.[114] The UK Information Commissioner however also stated that when the sender has clearly given the opportunity to the potential recipient to object to receiving unsolicited electronic communications and the

[108] ibid.
[109] See part IV (Section 27 to Section 39) of the Data Protection Act 1998, Chapter 29.
[110] See Section 11 (1) and 11 (2) of the Data Protection Act 1998, Chapter 29.
[111] See Section 11 (3) of the Data Protection Act 1998, Chapter 29.
[112] Kosta 'Construing the meaning of "opt-out"- An analysis of the European, U.K. and German data protection legislation' (2015) 1 (1) *European Data Protection Law* 23.
[113] R Jay *Data Protection Law and Practice* 3 ed (2007) 65.
[114] See Note 112 above.

latter does not make use of this option, consent can then be implied thus supporting the position of the 1998 DPA.[115]

Besides an opportunity being given to opt out before personal information is processed, the information must not be sensitive personal data.[116] As stated in paragraphs above, sensitive personal data is described in the 1998 DPA as consisting of information relating to the data subject's race, ethnicity, political opinions, religious beliefs or information of such a nature and the physical or mental condition of a data subject.[117] It also includes the sexual life and commission or alleged commission by him of any offence by the data subject.[118]

5.4. Human Rights Act 1998

As mentioned in the paragraphs above, the Human Rights Act of 1998[119] is an Act of Parliament of the UK which received royal assent on 9 November 1998, and came into force on 2 October 2000 in Scotland and in the UK it came into effect on 1 October 2001.[120] In 2001, the Human Rights Act of 1998[121] was finally enacted fully adopted in the UK.[122]

In *Earl and Countess Spencer v United Kingdom Applications* Nos 28851/95 and 28852/95,[123] the application was deemed inadmissible because the domestic law remedies had not been exhausted.[124] Prior to the adoption and enactment of the Human Rights Act of 1998[125] in the UK, any applicant who wished to sue someone for violating their privacy right,

---

[115] ibid 23.
[116] I Lloyd *Information Technology Law* 5 ed (2008) 32-33.
[117] See Part I, Section 2 of the Data Protection Act 1998, Chapter 29.
[118] ibid.
[119] Human Rights Act 1998, Chapter 42.
[120] Cardonsky 'Towards A meaningful right to privacy in the United Kingdom' (2002) 20 (2) *Boston University International Law Journal* 399.
[121] See Note 119 above.
[122] See Note 120 above.
[123] *Earl and Countess Spencer v United Kingdom Applications* Nos 28851/95 and 28852/95.
[124] ibid.
[125] See Note 119 above.

could appeal to the European Court of Human Rights provided all the available domestic law remedies had been exhausted.[126]

Section 2 (1) of the Human Rights Act of 1998[127] states that the court in dealing with matters concerning human rights must consider judgements, decisions, declarations, and advisory opinions of the European Convention on Human Rights,[128] and any other relevant opinions and decisions as set out in Section 2 (1) (*b*) to (*d*) of the Human Rights Act 1998.[129]

It was the case of *Kaye v Robertson* which depicted the need to enumerate the right to privacy in the UK since there is no Constitution to guarantee this right at any moment.[130] The English actor Kaye had undergone brain surgery and during his recovery, he was unable to prevent an interviewer from entering his hospital room to conduct an interview since he was heavily sedated. [131] While ignoring all the notices outside the hospital room forbidding entry, Robertson proceeded with the interview on behalf of Sunday Sport.[132]

The case was brought before the court by Kaye in order to stop Sunday Sport from publishing the interview and the pictures, but the court nevertheless did not grant the interdict sought after.[133] It pointed out that while there was indeed the invasion of privacy, there was no legislation which guaranteed the right to privacy.[134]

---

[126] F O Laosebikan 'Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in internet Cafes and Suggestions for Appropriate Legislation in Nigeria' (unpublished LLD dissertation, University of KwaZulu-Natal, 2007) 107.
[127] See Note 119 above.
[128] See Article 8 of The European Convention on Human Rights 1953.
[129] See Section 2 (1) (*b*) to (*d*) of the Human Rights Act 1998, Chapter 42. Laosebikan see Note 137 above.
[130] *Kaye v Robertson* [1990] F.S.R. 62, 71 (CA).
[131] ibid.
[132] ibid.
[133] ibid.
[134] ibid.

The UK introduced the right to privacy by incorporating the European Convention on Human Rights [135] (ECHR) (formally the Convention for the Protection of Human Rights and Fundamental Freedoms) into law.[136] The European Convention on Human Rights guarantees individuals a general right to privacy and since its adoption by the UK into law, it has provided for rights to be directly enforced by the UK government.[137] The Human Rights Act of 1998 incorporates the European Convention on Human Rights which protects privacy in articles 8 (1) and 8 (2).[138]

Domestic courts in the UK now apply article 8 of the European Convention on Human Rights which provides for a right to respect one's "private and family life, his home and his correspondence".[139] Both article 8 of the European Convention on Human Rights and the Human Rights Act of 1998 however do not provide for the extent of the right to privacy over the right of freedom of expression.[140] Due to the application of article 8 of the European Convention on Human Rights in the UK, the courts have, as stated in *Douglas v Hello! Ltd*

> "…reached a point at which it can be said with confidence that the law recognizes and will appropriately protect a right of personal privacy."[141]

Article 8 of the European Convention on Human Rights extends to protect an individual from the acts of other individuals.[142] This means that the Human Rights Act of 1998 also applies to relationships vertically as well as horizontally.

---

[135] See Note 128 above.
[136] Cardonsky See Note 120 above at 393. S Haenggi 'The right to privacy is coming to the United Kingdom: Balancing the individual's right to privacy from the press and the media's right to freedom of expression' (1999) 531 (1) *Journal of International Law* 533.
[137] Haenggi ibid.
[138] See Schedule 1, part 1 aa 8 (1) and (2) of the Human Rights Act of 1998, Chapter 42.
[139] Cardonsky see Note 120 above at 394.
[140] ibid 394.
[141] *Douglas v Hello! Ltd* [2001] Q.B. 967, 997 (Eng. C.A.).
[142] *X and Y v The Netherlands* (1986) 8 EHRR 235 at para 23.

Halford v United Kingdom was the leading case in the application of article 8 to the workplace.[143] Alison Halford, the assistant chief constable of the Merseyside Police, had a telephone at work which was designated for her personal use but subject to covert monitoring by the police authority in order to gain information about a sex discrimination case which Ms Halford was bringing against them.[144]

The court found that the employer breached the employee's right to respect for private life and correspondence which is a right guaranteed by article 8 of the European Convention on Human Rights.[145] The decision was based on the reasonable expectation that such calls would remain private.[146] Although the Human Rights Act of 1998 was created to govern the relationships between the state and the individuals, since its adoption by the UK legislature, it also applies horizontally in private actions.[147]

According to the jurisprudence developed by the European Court of Human Rights, when sensitive personal data (which includes health data, hence genetic data for medical research) is processed without explicit consent, article 8.1 of the European Convention on Human Rights is engaged.[148] This means that if there is explicit consent, there is no breach of privacy or confidentiality and in effect, the duties that would otherwise arise are negated, and no justification is required for the action in question.[149]

However, if there is no explicit consent, then *prima facie* duties exist and there will be a breach of privacy or confidentiality unless justification can be found under article 8.2 for

[143] *Halford v United Kingdom* [1997] IRLR 471.
[144] J Mann 'Privacy at work in the United Kingdom' (2002) 1 (1) *International Business Lawyer* 151.
[145] ibid.
[146] ibid.
[147] Cardonsky 'Towards a meaningful right to privacy in the United Kingdom' (2002) 20 (2) Boston University International Law Journal 404.
[148] See for example *Z v Finland* (1998) 25 EHRR 371 and *MS v Sweden* (1999) 28 EHRR 313.
[149] Beyleveld 'Data protection and genetics: Medical research and the public good' (2007) 18 (1) *King's Law Journal* 284.

breaching or overriding the right enshrined in article 8.1 which was adopted by the United Kingdom as binding legislation.[150]

Section 2 (1) and section 8 of the Human Rights Act of 1998 give the domestic courts the power to give an order or to grant any remedies or relief for a breach of the rights given by the European Convention on Human Rights provided that such order, right or relief is within the powers of the court.[151]

Section 3 of the Human Rights Act points out that when interpreting any legislation, interpretation given to any such act must favour the provisions of the European Convention on Human Rights.[152] However, any interpretation given which is incompatible with the European Convention on Human Rights is not rendered invalid due to its incompatibility.[153]

According to section 6 of the Human Rights Act, that unless a statute positively prevents it, public authorities and courts must apply the European Convention on Human Rights.[154] If there is an inconsistency between the Human Rights Act of 1998 and the European Convention on Human Rights provisions, the Human Rights Act will take priority over the European Convention on Human Rights to the point of the inconsistency.[155]

5.4.1. Effectiveness of the Human Rights Act 1998

The Human Rights Act of 1998 is only enforceable against public authorities, thus limiting the protection of the right to privacy by the Human Rights Act of 1998 as it essentially strengthens the rights of individuals against the state and not individuals.[156] However, in *Douglas v Hello!*, the court took into account the provisions of the Human Rights Act of

[150] ibid 284.
[151] See Section 2 (1) and Section 8 of the Human Rights Act 1998, Chapter 42.
[152] See Section 3 of the Human Rights Act 1998, Chapter 42.
[153] ibid.
[154] See Section 6 of the Human Rights Act 1998, Chapter 42.
[155] ibid.
[156] ibid.

1998 and article 8 of the European Convention on Human Rights, although the action was brought against a newspaper company and not against the government.[157]

The Human Rights Act of 1998 is also less effective because of its implementation mechanism and weak remedial scheme, since, according to the Human Rights Act of 1998, a person who feels aggrieved by an act or omission on the part of a public authority which is in contravention of any right in terms of the European Convention on Human Rights, may challenge the act or omission in court.[158] The public authority is exposed to criminal penalties if found to have acted outside the confines of the European Convention on Human Rights.[159] The court in circumstances like the one above, may, within its normal powers, grant a remedy that it considers reasonable and appropriate.[160]

The Human Rights Act of 1998 is also less effective in circumstances where the legislation is incompatible with the European Convention on Human Rights and a declaration of incompatibility is made.[161] Even though a declaration of incompatibility is pronounced, such a declaration does not change the law, or its validity, or continuing operation, neither is it binding on the parties to the proceedings.[162] This is only left to the parliament to change the law or the minister may by order amend the offending legislation.[163]

5.5. The Electronic Commerce (EC Directive) Regulations 2002

Modelled after the European Union Electronic Commerce Directive 2000, The Electronic Commerce (EC Directive) Regulations 2002 were published in 2002 by the UK government

[157] *Douglas v Hello! Ltd* [2001] QB 967, [2001] 2 WLR 992, [2002] 1 FCR 289, [2001] 1 FLR 982, Ca.
[158] See Section 7 of the Human Rights Act 1998, Chapter 42.
[159] See Section 6 (7) of the Human Rights Act 1998, Chapter 42.
[160] See Section 8 (1) of the Human Rights Act 1998, Chapter 42.
[161] See Section 4 of the Human Rights Act 1998, Chapter 42.
[162] See Section 4 (6) of the Human Rights Act 1998, Chapter 42.
[163] See Section 10 of the Human Rights Act 1998, Chapter 42.

and it applies to virtually every electronic business.[164] The Electronic Commerce (EC Directive) Regulations 2002 were established to harmonise the rules regulating electronic commerce throughout Europe by implementing the European Union's Electronic Commerce Directive 2000 into the UK law.[165]

The main objective of the Electronic Commerce (EC Directive) Regulations 2002 is to bolster the single market by ensuring the free movement of "information society services" (ISSs) across the European Economic Area and to encourage greater use of e-commerce by clarifying the rights and obligations of businesses and consumers.[166]

The Electronic Commerce (EC Directive) Regulations 2002 only apply to people who are involved in the sale of goods or services to businesses or consumers on the internet or by email or those who advertise on the internet or by email.[167] The Electronic Commerce (EC Directive) Regulations 2002 apply only to online trade and advertising and do not apply to online activities that are not of a commercial nature.[168]

Anyone who provides or receives a service normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data and at the individual request of the recipient is bound by the provisions of The Electronic Commerce (EC

---

[164] 'The UK's E-Commerce Regulations' available at https://www.out-law.com/page-431, accessed on 27 June 2017. See also Regulation 1 (1) and 1 (2) of the The Electronic Commerce (EC Directive) Regulations 2002, No. 2013.
[165] Regulation 1 (1) and 1 (2) of the Electronic Commerce (EC Directive) Regulations 2002, No. 2013.
[166] M Turner … et al 'E-commerce Directive - UK implementation. Electronic Commerce (EC Directive) Regulations 2002 - Worth the wait?' (2002) 18 (6) *Computer Law & Security Report* 396.
[167] 'A Guide for Business to the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013) 31 July' at 4 available at http://webarchive.nationalarchives.gov.uk/20121212135622/ http:/www.bis.gov.uk/files/file14635.pdf, accessed on 28 June 2017.
[168] ibid at 5.

Directive) Regulations 2002.[169] As entailed in chapter two of this thesis, online commercial activities entail a business-to-business as well as any business-to-consumer online services.[170]

Put in e-commerce terms, every company which operates a virtual world website must comply with the provisions of The Electronic Commerce (EC Directive) Regulations 2002, if that virtual website offers merchandise or services, failure of which will lead to prosecution by the relevant authorities.[171] Any virtual world website that advertises goods or services online should comply with The Electronic Commerce (EC Directive) Regulations 2002.[172] "Online" in this case would include, via the internet, on interactive television, as well as by mobile telephones as the internet and mobile phones are now the primary means of access to virtual forums.[173]

According to The Electronic Commerce (EC Directive) Regulations 2002, a consumer must be a natural person who is acting for purposes other than those of his trade, business or profession and must be a recipient of the service.[174] In terms of the definition in the Electronic Directive (EC Directive) Regulations 2002, a consumer is a "recipient of the service".[175] The Electronic Commerce (EC Directive) Regulations 2002 states that, in any form, commercial communications is defined as communications that is designed to promote, directly or indirectly, the goods, services or image of any person pursuing a commercial, industrial or craft activity or exercising a regulated profession.[176]

The definition of commercial communications given by The Electronic Commerce (EC Directive) Regulations 2002 includes any online forms of communication, including websites

[169] M Turner … et al 'E-commerce directive - UK implementation. Electronic Commerce (EC Directive) Regulations 2002 - Worth the wait?' (2002) 18 (6) *Computer Law & Security Report* 396.
[170] Z Qin *Introduction to E-commerce* (2010) 24.
[171] A Sparrow *The Law of Virtual Worlds and Internet Social Networks* (2010) 41.
[172] ibid 42.
[173] ibid.
[174] See Regulaiton 2 (1) (*b*) of the Electronic Commerce (EC Directive) Regulations 2002, No. 2013.
[175] See Regulation 2 (1) of the Electronic Commerce (EC Directive) Regulations 2002, No. 2013.
[176] See Regulation 2 of the Electronic Commerce (EC Directive) Regulations 2002, No. 2013.

and emails.[177] Some other forms of commercial communication such as mobile text messages or electronic greeting cards are not considered to fall within the definition of "commercial communication"[178]

Although the Electronic Commerce (EC Directive) Regulations 2002 apply virtually to almost every electronic business, [179] there are other various transactions to which it does not apply, chief among them being the field of taxation.[180] The Electronic Commerce (EC Directive) Regulations 2002 also do not apply to questions relating to information society services covered by the Data Protection Directive 95/46/EC, the Telecoms Data Protection Directive 97/66/EC, and Directive 2002/58/EC.[181] The Electronic Commerce (EC Directive) Regulations 2002 do not apply to questions relating to agreements or practices governed by cartel law nor to betting, gaming or lotteries which involve wagering a stake with monetary value.[182]

Regulation 6 of the Electronic Commerce (EC Directive) Regulations 2002 requires that the information society service providers should, in a manner that is "easily, directly and permanently accessible" make certain information available to their recipients.[183] The information that the information society service provider is supposed to provide to the recipients includes, but not limited to:

> "(a) the name of the service provider;
>
> (b) the geographic address at which the service provider is established;

[177] See Note 167 above.
[178] ibid at 7.
[179] 'The UK's E-Commerce Regulations' available at https://www.out-law.com/page-431, accessed on 27 June 2017. See also Regulation 1 (1) and 1 (2) of the Electronic Commerce (EC Directive) Regulations 2002, No. 2013.
[180] See Regulation 3 (1) (*a*) of Electronic Commerce (EC Directive) Regulations 2002, No. 2013.
[181] ibid.
[182] See Regulation 3 (1) (*c*) and (*d*) of the Electronic Commerce (EC Directive) Regulations 2002, No. 2013.
[183] See Regulation 6 (1) of the Electronic Commerce (EC Directive) Regulations 2002, No. 2013.

(c) the details of the service provider, including his electronic mail address, which make it possible to contact him rapidly and communicate with him in a direct and effective manner;

(d) where the service provider is registered in a trade or similar register available to the public, details of the register in which the service provider is entered and his registration number, or equivalent means of identification in that register;

(e) where the provision of the service is subject to an authorisation scheme, the particulars of the relevant supervisory authority;

(f) where the service provider exercises a regulated profession;

(i) the details of any professional body or similar institution with which the service provider is registered;

(ii) his professional title and the member State where that title has been granted;

(iii) a reference to the professional rules applicable to the service provider in the member State of establishment and the means to access them; and

(g) where the service provider undertakes an activity that is subject to value added tax, the identification number referred to in Article 22(1) of the sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonisation of the laws of the member States relating to turnover taxes—Common system of value added tax: uniform basis of assessment (1).”[184]

[184] See Regulation 6 (1) (*a*) – (*g*) of the Electronic Commerce (EC Directive) Regulations 2002, No. 2013.

If the information society service provider makes mention of prices in his email to the information society services recipient, then those prices referred to shall be indicated clearly and unambiguously and, in particular, shall indicate whether they are inclusive of tax and delivery costs.[185] Again this provision does not describe how "clearly and unambiguously and, in particular" are to be met in practical terms.[186]

Regulation 7 provides that any form of communication designed to promote either directly or indirectly, the goods, services or image of any person pursuing a commercial, industrial or craft activity must:

> "(a) be clearly identifiable as a commercial communication;
>
> (b) clearly identify the person on whose behalf the commercial communication is made;
>
> (c) clearly identify as such any promotional offer (including any discount, premium or gift) and ensure that any conditions which must be met to qualify for it are easily accessible, and presented clearly and unambiguously; and
>
> (d) clearly identify as such any promotional competition or game and ensure that any conditions for participation are easily accessible and presented clearly and unambiguously."[187]

The provisions of regulation 7 of The Electronic Commerce (EC Directive) Regulations 2002 do not prescribe how the requirement to make commercial communications "clearly identifiable" should be met in practice. [188]

---

[185] See Regulation 6 (2) of the Electronic Commerce (EC Directive) Regulations 2002, No. 2013.
[186] Turner … et al 'E-commerce directive - UK implementation. Electronic Commerce (EC Directive) Regulations 2002 - Worth the wait?' (2002) 18 (6) *Computer Law & Security Report* 399.
[187] See Regulation 7 (*a*) – (*d*) of the Electronic Commerce (EC Directive) Regulations 2002, No. 2013.

The provisions of regulation 8 of The Electronic Commerce (EC Directive) Regulations 2002 state that all unsolicited commercial communications by email (for example an email advertising goods or services which is sent to a recipient who has not requested it), must be "clearly and unambiguously identifiable as such" when it gets to the recipient.[189] This provision has been stipulated for the sole purpose of ensuring that the recipients can delete the email or block the sender without the need to actually open and read message send.[190]

5.6. Privacy and Electronic Communications (EC Directive) Regulations 2003 (PEC Regulations)

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PEC Regulations) came into force on the 11th of December 2003.[191] The European Union passed a Directive on Privacy and Electronic Communications known as The Unsolicited Communications Order,[192] under the European Communities Act of 1973.[193] The Order's recital number 40 gives the aim of the directive which states that:

> "Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient."[194]

---

[188] Turner … et al see Note 186 above.
[189] See Regulation 8 of the Electronic Commerce (EC Directive) Regulations 2002, No. 2013.
[190] See Note 186 above at 399.
[191] Privacy and Electronic Communications (EC Directive) Regulations 2003, No. 2426.
[192] The Unsolicited Communications Order 2005.
[193] European Communities Act of 1973, Chapter 68.
[194] See Recital 40 of the European Communities Act 1973, Chapter 68. G J H Smith *Internet Law and Regulation* 4 ed (2007) 801.

In the UK, the Directive was implemented by the adoption of the Privacy and Electronic Communications (EC Directive) Regulations 2003.[195]

Regulation 6 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 prohibits the free use of an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements sets out in the same regulation are met.[196] Before this information can be stored or before access is gained in the terminal equipment of a subscriber, clear and comprehensive information about the purposes of the storage of, or access to, that information must be given to the subscriber and the subscriber must be given an opportunity to refuse the storage of or access to that information.[197]

Consent to the storage of and/or access to information can be given by means of any appropriate web browser settings or any other application that is linked to it.[198]

Organizations or companies that carry out their marketing businesses by mobile phones, emails, fax or text messages are bound by the provisions of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PEC Regulations) which provides some legal constrains.[199] The regulations of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PEC Regulations) apply to all the electronic communications services as defined by section 32 of the Communications Act which states that "electronic communications service" means:[200]

---

[195] Smith ibid.
[196] See Regulation 6 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 Number 2426.
[197] See Regulation 6 (2) (*a*) and (*b*) of the Privacy and Electronic Communications (EC Directive) Regulations 2003 Number 2426.
[198] J Riordan *The Liability of Internet Intermediaries* (2016) 322.
[199] R Morgan and R Boardman *Data Protection Strategy: Implementing Data Protection Compliance* 2 ed (2012) 143.
[200] ibid 144.

> "…a service consisting in, or having as its principal feature, the conveyance by means of an electronic communications network of signals, except in so far as it is a content service."[201]

Regulation 19 of the PEC Regulations prohibits, without the consent of the called party, any transmission of automated recorded calls for the purposes of direct marketing.[202] Regulation 20 prohibits the use of faxes as direct marketing faxes, in some instances when faxes are unsolicited and in other instances when such faxes are send to numbers that are not part of the official register for that purpose.[203] Regulation 21 also prohibits the making of calls for direct marketing telephone calls if the subscriber has notified the caller that such calls should not be made to their cell phone or to their mobile number.[204] Lastly, regulation 25 prohibits the sending of unsolicited messages or emails for the purposes of direct marketing unless if consent has been given by the recipient of such emails or messages.[205]

All the PEC regulations are enforced by the Information Commissioner under the Data Protection Act[206] of 1998.[207] Regulation 4 states that:

> "Nothing in these Regulations shall relieve a person of his obligations under the Data Protection Act 1998 in relation to the processing of personal data."[208]

---

[201] See Section 32 (2) of the Communications Act 2003, Chapter 21.
[202] See Regulation 19 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 Number 2426.
[203] See Regulation 20 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 Number 2426.
[204] See Regulation 21 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 Number 2426.
[205] See Regulation 25 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 Number 2426.
[206] Data Protection Act of 1998, Chapter 29.
[207] Great Britain: Parliament: House of Commons: Culture, Media and Sport Committee, 'House of Commons - Culture, Media and Sport Committee: Nuisance Calls: Volume I - HC 636: Fourth Report of Session 2013-14, Vol. 1: Report, Together with Formal Minutes, Oral and Written Evidence', Volume 1, 64-65.
[208] See Regulation 4 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 Number 2426.

This is because the definition of direct marketing used in regulations 19, 20, 21 and 25 of the Privacy and Electronic Communications (EC Directive) regulations 2003 (PEC Regulations) is the same definition that is used in the Data Protection Act 1998 as the PEC regulation states that the definition in the Data Protection Act shall apply to it as well.[209] The Data Protection Act defines direct marketing as:

> "…the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals".[210]

Although the two have a similar definition of direct marketing, PEC regulations have a broader application since they are applying to processing of "any personal data" which means they apply even if the organization does not know the name of the person it is contacting.[211]

5.7. Computer Misuse Act 1990

The substantive legislation governing e-commerce and computer usage in the UK is the Computer Misuse Act of 1990 hereafter referred to as the (CMA).[212] In *Regina v Gold & Schifreen*, the call for the introduction of the CMA came as a result of the court pointing out that existing computer laws did not accommodate as well as reflect the changes brought about by the computer technology.[213] This led to the eventual acquittal of the defendants who were being accused of hacking into bank's computer system.[214] They were initially charged and

[209] See Regulation 2 (2) of the Privacy and Electronic Communications (EC Directive) Regulations 2003 Number 2426.
[210] Section 11 (3) of the Data Protection Act 1998, Chapter 29.
[211] Commissioner's Office (UK) 'Direct Marketing' available at https://ico.org.uk/media/fororganizations/documents/1555/direct-marketing-guidance.pdf, accessed on 25 July 2017 on page 6-7.
[212] Computer Misuse Act 1990, Chapter 18.
[213] *Regina v Gold & Schifreen* [1988] 2 All ER 186 (HL).
[214] ibid.

convicted under section 1, and section 8 (1) (*d*) of the Forgery and Counterfeiting Act of 1981.[215]

In upholding the decision of the UK Appeal Court in which the defendants were acquitted, the House of Lords stated that;

> "A device could not be an instrument under 8 (1) (*d*) of the 1981 Act by which the information was recorded or stored by electronic means, unless it preserved the information for an appreciable time with the object of subsequent retrieval or recovery. Since the momentary holding of the customer identification numbers and passwords while they were verified did not amount to the recording and storage of information, the respondents had not made an instrument within section 8 (1) (*d*) and could not be guilty of an offence under section 1."[216]

On 1 October 2008, the CMA was amended to clarify the meaning of "unauthorized access" to a computer after certain loopholes were discovered.[217]

The CMA made the access of computer material without authorization (also known as hacking) a crime and by extension, invasion of privacy.[218] According to the CMA, computer misuse offences are (a) unauthorized access to computer material, (b) unauthorized access with intent to commit or facilitate commission of further offences, (c) unauthorized acts with

[215] Forgery and Counterfeiting Act 1981, Chapter 45. A Charlesworth 'Legislating against computer misuse: The trials and tribulations of the UK Computer Misuse Act 1990' (1993) 4 (1) *Journal of Law and Information Science* 81.
[216] See Note 213 above.
[217] F Cassim 'Formulating specialised legislation to address the growing spectre of Cybercrime: A comparative study' (2009) 12 (4) *Potchefstroom Electronic Law Journal* 47.
[218] ibid.

intent to impair, or with recklessness as to impairing, operation of a computer, etcetera and the unauthorized acts causing, or creating risk of and/or serious damage.[219]

The actual act (*actus reus)* of unlawfully gaining access to a computer system suffices for a finding of guilt as it is in itself an invasion of privacy as pointed out by the CMA.[220] Thus the offence of invasion of privacy in e-commerce is clearly stated by the CMA when it points out that, a person is guilty of an offence if the access he intends to secure is unauthorized.[221]

Although any unauthorized use of or access to a computer is defined as "computer misuse", Stefan Fafinski argues that not all computer misuse attracts the attention of criminal law since computer misuse is not a computer crime.[222] The CMA does not in itself define neither "computer" nor "misuse" and this judicial uncertainty has made the CMA to see relatively very little use in the UK.[223]

5.8. Other UK Acts of Parliament with Components of Privacy and Data Protection

In this discussion, acts of parliament will be cited, not to demonstrate the utility of specific individual statutes in the protection of privacy, but instructive as examples of details that may be included in general legislation for the protection of privacy in e-commerce. The guaranteed privacy protection provided for in the statutes below is necessarily limited to the subject matter dealt with by the relevant statute, and the specific circumstances provided for and specified in the relevant provisions.

---

[219] See Section 1 - 3 of the Computer Misuse Act 1990, Chapter 18.
[220] See Section 1 (1) and 2 of the Computer Misuse Act 1990, Chapter 18.
[221] See Section 1 (1) (*b*) of the Computer Misuse Act 1990, Chapter 18.
[222] S Fafinski 'Access denied: Computer misuse in an era of technological change' (2006) 70 (1) *The Journal of Criminal Law* 424.
[223] ibid.

5.8.1. Rehabilitation of Offenders Act 1974

The Rehabilitation of Offenders Act of 1974 protects privacy by making evidence about a spent conviction inadmissible.[224] According to the Rehabilitation of Offenders Act of 1974, a person who maliciously publishes details of the plaintiffs spent conviction can be sued for damages.[225]

5.8.2. Telecommunications Act 1984

Section 43 of the Telecommunications Act of 1984 (as amended by the Telecommunications Regulations of 1999) makes it an offence to use a public tele-communications system to send any material that is threatening, grossly offensive, and/or obscene.[226]

5.8.3. Police Act 1997

The Police Act of 1997 in section 97, contains provisions similar to those found in The Interception of Communications Act of 1985[227] regulating police interception of confidential material.[228] The Police Act of 1997 also requires authorisation from a Commissioner for the use of listening devices by the police.[229]

5.8.4. Broadcasting Act 1996

Section 166 of the Broadcasting Act of 1996 states that defamatory words, visual images, pictures, gestures and other forms of broadcast on radio or television or any other programme service are actionable as libel.[230]

---

[224] See Section 4 (1) of the Rehabilitation of Offenders Act 1974, Chapter 53.
[225] See Section 8 of the Rehabilitation of Offenders Act 1974, Chapter 53.
[226] See Section 43 of the Telecommunications Act 1984, Chapter 12.
[227] The Interception of Communications Act of 1985, Chapter 56.
[228] See Section 97 of the Police Act 1997, Chapter 50.
[229] ibid.
[230] See Section 166 of the Broadcasting Act 1996, Chapter 55.

5.8.5. Copyright, Designs and Patents Act 1988

The Copyright, Designs and Patents Act of 1988, also gives limited protection for privacy where a person's proprietary interest in literary[231] or artistic work[232] has been infringed.[233] The Copyright, Designs and Patents Act of 1988, gives a cause of action for false attribution of authorship.[234]

5.8.6. Theatres Act 1968

The Theatres Act of 1968 has similar provisions as those found in the Broadcasting Act of 1996 in section 4 (1) which states that it is an actionable libel to publish defamatory words in the course of a performance of a play.[235]

5.8.7. Adoption Act 1976

Section 64 of the Adoption Act of 1976 provides that proceedings under that same act should be held in private.[236]

5.8.8. Official Secrets Act 1989

The Official Secrets Act of 1989 provides penalties for spying which is "prejudicial to the safety or interests of the State".[237]

5.8.9. Access to Health Records 1990

The Access to Health Records of 1990 states that it is an offence to obtain or communicate information where such information is calculated or intended to be "directly or indirectly useful to an enemy."[238]

[231] See Section 3 (1) of the Copyright, Designs and Patents Act 1988, Chapter 48.
[232] See Section 4 (1) of the Copyright, Designs and Patents Act 1988, Chapter 48.
[233] See Sections 3 and 4 of the Copyright, Designs and Patents Act 1988, Chapter 48.
[234] See Sections 83 and 84 of the Copyright, Designs and Patents Act 1988, Chapter 48.
[235] See Section 4 (1) of the Theatres Act 1968, Chapter 54.
[236] See Section 64 of the Adoption Act 1976, Chapter 36.
[237] See Section 1 of the Access to Health Records 1990, Chapter 23.

Access to Health Records Act 1990 also had some privacy components in it when it was enacted. The 1998 DPA replaced the Access to Health Records Act[239], which gave access to manual records kept after 1 November 1991. The Access to Health Records Act was repealed except in respect of records of deceased patients.[240] According to the Access to Health Records Act, a health record includes all nursing records, physiotherapy records, pathology laboratory records and any other record relating to the patient's health.[241] The Access to Health Records of 1990[242] like the Access to Medical Reports Act of 1988[243] also gives guidelines for disclosure of health records by making provision for patients and other persons authorised by law to gain access to their health records.[244]

5.8.10. Access to Medical Reports Act of 1988

The Access to Medical Reports Act of 1988 provides guidelines for the disclosure of medical records.[245] The Access to Medical Reports Act has limited provisions for the general protection of data, but exemptions to giving access to medical records are provided for section 7 of the Access to Medical Reports Act, thus maintaining privacy by protecting data.[246] Where the disclosure of a medical report or part thereof is likely to reveal information about another person, or to reveal the identity of another person who has supplied information to the medical practitioner about the individual, access is denied.[247]

By defining "medical report", as a report relating to the physical or mental health of the individual prepared by a medical practitioner who is or has been responsible for the clinical

---

[238] See Section 1 (*c*) of the Access to Health Records 1990, Chapter 23.
[239] Access to Health Records Act 1990, Chapter 23.
[240] B Dimond 'Rights to information access under the Data Protection Act' (2005) 14 (14) *British Journal of Nursing* 774.
[241] ibid 774.
[242] See Note 239 above.
[243] See Section 1 of the Access to Medical Reports Act 1988, Chapter 28.
[244] See Section 3 of the Access to Health Records 1990, Chapter 23.
[245] See Section 4 of the Access to Medical Reports Act 1988 Chapter 28.
[246] See Section 7 (1) to 7 (4) of the Access to Medical Reports Act 1988, Chapter 28.
[247] See Section 7 (2) of the Access to Medical Reports Act 1988, Chapter 28.

care of the individual, the Access to Medical Reports Act of 1988 protects not just the computerized records but manual records as well.[248]

5.8.11. Children and Young Persons Act 1933

Similarly, section 49 of the Children and Young Persons Act of 1933 restricts the reporting of the proceedings of juvenile courts.[249] Section 39 of the same act also provides for the obtaining of a court order prohibiting newspaper reports from publishing personal details such as the name, address, school or any detail "calculated to lead to the identification of any child or young person" concerned in proceedings.[250]

5.8.12. Sexual Offences (Amendment) Act 1976

Section 4 of the Sexual Offences (Amendment) Act of 1976 provides for anonymity to victims of rape and any other case of sexual offences.[251]

5.8.13. Criminal Justice Act 1988

In Section 158, the Criminal Justice Act of 1988 protects the anonymity of victims in cases involving conspiracy to rape and burglary with intent to rape.[252]

5.8.14. Magistrates' Courts Act 1980

Section 69 of the Magistrates' Courts Act of 1980 provides that the public is excluded from family proceedings in the magistrates' courts.[253]

[248] See Section 1 (1) of the Access to Medical Reports Act 1988, Chapter 28.
[249] See Section 49 of the Children and Young Persons Act 1933, Chapter 12.
[250] See Section 39 of the Children and Young Persons Act 1933, Chapter 12.
[251] See Section 4 of the Sexual Offences Amendment Act 1976, Chapter 82.
[252] See Section 158 of the Criminal Justice Act 1988, Chapter 33.
[253] Section 69 of the Magistrates' Courts Act of 1980, Chapter 43.

5.8.15. Protection from Harassment Act 1997

The Protection from Harassment Act of 1997 does not define harassment; however Wessels J in a South African case of *Epstein v Epstein* defines harassment as "a most vexatious nuisance" that amounts to an invasion of privacy.[254] Section 1 of the Protection from Harassment Act states that, a person must not pursue a course of conduct that amounts to harassment of another and which he or she knows or ought to know amounts to harassment of another.[255] Section 7 of the same provides that harassing a person includes alarming a person or causing the person distress which may include the invasion of their privacy.[256]

5.8.16. Interception of Communications Act 1985

The Interception of Communications Act of 1985 sets some limitations on surveillance of any tele-communications.[257] The Interception of Communications Act in section 1 makes it an offence to intercept communications sent through the post and telecommunication system, without authorisation by the Secretary of State, thus promoting privacy.[258] The Interception of Communications Act in section 2 also specifies conditions under which a warrant may be issued.[259]

5.8.17. Consumer Credit Act 1974

Consumer Credit Act of 1974, among many other functions, governs consumer credit information by providing protection in respect of information collected by credit reference agencies. Sections 158 to section 160 of the Consumer Credit Act[260] was amended by section

[254] *Epstein v Epstein* 1987 (4) SA 606 (C) at 87.
[255] See Section 1 (1) of the Protection from Harassment Act 1997, Chapter 40.
[256] See Section 7 (2) of the Protection from Harassment Act 1997, Chapter 40.
[257] See Section 1 of the Interception of Communications Act 1985 Chapter 56.
[258] *Christie v United Kingdom* (1994) 7S-A DR 119.
[259] See Section 2 (2) of the Interception of Communications Act 1985, Chapter 56.
[260] Consumer Credit Act 1974, Chapter 39.

62 of the 1998 DPA.[261] Section 158 gives an agency the duty to disclose filed information.[262] Section 62[263] also amended section 159 which deals with the Consumer Credit Act which deals with the correction of wrong information[264]. The effect of section 62 amendments is to widen the scope of section 158, 159 and 160.

5.9. What lessons can South Africa learn from United Kingdom and its laws in protecting e-traders or buyers

The UK e-commerce legislation is applied as a collaborative initiative involving the police, members of the private sector and academics jointly working together to stamp out cyber-crime. In all the different sectors that deal with personal information of individuals when transacting commercially, there are laws that deal with privacy protection. South Africa can learn from this ingenious and commendable step in the sense that various stakeholders in the economy are brought together from various walks of life to contribute a significant measure of information, based on their knowledge and experiences to make practical propositions on how to address the growing menace of cyber-crime and breach of personal information privacy.

South Africa like the UK can also adopt sector-specific e-commerce policies and legislation in order to encourage and/or restrict the use of encryption in commercial data transmissions. In order to encourage greater public confidence in e-commerce, the South African government should officially endorse certain cryptographic methods, or institutions like in the UK.

In domestic businesses' electronic transactions, the South African government law enforcement agencies can participate in international deliberations and agreements toward

[261] See Section 62 of the Data Protection Act 1998, Chapter 29.
[262] See Section 158 of the Consumer Credit Act 1974, Chapter 39.
[263] See Section 62 (2) of the Data Protection Act 1998, Chapter 29.
[264] See Section 159 of the Consumer Credit Act 1974, Chapter 39.

common standards for cross-border data security and access as the UK adopted most if not all of the EU directives on electronic commerce as its domestic e-commerce legislation. This will help South Africa on matters of standardisation and international harmonisation. As noted in the previous chapters, South Africa is not bound by some international treaties controlling e-commerce because it is not a member to those treaties.

Finally, as noted in the discussion above, the UK presents an equally interesting case study as it amended its existing law (the CMA) a number of times to bring it in line with current trends. This is reflective of the legislature‘s attempt at keeping pace with the technology, in view of the dynamic nature of technology, which has the ability to render legislation in this field outdated. If South Africa adopts this approach, it will bring its e-commerce laws up to date with the latest technology being used in electronic commerce transactions.

5.10. Conclusion

Countries with sector-specific e-commerce legislation like the UK and those countries without such sector specific e-commerce legislation like South Africa, face somewhat similar problems. These problems could be seen through different UK and South African case law, although it is at very different scales. The main problem that seems to cause glitches in the UK is on implementation of e-commerce legilslation and is worse in South Africa.

CHAPTER SIX

6. PRIVACY, DATA PROTECTION AND E-COMMERCE IN THE UNITED STATES OF AMERICA

6.1. Introduction

There is a direct relationship between efficiency of e-commerce and the privacy protection laws as privacy has always been largely a matter of commerce rather than a matter of law.[1] With efficiency and privacy being amorphous terms in e-commerce, consumers expect some level of protection of their privacy to be provided when they engage in some electronic transactions and if this level of privacy is not provided for by the government, the same will weaken the e-commerce industry of that nation.[2]

The relationship between e-commerce efficiency and privacy is summarised by Stephen R Bergerson as follows:

> "While privacy concerns predate the personal computer, the advent of e-commerce has heightened consumers' concerns and intensified their distrust of information gatherers."[3]

In the United States America (hereafter USA), discussions on e-commerce and privacy protection moved from national privacy to international transactions with so much focus being on four aspects:

a) collection of personal identifiable information;

b) use of personal identifiable information;

---

[1] K H Sohn 'Privacy and security protection under korean e-commerce law and proposals for its improvements' (2016) 33 (1) *Arizona Journal of International & Comparative Law* 241.

[2] J Spratt 'An economic argument for electronic privacy' (2011) 6 (3) *I/S*: *A Journal of Law and Policy for the Information Society* 516.

[3] S R Bergerson 'E-commerce privacy and the black hole of cyberspace' (2001) 27 (3) *William Mitchell Law Review* 1528.

c) dissemination of personal identifiable information; and

d) redress after violations are discovered.[4]

One of the major privacy concerns that emerge with the rise of e-commerce is interruption and/or intrusion.[5]

Even though the rules used when doing online business in the USA are the same as those used to conduct a regular storefront business, there are extra rules that apply only to online businesses.[6] For privacy and security purposes, special attention in online businesses must be given to the collection of information, the storage of such information, and the use of personal identifiable information that has been collected online.[7]

In the USA, computer-communication systems and data processing services that are internationally operated such as Tymnet and Telenet are examples of transnational communications networks which are remotely computerized.[8] When it comes to the record keeping systems of automated personal identifiable data, the right to privacy refers to the rights that individuals have in relation to the collection, storage, usage (processing) and dissemination of such personal identifiable information.[9]

Just like South Africa and many other countries in the world, the USA does not have a single overarching electronic privacy law, but it uses the scattered system of threat-and-industry-

[4] See Note 2 above at 518.
[5] S D Balz & O Hance 'Privacy and the internet: Intrusion, surveillance and personal data' (1996) 10 (2) *International Review of Law Computers & Technology* 220.
[6] L Plave 'Franchising: Data protection and e-commerce issues in the United States' (2006) 4 (2) *International Journal of Franchising Law* 3.
[7] ibid.
[8] R Turn 'Privacy protection and security in transnational data processing systems' (1980) 16 (1) *Stanford Journal of International Law* 67.
[9] ibid 69.

specific protections aimed at curbing particularized threats to privacy.[10] A lot of companies in the USA do not acknowledge personal data privacy as a fundamental human right.[11]

6.2. Common Law Privacy Protection in the United States of America

From the time when there were no individual privacy rights, to the current time when judges are now giving definition to privacy rights, the courts have found and/or used very little common law.[12] Even though there was little use of common law to protect individual privacy in the USA, common law rights to privacy originated in the theory of property law in cases where it protected data.[13] After Warren and Brandeis wrote their journal article on common privacy in 1890,[14] Dean Prosser many years later categorized the common law right to privacy into four torts in his journal article.[15]

In common law, the right to privacy was accepted as falling into one or more of the following categories (otherwise known as Torts of Law) which did not include informational privacy:

a) "wrongful appropriation and use of a person's name, likeness or personality;

b) physical intrusion into a person's solitude or seclusion;

c) public disclosure of private facts that a reasonable person would find objectionable; and

d) publicity that places a person in a false light in the public eye."[16]

[10] See Note 2 above at 515 and 525.
[11] ibid 525.
[12] M W Iannotta 'Protecting individual privacy in the shadow of a national data base: The need for data protection legislation' (1989) 17 (1) *Capital University Law Review* 123.
[13] ibid.
[14] S D Warren & L D Brandeis 'The right to privacy' (1890) 4 (5) *Harvard Law Review* 193.
[15] D Prosser 'Privacy' (1960) 48 (1) *California Law Review* 383 and 389.
[16] Iannotta see Note 12 above. Prosser ibid. Bergerson 'E-commerce privacy and the black hole of cyberspace' (2001) 27 (3) *William Mitchell Law Review* 1535.

The leading case in the application of these privacy law torts is *Shibley v Time, Inc.* in which the Court of appeal in Ohio pointed out that the sale of a mailing list does not give rise to a privacy cause of action.[17] There are some courts that have since adopted the decision of the aforesaid case while several others are of the view that the decision in *Shibley v Time, Inc.* should be revisited due to the circumstances which have also changed.[18]

6.2.1. Appropriations

The *Second Restatement of Torts* provides that "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy".[19]

In *Hirsch v S.C. Johnson & Sons Inc.*, it was pointed out that using another person's nickname amounts to appropriation of their name.[20] The use of a nickname 'Crazylegs' on a women's shaving gel by the defendant violated publicity rights of a famous football player well known by that nickname and ultimately resulting in the invasion of privacy by appropriation.[21] In *John W. Carson v Here's Johnny Portable Toilets Inc.*, it was pointed out that using another person's slogan without their permission amounts to appropriation.[22] A Michigan company in this case violated the plaintiff's publicity rights by using (without consent) the phrase 'Here's Johnny' which was a slogan belonging to a certain entertainer.[23] In *Motschenbacher v R J Reynolds Tobacco Co.*, it was also pointed out that using another person's costume without their permission amounts to appropriation.[24]

---

[17] *Shibley v Time, Inc.* 341 N.E.2d 337 (Ohio Ct. App. 1975) at 337 and 339.
[18] Bergerson 'E-commerce privacy and the black hole of cyberspace' (2001) 27 (3) *William Mitchell Law Review* 1535.
[19] See the *Second Restatement of Torts* (1977) Section 652C.
[20] *Hirsch v S.C. Johnson & Sons Inc.* 90 Wis. 2d 379, 280 NW2d (1979) at 389.
[21] ibid.
[22] *John W. Carson v Here's Johnny Portable Toilets Inc.* 698 F2d 831 (6th Cir. 1983) at 835-836.
[23] ibid.
[24] *Motschenbacher v R J Reynolds Tobacco Co.* 498 F2d 821 (9th Cir. 1974) at 824 and 826-827.

6.2.2. Intrusions

In explaining the common torts above, the American Law Institute defined intrusion upon seclusion by stating that:

> "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[25]

This definition of intrusion includes, but is not limited to eavesdropping, any illegal search and the invasion of one's physical solitude.[26]

The case of *Miller v Motorola, Inc.* rejected the idea that, if someone willingly gives access to private personal information, it is considered as if consent has been given to the intrusion.[27] Consent should not be inferred by reason of employees having provided their personal private information willingly in compliance with the employment requirements.[28]

In-order for someone to invoke the intrusion tort, the act for which the tort is to be invoked should be of such a nature that it is very offensive to a reasonable person.[29] In *Cape Pubs. Inc. v Bridges*, the publishing of someone's naked picture in the newspaper did not invoke the intrusion tort since the court pointed out that the photo published did not reveal more flesh that did any woman on the beach.[30]

6.2.3. Disclosure of Private Facts

In the *Second Restatement of Torts*, it is also stated that:

---

[25] See Comment (a) of the American Law Institute *Second Restatement of Torts* (1977) Section 652B.
[26] ibid.
[27] *Miller v Motorola, Inc.* 202 Ill. App.3d 976 (Ill. App. Ct. 1990) at 978-979.
[28] ibid.
[29] See the *Second Restatement of Torts* (1977) Section 652B.
[30] *Cape Pubs. Inc. v Bridges* 423 So 2d 426 (1982 Fla App).

> "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for the invasion of his privacy if the matter publicised is of a kind that: would be highly offensive to a reasonable person, and is not of legitimate concern to the public."[31]

In *Melvin v Reid*, the court defended the plaintiff's right to privacy after a film revealed her past life as a prostitute, the profession she had renounced and had reformed from.[32] The court considered exposing the past life of the plaintiff to be falling under the tort prohibiting the public disclosure of private facts.[33]

However, critiques are raised against this tort on the basis that it infringes against the USA Constitutional freedom of speech as guaranteed by the First and the Fourteenth Amendments to the USA Constitution.[34] In *Florida Star v B. J. F.*, the court went against the decision in *MeIvin v Reid* by citing that matter was of public significance.[35] In this case of *Florida Star v B.J.F.*, the rape victim who had challenged the newspaper company for clearly citing her name in newspaper lost the case.[36]

6.2.4. False Light

The Second Restatement of Torts also provides that:

> "One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if: the false light in which the other was placed

[31] See Section 652 B of the *Second Restatement of Torts* (1977).
[32] *Melvin v Reid* 112 Cal. App 285, 286; 297 P. 91 (1931) at 292.
[33] ibid.
[34] F O Laosebikan 'Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in internet Cafes and Suggestions for Appropriate Legislation in Nigeria' (unpublished LLD dissertation, University of KwaZulu-Natal, 2007) 206.
[35] *Florida Star v B. J. F.* 491 U.S. 524 (1989) at 536-7.
[36] ibid 537.

> would be highly offensive to a reasonable person, and the actor had knowledge or acted in reckless disregard as to the falsity of the publicised matter and the false light in which the other would be placed"[37]

Publicity that places a person in a false light in the public eye is publicity that is objectionable to an ordinary reasonable man and has major inaccuracies.[38] Critics have however observed that this requirement does not protect the right to privacy because there may never be major inaccuracies since the victim's information when published is often true.[39]

6.3. Common Law Data Protection in the United States of America

In the USA, there was very little to no common law to protect data from being exploited and used for things other than what it was intended for.[40] The only time when common law data protection was applied by the courts, was when privacy law also protected data, like in *Melvin v Reid* wherein data infringement resulted in the publication of private facts.[41] Data protection was also coupled with privacy protection in a common law appropriation case of *Goodyear Tire Rubber Co. v Vandergriff*,[42] where the defendant impersonated the plaintiff to obtain information about him, or in the intrusion case of *Dietemann v Time, Incorporated* [43] where the defendant unlawfully gained access to the plaintiff's land in order to obtain information and to use it without the plaintiff's consent.[44]

---

[37] See Note 31 above.
[38] Laosebikan 'Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in Internet Cafes and Suggestions for Appropriate Legislation in Nigeria' (unpublished LLD dissertation, University of KwaZulu-Natal, 2007) 207.
[39] ibid.
[40] ibid 211.
[41] *Melvin v Reid* 112 Cal. App. 285, 297 P. 91 (1931) at 285-287ff.
[42] *Goodyear Tire & Rubber Co. v Vandergriff* 52 Ga. App. 662, 184 S.E. 452 (1936).
[43] *Dietemann v Time, Incorporated* 284 F. Supp. 925 (C.D. Cal. 1968).
[44] 284 F. Supp. 925 (C.D. Cal. 1968) at 927. Cf See also the South African case where the plaintiff's correspondence is read unlawfully (*S v Hammer* 1994 (2) SACR 496 (C) at 498.)

6.4. State Laws on Privacy and Data Protection in the United States of America: The Right to Privacy

The right to privacy is now formally protected in the USA following the Supreme Court's decision in the important milestone constitutional case of *National Association for the Advancement of Colored People v Alabama ex. Rel. Patterson*.[45] Even though the Supreme Court's decision allowed private groups to keep membership information confidential from the state, when dealing with matters of associational privacy, the decision also became a precedent for cases dealing with decisional as well as informational privacy.[46]

It is common knowledge in the USA that the state can legitimately demand to know the agents of any organization, its mandate, its activities as well as its officers.[47] In the landmark case of *NAACP v Alabama*, the court decided that the state should never ask for information about the members of the organization because this amounts to the invasion of privacy.[48] Again, from the decision of *NAACP v Alabama*, confidentiality and anonymity are promised to members as their data is constitutionally protected from mandatory disclosure whether that information is handwritten on lined paper or it is just stored electronically in a computer system.[49]

In the progressive cases of *Griswold v Connecticut*[50] and *Roe v Wade*,[51] decisional privacy as well as informational privacy were extended by the Supreme Court's decision which allowed private groups to keep membership information confidential from the state.[52]

---

[45] *National Association for the Advancement of Colored People v Alabama ex. Rel. Patterson* 357 U.S. 449 (1958) at 462.
[46] A L Allen 'Associational privacy and the First Amendment: NAACP v Alabama, privacy and data protection' (2011) 1 (1) *Alabama Civil Rights & Civil Liberties Law Review* 1.
[47] See Note 45 above at 464-465.
[48] ibid 465.
[49] ibid.
[50] *Griswold v Connecticut* 381 U.S. 479 (1965). Balz & Hance 'Privacy and the internet: Intrusion, surveillance and personal data' (1996) 10 (2) *International Review of Law Computers & Technology* 222.
[51] *Roe v Wade* 410 U.S. 113 (1973). Balz & Hance ibid.

The State of California took the leading role in privacy protection by passing the California Assembly Bill 1950 also known as the California "A.B. 1950" which requires businesses to implement and to maintain reasonable security procedures and practices for the purposes of protecting certain unencrypted personal identifiable information from unauthorized access, destruction, use, modification, or disclosure.[53] This privacy law also means that third parties who are unaffiliated are contractually required to maintain reasonable security procedures and practices if they receive such unencrypted personal identifiable information.[54]

'Personal identifiable information' means an individual's first name or first name initial and his or her last name in combination with any one or more elements like the social security number, driver's license number or California identification card number, his or her account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account and medical information.[55] Personal identifiable information according to the California Assembly Bill 1950 does not include any information that is publicly available and has been lawfully made available to the general public through the Federal, State, or local government's records.[56]

Another data protection mechanism introduced by many other States after the State of California was the exemption from the notification laws if the company's data was by any means encrypted.[57] Although encryption of data was not a requirement, the exemption from

[52] See Note 46 above. Griswold v Connecticut 381 U.S. 479 (1965) at 483. Roe v Wade 410 U.S. 113 (1973) at 154-155.
[53] See Section 1 of the California Assembly Bill 1950. Plave 'Franchising: Data protection and e-commerce issues in the United States' (2006) 4 (2) *International Journal of Franchising Law* 11.
[54] See Section 1 of the California Assembly Bill 1950.
[55] See Section 1 (*d*) (1) (A)-(D) of the California Assembly Bill 1950.
[56] See Section 1 (*d*) (3) of the California Assembly Bill 1950.
[57] A C Border 'Untangling the web' (2012) 35 (2) *Suffolk Transnational Law Review* 369.

notification laws is meant to influence corporations to encrypt their data, and thus protect personal identifiable information.[58]

In 1972, the State of California amended its Constitution[59] in order to give its residents the right to privacy and it also became the first State in the entire USA to make security breach notification law in order to deal with security data breaches in online businesses.[60] These security breach notification laws apply to any person owning an online business or anyone owning or licencing computerized data in their business, if that data contains personal identifiable information.[61]

Even though this law only applies to California, the security breach notification law also applies to any breach of personal information regarding California residents despite the fact that the personal information is maintained by an online business that is outside of California.[62] The California privacy law requires that, if there is a breach of security that leads to the exploitation of personal information by an unauthorized person, the breach must be reported by the discovering institution as soon as it gets a notification of breach.[63]

The 'Shine the Light' Law, Civil Code 1798.83 is privacy law in California otherwise also known as the 'S.B. 27' the name given during its designation when it was passed by the California State Legislature in 2003.[64] After its consideration by the legislature, it became

[58] ibid 370.
[59] See Article 1 Section 1 of the California Constitution, November 1972 stating, "All people are by nature free and independent, and have certain inalienable rights, among which are those of enjoying and defending life and liberty; acquiring, possessing, and protecting property; and pursuing and obtaining safety, happiness, and privacy."
[60] Border 'Untangling the web' (2012) 35 (2) *Suffolk Transnational Law Review* 369. D H Flaherty 'On the utility of constitutional rights to privacy and data protection' (1991) 41 (1) *Case Western Reserve Law Review* 837.
[61] D Medine & N D Steimer 'Recent developments in data security and data privacy' (2006) 1 (1) *Journal of Payment System Laws* 264.
[62] ibid.
[63] ibid.
[64] CA Civil Code Section 1798.83 of 2005.

active in 2005.[65] Although this code does not specifically deal with online privacy, it certainly has an impact on the online privacy services.[66]

The Civil Code 1798.83 privacy law gives all the privacy advocates and the press members the right to obtain detailed information about a business' and non-profit organization's data disclosure practices for the purposes of giving it to a third party for commercial marketing purposes unless if, and only if, the business or non-profit organization provides a broad opt-out of disclosures to its affiliates.[67] The California Civil Code 1798.83 serves e-businesses by providing an incentive to opt-out of third party disclosures for marketing purposes, which is an incentive that is missing from the Federal government's online privacy laws.[68]

At the beginning of 2006, about twenty-two other States in the USA also joined California in making it mandatory for e-business to give some form of notice in the case of a suspected data security breach or in the case of an inadvertent disclosure, fortuitous disclosure or otherwise.[69] On 1January 2010, the State of Nevada went a step further in privacy protection by making encryption of personal information a requirement, when personal identifiable information is being transmitted within an insecure system.[70]

On 1 March 2010, the State of Massachusetts surpassed every other State or Federal law when it introduced a new broad and strict regulatory scheme for the purposes of data privacy

---

[65] ibid.
[66] Plave 'Franchising: Data protection and e-commerce issues in the United States' (2006) 4 (2) *International Journal of Franchising Law* 11.
[67] ibid.
[68] ibid.
[69] Arkansas, Ark. Code Ann. Section 4-110-101; Connecticut, Conn. Gen. Stat. Section 36a-701; Delaware, Del. Code Ann. tit. 6, Section 12B1-01; Florida, Fla. Stat. Section 817.5681; Georgia, Ga Code. Ann. Section 10-1-910; Illinois, 815 ill. comp. stat. Section 530/1; Indiana (applies only to state agencies), Ind. Code Section 4-1-10-1; Louisiana, La Rev. Stat. Ann Section 51:3071; Maine, Me. Rev. Stat. Ann. tit. 10, Section 1346; Minnesota, Minn. Stat. Section 325E.61; Montana, Mont. Code Ann. Section 30-14-1701 et seq.; Section 33-19-321; Nevada, Nev. Rev. Stat. Section 603A.010; New Jersey, N.J. Rev. Stat. Section 56:8-161; New York, N.Y. Gen. Bus. Law Section 899-aa; North Carolina, N.C. Gen Stat., Section 75-65(a); North Dakota, N.D. Cent. Code Section 51-30-02; Ohio, Ohio Rev. Code Section 1349.19(B) (1); Pennsylvania, Pa. Cons. Stat. Section 3(a); Rhode Island, R.I. Gen. Laws Section 11-49.2-7(a); Tennessee, Tenn. Code. Ann. Section 47-18-2107; Texas, Tex. Bus. & Com. Code Section 48.103(b); Washington, Wash. Rev. Code Section 19.255.010. See alos Plave Note 66 above at 11 and 22.
[70] Border 'Untangling the web' (2012) 35 (2) *Suffolk Transnational Law* Review 371.

by regulating anyone who possessed another's personal identifiable information regardless of their industry.[71] Even though the privacy law passed by the State of Massachusetts is limited in its scope and effect, it has had a nationwide impact on companies doing business within Massachusetts and on companies that have customers within Massachusetts.[72]

Besides the Californian Constitution having some provisions protecting the right to privacy in the State of California, there are many other states with similar provisions in their State Constitutions.[73]

The Alaska Constitution has a provision that encourages all kinds of privacy rights including informational privacy rights and it states that:

> "…the right of the people to privacy is recognized and shall not be infringed".[74]

The New York Constitution also has a provision protecting the right to privacy, which is in every respect similar to the Fourth Amendment to the USA Constitution.[75] The New York Constitution inter alia states that:

> "…the right of the people to be secure in their persons, houses, papers and effects, and against unreasonable searches and seizures, shall not be violated".[76]

---

[71] ibid.
[72] ibid 372.
[73] Laosebikan 'Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in internet Cafes and Suggestions for Appropriate Legislation in Nigeria' (unpublished LLD dissertation, University of KwaZulu-Natal, 2007) 199-200.
[74] See Article I (Declaration of Rights), Section 22 of the Alaska Constitution (1972).
[75] See Article I (Bill of Rights), Section 12 of the New York Constitution (1938).
[76] ibid.

6.5. United States of America Data and Privacy Protection Through the Federal Constitution

Although the USA Constitution does not explicitly provide for the right to privacy in its articles or in its amendments, the Supreme Court of the USA has in a number of cases, implied the right of privacy in the word 'liberty' as found in the Fifth and the Fourteenth Amendment to the USA Constitution.[77]

Jurisprudence has found a certain 'zone of privacy' in the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments to the USA Constitution which limit the Federal and State government from certain activities, in order to protect privacy.[78] It was in *Griswold v Connecticut* that privacy protection was extracted from the First, Third, Fourth, Fifth and Ninth Amendments to the USA Constitution.[79]

In a privacy and abortion case of *Roe v Wade*, the Supreme Court took a huge step in the development of the constitutional right to privacy.[80] As stated in the paragraphs above, prior to this interpretation, the Supreme Court did not interpret the right of privacy to include informational privacy.[81] The right to privacy was always limited to decisional privacy.[82] Decisional privacy applied only to cases of marriage,[83] procreation,[84] abortion,[85] contraception,[86] family relationships,[87] and to child rearing matters.[88] It was in *Whalen v Roe*

[77] J Spratt 'An economic argument for electronic privacy' (2011) 6 (3) *I/S: A Journal of Law and Policy for the Information Society* 525. D Banisar & S Davies 'Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments' (1999) 18 (1) *Journal of Computer and Information Law* 108.
[78] Balz & Hance 'Privacy and the internet: Intrusion, surveillance and personal data' (1996) 10 (2) *International Review of Law Computers & Technology* 220. *Griswold v Connecticut* 381 U.S. 479 (1965) at 480-486.
[79] *Griswold v Connecticut* 381 U.S. 479 (1965) at 480-486.
[80] *Roe v Wade* 410 U.S. 113 (1973) at 117 and 153.
[81] Flaherty 'On the Utility of Constitutional Rights to Privacy and Data Protection' (1991) 41 (1) *Case Western Reserve Law Review* 838.
[82] Banisar & Davies see Note 77 above.
[83] *Zablocki v Redhail* 434 U.S. 374 (1978).
[84] *Skinner v Oklahoma* 316 U.S. 535 (1942).
[85] *Roe v Wade* 410 U.S. 113 (1973) and *Doe v Bolton* 410 U.S. 179 (1973).
[86] *Eisenstadt v Baird* 405 U.S. 438 (1972).
[87] *Moore v City of East Cleveland* 431 U.S. 494 (1971).

that the court dealt with the issue of informational privacy.[89] The Supreme Court in the case *insupra* rendered the decision which expands the right to privacy to include informational privacy, clearly illustrating the government's reluctance when interpreting the Bill of Rights.[90]

The case of *United States Department of Justice v Reporters Committee for Freedom of the Press*[91] is another landmark case which dealt with informational privacy.[92] The case arose when a CBS news reporter and a media rights advocacy group requested criminal identification records from the Federal Bureau of Investigation by filing a request under the Freedom of Information Act.[93] The main issue was whether the disclosure of criminal identification records to a third party would amount to the invasion of personal privacy.[94] The court pointed out that right of privacy that is 'strong' exists essentially and permanently in the non-disclosure of computerized information.[95]

In *Katz v United States*, the Supreme Court decided that although the Fourth Amendment protected the USA citizens against unreasonable search and seizure, it should be interpreted to protect people rather than places and to protect the privacy rather than property.[96] Following the decision of *Katz v United States*, the Canadian case of *Hunter v Southam*[97] and

---

[88] *Pierce v Society of Sisters* 268 U.S. 510 (1925).
[89] *Whalen v Roe* 429 U.S. 589 (1977). M W Iannotta 'Protecting individual privacy in the shadow of a national data base: The need for data protection legislation' (1989) 17 (1) *Capital University Law Review* 125.
[90] *Whalen v Roe* 429 U.S. 589 (1977) at 592-595 and at 600-605.
[91] *United States Department of Justice v Reporters Committee for Freedom of the Press* 489 U.S. 749 (1989) at 754.
[92] Flaherty 'On the utility of constitutional rights to privacy and data protection' (1991) 41 (1) *Case Western Reserve Law Review* 839.
[93] See Note 91 above at 757.
[94] ibid.
[95] ibid at 766.
[96] *Katz v United States* 389 U.S. 347 (1967) at 351.
[97] *Hunter v Southam* [1984] 2 SCR 145 at 157 and 159.

the case of *R v Dyment*,[98] also interpreted the right against unreasonable search and seizure to constitute the right to privacy.[99]

In *R v Duarte*, the court reiterated that the right against unreasonable search and seizure should be interpreted to constitute the privacy right if there is a reasonable expectation of privacy.[100] With the Supreme Court not being able to give an exhaustive list on the protection of informational privacy, it cited a list of other cases in which the word 'liberty' was interpreted to include other specific rights.[101] In *Lochner v New York* however, the court was very reluctant to interpret new substantive rights by reading into the word 'liberty'.[102]

6.5.1. First Amendment

As mentioned in paragraphs above, in *NAACP v Alabama*, the court decided that the State should never ask for information about the members of the organization because this amounts to the invasion of privacy.[103] Again, from the decision of *NAACP v Alabama*, confidentiality and anonymity are promised to members as their data is constitutionally protected from mandatory disclosure, whether that information is handwritten and on paper or it is just stored electronically in a computer system.[104]

Thus the Alabama State Law was deemed to be contrary to the First Amendment provision by requiring constitutionally formed private associations to reveal the names of its members

[98] *R v Dyment* [1988] 2 RCS 417 at 427-8.
[99] S D Balz & O Hance 'Privacy and the internet: Intrusion, surveillance and personal data' (1996) 10 (2) *International Review of Law Computers & Technology* 222-223.
[100] *R v Duarte* [1990] 1 SCR 30 at 47.
[101] *Loving v Virginia* 388 U.S.1 (1967) on interracial marriage; *Parenthood v Casey* 505 U.S. 833 (1992) on termination of pregnancy through abortion and *Lawrence v Texas* 539 U.S. 558 (2003) on same-sex sodomy. See also Spratt 'An economic argument for electronic privacy' (2011) 6 (3) *I/S: A Journal of Law and Policy for the Information Society* 526.
[102] *Lochner v New York* 198 U.S. 45 (1905) at 57.
[103] *National Association for the Advancement of Colored People v Alabama ex. Rel. Patterson* 357 U.S. 449 (1958) at 464-465.
[104] ibid 465.

and officers.[105] The First Amendment to the USA Constitution has provisions that prohibit the making of laws curtailing the freedom of assembly and the freedom of speech.[106]

The Supreme Court of the USA also relied on the First Amendment to protect informational privacy in *Bartnicki v Vopper*, in which it prohibited the re-broadcasting of a telephone conversation that had been illegally intercepted by a commercial radio station.[107] This was deemed to be unconstitutional by the Supreme Court because the interception violated the right to privacy and the freedom of speech granted by the First Amendment.[108]

The Supreme Court also based its decision on the First Amendment to the USA Constitution in *McIntyre v Ohio Elections Commission* by recognising the right to anonymity.[109] In *Watchtower Society v Village of Stratton,* the First Amendment implied right to anonymity was also the basis for repudiating a law that required registration with the government in order to do door-to-door canvassing or soliciting.[110]

In *Reno v American Civil Liberties Union*[111] and in *McNamara v Freedom Newspapers, Inc.*,[112] the court defended both the right to privacy and the right to access information by applying the First Amendment to the USA Constitution.[113] In *McNamara v Freedom Newspapers*, the case involved a plaintiff who was featured in a newspaper article that reported a school game as chasing a soccer ball with his pants falling and his genitalia exposed.[114] The plaintiff lost the case because the court pointed out that this article was an

[105] ibid.
[106] First Amendment to the United States Constitution.
[107] *Bartnicki v Vopper* 532 U.S. 514 (2001) at 516.
[108] ibid.
[109] *McIntyre v Ohio Elections Commission* 514 U.S. 334 (1995) at 378.
[110] *Watchtower Society v Village of Stratton* 536 U.S. 150 (2002) at 166-169.
[111] *Reno v American Civil Liberties Union* 521 U.S. 844 (1997).
[112] *McNamara v Freedom Newspapers, Inc.* 802 S.W.2d 901 (Tex. App. 1991).
[113] See Note 107 above.
[114] *McNamara v Freedom Newspapers, Inc.* 802 S.W.2d 901 (Tex. App. 1991) at 901.

accurate depiction of the event and that the event was newsworthy, thereby protecting the right of access to information.[115]

6.5.2. Third Amendment

The Third Amendment to the USA Constitution provides that in the time of peace in the USA, no soldier shall be quartered in any house unless consent has been given by the owner of the house.[116] This is a guarantee against invasion of privacy by the army during the time of peace.[117] The Third Amendment provision extends to require that if there is war; quartering of soldiers must be done in a way prescribed by the law.[118]

6.5.3. Fourth Amendment

The Fourth Amendment to the USA Constitution provides that:

> "…the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated...."[119]

In *Rakas v Illinois* the court defined 'unreasonable search' defined by the Bill of Rights 1791, Fourth Amendment as the 'governmental invasion of privacy'.[120]

Both the case of *Olmstead v United States*[121] and the case of *Katz v United States*[122] involved the issues of telephone interception with the court pointing out in *Olmstead v United States*

---

[115] ibid.
[116] Laosebikan 'Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in internet Cafes and Suggestions for Appropriate Legislation in Nigeria' (unpublished LLD dissertation, University of KwaZulu-Natal, 2007) 187.
[117] ibid.
[118] ibid.
[119] See Fourth Amendment to the USA Constitution.
[120] *Rakas v Illinois* 439 U.S. 128 (1978) at 132 and 143.
[121] *Olmstead v United States* 277 U.S. 438 (1927).
[122] *Katz v United States* 389 U.S. 347 (1967).

that telephone tapping did not constitute an 'unreasonable search'.[123] In *Katz v United States*, the Supreme Court applied the Fourth Amendment by pointing out that electronic eavesdropping was considered to be an "unreasonable search" if the conversation was private.[124]

By expanding the scope of the Fourth Amendment to render wiretapping without a warrant unconstitutional, the decision in *Katz v United States* reversed the Supreme Court's decision in the case of *Olmstead v United States*.[125] In *People v Shinkle*, the court accepted an intercepted telephone conversation as admissible evidence since consent had been given by another party to the conversation and it was therefore considered that there was no breach of the right to privacy.[126] In the United Kingdom case of *Attorney General v Guardian Newspapers*, Lord Goff also stated that the only time when eavesdropping or a telephone interception amounts to a violation of the right to privacy is when a third party eavesdrops on a conversation without the consent of both or any one of the parties to that conversation. [127]

Again, in the 'Fourth Amendment' case of *Olmstead v United States*,[128] Justice Brandeis argued (in dissent) that although there is no express right to privacy in the USA Constitution, there is 'the right to be let alone' as first described by Judge Thomas M. Cooley in 1864 when he was still a Michigan jurist at the beginning of his profession as city clerk.[129] It was in the same case of *Olmstead v United States* that Justice Brandeis, concerning individual privacy, stated that:

---

[123] See Note 120 above. Olmstead v United States 277 U.S. 438 (1927) at 466.
[124] *Katz v United States* 389 U.S. 347 (1967) at 353.
[125] F O Laosebikan 'Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in internet Cafes and Suggestions for Appropriate Legislation in Nigeria (unpublished LLD dissertation, University of KwaZulu-Natal, 2007) 189.
[126] *People v Shinkle* 128 Ill.2d 480, 486, 132 Ill.Dec. 432, 539 N.E.2d 1238 (1989) at 483.
[127] *Attorney General v Guardian* Newspapers (No2) [1990] 1 AC 109 at 281.
[128] *Olmstead v United States* 277 U.S. 438 (1927) at 478.
[129] Iannotta 'Protecting individual privacy in the shadow of a national data base: The need for data protection legislation' (1989) 17 (1) *Capital University Law Review* 125.

> "The makers of our Constitution undertook to secure conditions favourable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things.
>
> They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone - the most comprehensive of rights and the most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[130]

This argument received a lot of support in the USA, Canada and other outside countries' courts, even though it was a judgement in the minority.[131] In another 'Fourth Amendment' case of *United States v Jones*,[132] the right to privacy was also advocated for by a successful challenge made on GPS surveillance.[133] The judge in this case considered surveillance to be an infringement on an individual's right of privacy.[134]

The conclusion in *United States v Jones* is consistent with Supreme Court's Fourth Amendment jurisprudence applied in *Katz v United States*, which has moved from the exclusive property-based approach to an individual's 'reasonable expectation of privacy' in

[130] *Olmstead v United States* 277 U.S. 438 (1927) at 478.
[131] M Bharwaney and A Marwah 'Personal data privacy in the digital age' (2013) 43 (3) *Hong Kong Law Journal* 805.
[132] *United States v Jones* 132 S. Ct. 945, 949 (2012) at 955.
[133] ibid.
[134] ibid.

any industry.[135] The Court used the 'reasonable expectation of privacy' test in *Katz* but did not substitute it for the 'common-law of trespassing' test.[136]

The court in *Smith v Maryland*, also pointed out that, if there is no 'reasonable expectation of privacy', there can be no violation of the right to privacy.[137] In this case, the Fourth Amendment search could not be invoked because the law enforcement officials electronically monitored numbers that were dialled from a private phone and therefore, there was a clear 'reasonable expectation of privacy'.[138] It was also in *United States v David Lee Smith*, that the court also mentioned that if a cell-phone is used or any codeless phone, a Fourth Amendment search cannot be invoked since there is a 'reasonable right of privacy'.[139]

The Fourth Amendment search was permitted in *New Jersey v T.L.O.* where the court ruled that there could not be an invasion of privacy if a search is not conducted in a home but in a public space like a school, business environment or offices.[140] In this *New Jersey v T.L.O.* case, the vice-principal at a certain school had searched the purse belonging to a pupil suspected of possessing drugs.[141] In the purse she found some marijuana and the court deemed this search permissible citing that even though students have a reasonable 'expectation of privacy', the search conducted is reasonably related to the objectives of the search and not excessively intrusive in the light of the student's age, sex and the nature of the infraction.[142]

In *O'Connor v Ortega*, while a psychiatrist was on leave, his office was searched because he was suspected of being involved in illegal activities and the court pointed out that the

---

[135] A E Wade 'A new age of privacy protection: A proposal for an international personal data privacy treaty' (2010) 42 (1) *The George Washington International Law Review* 663.
[136] ibid.
[137] *Smith v Maryland* 442 U.S. 735 (1979) at 740.
[138] ibid 2577.
[139] *United States v David Lee Smith* 978 F.2d 171 (5th Cir. 1992) at para 10.
[140] *New Jersey v T.L.O.* 469 U.S. 325 (1985) at 340.
[141] ibid at 340.
[142] ibid at 340-341.

employer can use the Fourth Amendment search without violating the employees right of privacy, if that employee has a standard of reasonableness to conduct the search.[143] Similarly, in *Alana Shoars v Epson America, Inc. No*., even though the facts were different, the court stated that the employer has a right to read all employee emails since there is a reasonable expectation that all mails sent and received relate to work.[144]

In *United States v Miller* and in *Smith v Maryland*, the court concluded that the private personal identifiable information found in cheques that are deposited into a bank voluntarily, form part of ordinary commerce and therefore, there is no Fourth Amendment expectation of privacy arising from that.[145] These two decisions have been highly criticized since then for suggesting that customers can forfeit their right to privacy by complying with requirements of the service providers.[146]

6.5.4. Fifth Amendment

This Amendment protects against informational privacy by stating that a person shall not be compelled to testify against him/herself by giving information to be used for his or her prosecution.[147]

6.5.5. Ninth Amendment

The Fifth Amendment to the USA Constitution states that:

> "…the enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people".[148]

---

[143] *O'Connor v Ortega* 480 U.S. 709 (1987) at 718 and 731.
[144] *Alana Shoars v Epson America, Inc.* No. SWC112749 (L.A. Super. Ct. 1990).
[145] *United States v Miller* (1976) 425 US 435 at 441-443 and *Smith v Maryland* 442 U.S. 735 (1979) at 439-440.
[146] Laosebikan 'Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in internet Cafes and Suggestions for Appropriate Legislation in Nigeria' (unpublished LLD dissertation, University of KwaZulu-Natal, 2007) 194.
[147] ibid 196.

The Supreme Court used this provision in *Griswold v Connecticut*, disputing the fact that the lack of a specific right of privacy in the Bill of Rights means that no such right exists.[149] The Supreme Court argued that such a right to privacy exists if it is implicit in the concept of the ordered liberty.[150] The same sentiments were reiterated in *Bowers v Hardwick.*[151]

Again, in *Griswold v Connecticut*, Justice Goldberg also expressed his belief that the right to privacy was in the penumbra of the Bill of Rights by stating that:[152]

> "…the right of privacy in the marital relation is fundamental and basic - a personal right 'retained by the people' within the meaning of the ninth amendment." [153]

Thus the USA Supreme Court pointed out, that even though there is no explicit constitutional right to privacy, there was a Ninth Amendment implicit right to privacy.[154] The court also mentioned in *Bowers v Hardwick* that when considering whether any right should be recognized or not, the courts are also supposed to ask whether that right is deeply rooted in the country's history and or traditions.[155]

6.5.6. Fourteenth Amendment

The Supreme Court in *Griswold v Connecticut* also pointed to the Fourteenth Amendment of the Constitution of the USA which prohibits the making of laws or enforcing of laws that

---

[148] ibid 194.
[149] *Griswold v Connecticut* 381 U.S. 479 (1965) at 524.
[150] ibid.
[151] *Bowers v Hardwick* 478 U.S. 186 (1986) at 191-194.
[152] Bergerson 'E-commerce privacy and the black hole of cyberspace' (2001) 27 (3) *William Mitchell Law Review* 1534.
[153] *Griswold v Connecticut* 381 U.S. 479 (1965) at 499. Flaherty 'On the utility of constitutional rights to privacy and data protection' (1991) 41 (1) *Case Western Reserve Law Review* 838.
[154] Wade 'A new age of privacy protection: A proposal for an international personal data privacy treaty' (2010) 42 (1) *The George Washington International Law Review* 663.
[155] *Bowers v Hardwick* 478 U.S. 186 (1986) at 191-192.

abridge the citizens' immunities or privileges.[156] In *Roe v Wade*, the Supreme Court went even further in interpreting the Fourteenth Amendment's concept of personal liberty to include the right to privacy.[157]

In upholding substantive privacy rights in both of these cases, the Supreme Court applied the Fourteenth Amendment. Although the court defended substantive privacy rights, in these cases, it also noted that the scope covered by this Amendment is so wide and could include informational privacy rights.[158]

6.6. Statutory Protection of Privacy and Data in the United States of America under Federal Laws and Other Sector-Specific Privacy State Law Bills

Although there are various statutes that protect individual privacy in the USA as shall be seen below, the following Acts only protect against unwarranted government intrusion into personal privacy: The Electronic Communications Privacy Act of 1986 restricts warrantless electronic surveillance during criminal investigation;[159] The Family Educational Rights and Privacy Act of 1974 limits the disclosure of student information by Federally-funded schools:[160] and The Driver's Privacy Protection Act of 1994 restricts the disclosure of private information by state motor vehicle offices,[161] do not apply to the private sector.

The Privacy Act of 1974[162] and The Freedom of Information Act of 1966[163] are the only two statutes in the USA that deal with both privacy protection as well as data protection as shall be seen below.

---

[156] *Griswold v Connecticut* 381 U.S. 479 (1965) at 499.
[157] *Roe v Wade* 410 U.S. 113 (1973) at 129.
[158] ibid.
[159] Electronic Communications Privacy Act of 1986, 18 U.S.C. Section 2510 (1986).
[160] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. Section 1232g (1974).
[161] Driver's Privacy Protection Act of 1994, 18 U.S.C. Section 2721 (1994).
[162] Privacy Act of 1974, 5 U.S.C Section 552a (1974), as amended.
[163] Freedom of Information Act of 1966, 5 U.S.C Section 552 (1996), as amended.

It was due to the lack of an express direction in matters involving informational privacy by the common law and by the Constitution of the USA, that congress sought to remedy this by passing various pieces of legislation.[164] There are various laws that are aimed at protecting online data and privacy, but in specific sectors of the Federal government and these affect online businesses at the Federal level.[165] The sector-specific legislation is based on each industry determining the meaning of the term 'appropriate' in terms of privacy according to its industry norms and it relies heavily on self-created privacy standards that are outside the Federal privacy laws.[166] Some of these statutes are not created entirely for the purposes of protecting online business, although they serve well in that aspect.

There are some other state laws such as ones which stipulate restrictions on the use and display of social security numbers which generally function as Federal identification numbers for USA nationals.[167] Generally, most of these laws restrict or prohibit the use of social security numbers as account numbers without individuals consenting and the ability to request from individuals or display social security numbers on the internet over an unsecure connection or unencrypted transmission.[168]

6.6.1. Federal Trade Commission Act of 1914

The Federal Trade Commission Act of 1914, (38 Stat. 717) (hereafter Federal Trade Commission Act) was signed into law by President Woodrow Wilson in 1913 and it allows the Federal Trade Commission (independent administrative agency organised in 1915 pursuant to the Federal Trade Commission Act) to act in the interest of all consumers to

[164] Iannotta 'Protecting individual privacy in the shadow of a national data base: The need for data protection legislation' (1989) 17 (1) *Capital University Law Review* 125.
[165] Plave 'Franchising: Data protection and e-commerce issues in the United States' (2006) 4 (2) *International Journal of Franchising Law* 11.
[166] Border 'Untangling the web' (2012) 35 (2) *Suffolk Transnational Law Review* 367-368.
[167] See Note 165 above 12.
[168] ibid. See also Section 29 of the Privacy Act of 2005, (2005; 109th Congress Section 116).

prevent deceptive and unfair acts or practices, thus protecting the data and privacy of online traders.[169]

There are four core principles that can be extracted from the undertakings of the Federal Trade Commission in its bid to protect the privacy of consumer information collected over the internet and stored in databases.[170] To protect the privacy of consumer information collected over the internet and stored in databases, the four principals guiding data collection are 'notice or awareness', 'choice or consent', 'access or participation', and 'security, enforcement or redress'.[171]

In its Federal Trade Commission Report to Congress on Privacy Online, which contained a seminal report submitted to Congress, the Federal Trade Commission stated that:

> "…these core principles require that consumers be given notice of an entity's information practices; that consumers be given choice with respect to the use and dissemination of information collected from or about them; that consumers be given access to information about them collected and stored by an entity; and that the data collector take appropriate steps to ensure the security and integrity of any information collected."[172]

The report to Congress by the Federal Trade Commission was foundational to the establishment of the Privacy Act of 1974,[173] another very important piece of legislation dealing with e-commerce privacy and data protection.[174] The principles above as set out by

---

[169] See Section 5 of the Federal Trade Commission Act of 1914 (38 Stat. 717).
[170] See Note 165 above at 9.
[171] ibid.
[172] ibid. Federal Trade Commission 'Privacy online: A Report to Congress' June 1998 available at https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf, at part ii accessed on 31 July 2017.
[173] The Privacy Act of 1974, 5 U.S.C. Section 552a (1974).
[174] B E Robinson *Financial Privacy & Electronic Commerce: Who's in My Business* (2000) 18.

the Federal Trade Commission Act became a framework for online privacy and were to be adopted in online activities by all the online entities.[175]

As a follow up to the policy report, in August of 1998, the Federal Trade Commission began the enforcement of privacy violations by charging Geo-Cities for failure to protect individual privacy.[176] Geo-Cities is a web-based company that failed to protect the online consumer's privacy by collecting and using information from its website improperly.[177]

6.6.2. Freedom of Information Act of 1966

The Freedom of Information Act of 1966[178] is similar to the Privacy Act of 1974[179] in that it applies to Federal agencies and other private agencies that process and control information flow.[180] The Freedom of Information Act promotes access to government information by the public, with its main objective being the disclosure of government records according to the procedural laws.[181]

The Freedom of Information Act provides that information must be given to the public[182] and specific information must be made available for public inspection and copying.[183] The provisions above regulate the collection and the disclosure of information.[184]

To the extent required for the prevention of a clearly unwarranted privacy invasion, the Freedom of Information Act also provides that details that identify an individual may be deleted from the copies of records, policy statements, opinions, interpretations, staff manuals

[175] ibid.
[176] ibid 19.
[177] ibid 20.
[178] Freedom of Information Act of 1966, 5 U.S.C Section 552 as amended (1974) and (1986).
[179] Privacy Act of 1974, 5 U.S.C Section 552a (1974), as amended.
[180] See Section 552 (*f)* (l*)* of the Freedom of Information Act of 1996, 5 U.S.C Section 552 (1966).
[181] See Section 552 (*a*) (1)-(6) of the Freedom of Information Act of 1996, 5 U.S.C Section 552 (1966).
[182] See Section 552 (*a*) (I) (A)-(E) of the Freedom of Information Act of 1996, 5 U.S.C Section 552 (1966).
[183] See Section 552 (*a)* (2) of the Freedom of Information Act of 1996, 5 U.S.C Section 552 (1966).
[184] Laosebikan 'Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in internet Cafes and Suggestions for Appropriate Legislation in Nigeria' (unpublished LLD dissertation, University of KwaZulu-Natal, 2007) 219.

and instructions.[185] Even though the Freedom of Information Act provides for the disclosure of information by the government agencies, it also provides some exemptions for the purposes of privacy protection.[186]

Exempted information that cannot be disclosed includes all the trade secrets, commercial and financial information taken from an individual, certain financial records, privileged and confidential information, personnel and medical files or such files which would amount to invasion of privacy if disclosed records or information put together for the purposes of law enforcement.[187]

In *United States Department of Justice v Reporters Committee for Freedom of the Press*, the court upheld the decision by the Department of Justice to conceal some information because the disclosure of the criminal records would be contrary to one of the exemptions cited in section 552 (*b*) (7) (A)-(F) of the Freedom of Information Act.[188] The court pointed out that the main purpose of the Freedom of Information Act was not to disclose private information about citizens but to ensure openness in all the Government's dealings with its citizens.[189] The Freedom of Information Act also prohibits the disclosure of information or records compiled for the mere purposes of law enforcement if that information would amount to the invasion of privacy.[190]

The Freedom of Information Act also provides that the information described as 'classified information' by reason of an Executive Order must be kept as secret information, if it is for

[185] ibid 220. See also Section 552 (*a*) (2) (E) of the Freedom of Information Act of 1996, 5 U.S.C Section 552 (1966).
[186] See Note 184 above at 220.
[187] See Section 552 (*b*) (4), Section 552 (*b*) (6) and Section 552 (*b*) (7) (A)-(F) of the Freedom of Information Act of 1996, 5 U.S.C Section 552 (1966). Note: Where the production of such records might constitute an invasion of privacy, violate the confidentiality rights of the State, private institutions or persons, or in other ways jeopardise the interest of the law, private persons or the State.
[188] *United States Department of Justice v Reporters Committee for Freedom of the Press* 489 U.S. 749 (1989) at 774.
[189] ibid.
[190] See Section 552 (*b*) (7) (A)-(F) of the Freedom of Information Act of 1996, 5 U.S.C Section 552 (1966).

the purposes of national policy or national defence.[191] The Freedom of Information Act also exempts the disclosure of information relating to internal rules, information exempted by statute, inter-agency and intra-agency memorandums and letters that are not readily and ordinarily available to the public.[192]

However, in *Chrysler Corp. v Brown*, the exemptions in the Freedom of Information Act of 1966 were ruled not to be guaranteed rights as they are not compulsory.[193] An agent has discretion to disclose any kind of information and no individual can rely solely on these exemptions in order to prohibit the agent from disclosing such information.[194]

In order to include disclosure of computerized records, the Freedom of Information Act[195] was amended by the Electronic Freedom of Information Act of 1996[196] which makes the Freedom of Information Act to allow for electronic records to be disclosed in the same way as paper-based records.[197]

6.6.3. Wiretap Act of 1968

The Wiretap Act of 1968, 18 U.S.C. Sections 2510-2522 provides for informational protection against unlawful search and seizure of personal information only if the personal information is being transmitted through telephone communications systems.[198] The *Katz v Olmstead* decision which prohibited the tapping of telephone lines with no warrant, led to the passing of the Wiretap Act.[199] While it is illegal for a private person to record a third party's

[191] See Section 552 (*b*) (1) of the Freedom of Information Act of 1996, 5 U.S.C Section 552 (1966).
[192] Section 552 (*b*) (2), Section 552 (*b*) (3), Section 552 (*b*) (4) and Section 552b (5) of the Freedom of Information Act of 1996, 5 U.S.C Section 552 (1966).
[193] *Chrysler Corp. v Brown* 441 U.S. 281 (1979) at 290-294.
[194] ibid.
[195] See Section 552 of the Freedom of Information Act of 1996, 5 U.S.C Section 552 (1966).
[196] Electronic Freedom of Information Act of 1996, 5 U.S.C. Section 552 (Supp. II 1996).
[197] See Section 552 (*f*) (2) of the Freedom of Information Act of 1996, 5 U.S.C Section 552 (1966).
[198] See Section 2511 (2) of the Wiretap Act of 1968, 18 U.S.C. Sections 2510-2522.
[199] *Katz v United States* 389 U.S. 347 (1967) at 350-353.

phone call without their consent, the government can intercept telephone calls, provided it has met all the basic requirements given by the Wiretap Act in order to get a warrant.[200]

The decision in *Bartnicki v Vopper* permitted wiretapping as the court pointed out that disclosure of media is not prohibited if the information that has been published is a 'public concern'.[201] This decision was criticized by many as an erroneous decision.[202]

6.6.4. Fair Credit Reporting Act of 1970

The first piece of legislation advanced by the US Congress to deal with issues of privacy specifically was the Fair Credit Reporting Act of 1970, 15 U.S.C. Section 1681 (1970) (hereafter FCRA).[203] FCRA only applies to financial institutions that process and hold personal identifiable information.[204] FCRA prohibits the unauthorized disclosure of credit information that is arbitrary and inaccurate unless if such a disclosure is for the purposes described by the Act.[205] Although the FCRA prohibits information disclosures, there are some exemptions to this general rule, for example; giving information to someone named in a report, where there is a legitimate business need to do so and if the disclosure of information is in compliance with the court order.[206]

FCRA deals with the respect that should be given to consumers over their right of privacy.[207] This complex piece of legislation deals with the use of personal identifiable information by

[200] See Section 2511 (2) (*d*) of the Wiretap Act of 1968, 18 U.S.C. Sections 2510-2522.
[201] *Bartnicki v Vopper* 532 U.S. 514 (2001) at 524-525.
[202] T Wilkinson 'Is anyone listening to me? *Bartnicki v Vopper'* (2003) 63 (2) *Louisiana Law Review* 601.
[203] Border 'Untangling the web' (2012) 35 (2) *Suffolk Transnational Law Review* 365-366.
[204] Spratt 'An economic argument for electronic privacy' (2011) 6 (3) *I/S: A Journal of Law and Policy for the Information Society* 528. A H Davis… et al 'The economics of privacy and data security' (2013) 9 (1) *Journal of Law, Economics & Policy* 465.
[205] See Section 1681 (*b*) of the Fair Credit Reporting Act of 1970, 15 U.S.C. Section 1681 (1970). A J Marcella and C Stucki *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues* (2003) 133.
[206] See Section 1681 (*b*) (*a*) (1) (2) and (3) of the Fair Credit Reporting Act of 1970, 15 U.S.C. Section 1681 (1970).
[207] See Section 1681 (*a*) (4) of the Fair Credit Reporting Act of 1970, 15 U.S.C. Section 1681 (1970).

consumer credit reporting agencies.[208] It limited the consumer credit reports' information to some specific uses.[209] Any business that wants to use such information from the credit reports must first comply with the requirements of the Fair Credit Reporting Act's 'Disposal Rule' which requires proper and secure reporting of consumer credit information.[210] The Disposal Rule was included in the Fair and Accurate Credit Transactions Act of 2003 (FACTA) which amended the FCRA.[211]

The FCRA also deals with account number truncation by prohibiting any person that accepts a credit or a debit card for the transaction of business from printing more than the last five digits of the account number or of the expiration date of the credit or debit card on any receipt provided to the card-holder.[212]

The FCRA also requires that personal credit information be given by agencies if it benefits the federal government or if the one who requests the information will:

> "…use the information in connection with a credit transaction involving the consumer ... or otherwise has a legitimate business need for the information in connection with a business transaction involving the consumer"[213]

Nothing in the FCRA shall exempt persons from complying with any Federal state laws regarding the collection, the distribution or the use of any information on consumers, or for

[208] Border 'Untangling the web' (2012) 35 (2) *Suffolk Transnational Law Review* 366.
[209] ibid.
[210] See Section 216 of the Fair and Accurate Credit Transactions Act of 2003.
[211] D Eleftheriou… et al 'Data protection and e-commerce in the United States and the European Union' (2006) 40 (2) *The International Lawyer* 394.
[212] See Section 1681 (*g*) of the Fair Credit Reporting Act of 1970, 15 U.S.C. Section 1681 (1970). Bergerson 'E-commerce privacy and the black hole of cyberspace' (2001) 27 (3) *William Mitchell Law Review* 1537.
[213] See Section 1681 (*b*) (3) of the Fair Credit Reporting Act of 1970, 15 U.S.C. Section 1681 (1970).

the prevention or mitigation of identity theft, but of course with some exception to the extent of any inconsistency with the FCRA.[214]

Even though the applicability of the FCRA to consumers involved in electronic commerce businesses is limited, it has evidenced congressional interest when it comes to e-commerce personal identifiable information collection, distribution and disclosure.[215] The FCRA protects privacy by giving customers the right to correct information in credit files and thereby permitting consumers to be aware of the information that is available about them and to exercise some form of control over that information.[216] The FCRA prohibits certain information from being included in the credit files of customers and therefore privacy is protected.[217]

6.6.5. The Privacy Act of 1974

The Privacy Act of 1974, 5 U.S.C. Section 552a (1974), limits the Federal government's capacity to collect, retain, and process (use) personal identifiable information.[218] The Privacy Act also gives consumers who use electronic transactions in e-commerce the right to review and have their records corrected.[219] In the USA, the Privacy Act places on all record-keeping agencies of the Federal government, the requirement for privacy protection, but not private companies.[220] Private entities cannot be held responsible or liable under the Privacy Act since only public entities are subject to it.[221]

---

[214] See Section 1681, subsection 625 of the Fair Credit Reporting Act of 1970, 15 U.S.C. Section 1681 (1970).
[215] Bergerson 'E-commerce privacy and the black hole of cyberspace' (2001) 27 (3) *William Mitchell Law Review* 1537.
[216] See Section 1861 (*i*) of the Fair Credit Reporting Act of 1970, 15 U.S.C. Section 1681 (1970).
[217] See Section 1861 (*c*) of the Fair Credit Reporting Act of 1970, 15 U.S.C. Section 1681 (1970).
[218] Spratt 'An economic argument for electronic privacy' (2011) 6 (3) *I/S: A Journal of Law and Policy for the Information Society* 526.
[219] ibid. A J Marcella and C Stucki *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues* (2003) 134.
[220] R Turn 'Privacy protection and security in transnational data processing systems' (1980) 16 (1) *Stanford Journal of International Law* 70. See also *Ditman v California* 191 F 3d 804 (9th Cir 1999).
[221] *Sutton v Providence St Joseph Medical Center* 192 F 3d 826 (9th Cir. 1999).

This piece of legislation shows that increases in technology and increases in the sophistication of computer systems has led to intrusion and to the invasion of privacy that takes place when personal identifiable information is being collected, stored, maintained, processed and disseminated. [222] Although there is no express statement in the USA Constitution, in the Privacy Act, the right to privacy is deemed to be a fundamental and personal right.[223]

The Privacy Act permits individuals to have access to their personal information and to have that information corrected if it is considered to be inaccurate.[224] Besides the conditions for disclosure of any agency records, the Privacy Act also provides controls to be applied when collecting data and when publishing personal identifiable information as kept by the Federal agent.[225]

Agent maintained records must be reasonably accurate, timely, relevant and complete.[226] In *Bechhoefer v U.S. Department of Justice Drug Enforcement Admin*, the court defined records as any information about a person that is private and is only connected to that person through an identifying particular.[227] In *Tobey v NLRB*, the court also held that information which is defined as a record must have a person's name or any of the identifying particulars.[228] In *McGregor v Greer*, information which was retained in the records of the Department of Education was said to not constitute a "record" by the court since it was retrievable using the name of the employee or his identifying particulars.[229]

---

[222] See Section 552a (*a*) (2) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974).
[223] See Section 552a (*a*) (4) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974).
[224] See Section 552a (*d)* (2-(4) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974).
[225] See Section 552a (*e*) (2), 552a (*e*) (4) (A)-(I) and 552a (*b*) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974).
[226] See Section 552a (*e*) (5) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974).
[227] *Bechhoefer v U.S. Department of Justice Drug Enforcement Admin* 209 F3d 57 (2d Cir. 2000) at para 1.
[228] *Tobey v NLRB* 40 F3d 469 (Dc Cir. 1994).
[229] *McGregor v Greer* 748 F Supp 881(DC 1990) at 888-889.

There are several rules surrounding the collection, the use and the disclosure of personal identifiable information in the Privacy Act.[230] According to the Privacy Act, individuals from whom information is being collected must be informed of such a process, must be told if the disclosure is mandatory or voluntary and information must only be used for the purposes for which it was collected.[231]

While Congress sought to prohibit the Federal government agents from disclosing private personal identifiable information without the consent of the individual concerned, they also set up some exemptions to the provision under the 'routine use' exception.[232] 'Routine use', as an exemption to allow government agencies to disseminate personal identifiable information without prior consent would mean a use whose purpose is very much compatible with the purpose for which that information was collected.[233]

Most critics of these exemptions have termed this 'routine use' as the 'removal of teeth from a vicious dog'.[234] It is also worth noting that there are no mechanisms in place created by the Privacy Act to inform the Americans of their right of inspection.[235] This, according to critics, renders the Act ineffectual, since the Privacy Act then fails in securing individual right to privacy.[236]

For individuals whose right to privacy has been violated, the Privacy Act provides for civil remedies.[237] In other cases, the breach of someone's right to privacy can actually attract a

[230] See Section 552a (*b*) (*c*) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974).
[231] Section 552a (*e*) (3) (A) and (B) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974).
[232] Section 552a (*b*) (1)-(12) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974).
[233] Section 552a (*a*) (7) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974). Banisar & Davies 'Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments' (199) 18 (1) *Journal of Computer and Information Law* 109.
[234] Iannotta 'Protecting individual privacy in the shadow of a national data base: The need for data protection legislation' (1989) 17 (1) *Capital University Law Review* 127.
[235] ibid.
[236] ibid.
[237] See Section 52a (*g*) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974).

criminal penalty of a very limited scope.[238] Most remedies in cases of the violation of a person's right to privacy take the form of awards or court injunctions.[239]

6.6.6. Family Educational Rights and Privacy Act of 1974

The Family Educational Rights and Privacy Act of 1974, (hereafter FERPA) also known as the Buckley Amendment protects the privacy of student education records by prohibiting the disclosure of educational records to anyone else other than the learners themselves or the parents of the learners.[240] It applies to all the schools in the USA that are receiving Federal funding.[241] This restriction by the FERPA has an exception in that Federal, local, State and educational authorities are permitted to have access to educational records when performing their lawful duties.[242]

6.6.7. Copyright Act of 1976

The Copyright Act of 1976, 17 U.S.C. Section 106 protects all original:

> "literary works; musical works, including any accompanying words; dramatic works, including any accompanying music; pantomimes and choreographic works; pictorial, graphic, and sculptural works; motion pictures and other audio-visual works; sound recordings; and architectural works."[243]

[238] See Section 552a (*i*) (1) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974). A Solzhenitsyn & C Ward 'The Privacy Act of 1974: An overview and critique' (1976) 4 *Washington University Law Review* 692.
[239] See Section 552a (*g*) (I) (D) of the Privacy Act of 1974, 5 U.S.C. Section 552a (1974).
[240] See paragraph 1 (A) and Section 2 of the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. Section 1232g; 34 CFR Part 99.
[241] Marcella and Stucki *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues* (2003) 134.
[242] ibid Paragraphs 3, 4 (*a*) and 5.
[243] See Section 102 (*a*) (1)-(8) of the Copyright Act of 1976, 17 U.S.C. Section 106 (1976).

Commercial exploitation of another person's personality is also prohibited by the Copyright Act.[244] Commercial exploitation is defined by the Copyright Act to include the exploitation of a person's name, likeness, photograph, voice or their identifying slogans.[245] The plaintiff was awarded damages in the case of *Midler v Young & Rubicam* when that entertainer's sound and style was copied by another vocalist.[246] In *White v Samsung Electronics America Inc.* where the plaintiff's voice was imitated by a robot, the court ruled that this imitation amounted to commercial exploitation of the plaintiff's personality.[247]

6.6.8. Right to Financial Privacy Act of 1978

When scanning financial records of customers, strict procedures must be followed by Federal Government Agencies as described by The Right to Financial Privacy Act of 1978.[248] The Right to Financial Privacy Act was enacted for the purposes of protecting the confidentiality of personal financial records through a Fourth Amendment protection for all bank records.[249] Unless if it is for the purposes of complying with the Right to Financial Privacy Act, accessing of records by government authorities relating to customers' relationships with consumer reporting agencies, credit card companies and other financial institutions is deemed illegal.[250]

Financial institutions are also prohibited from disclosing customer's financial (records) information unless if it is for the purposes of compliance with the provisions of the Right to

[244] ibid.
[245] ibid.
[246] *Midler v Young & Rubicam* 849 F2d 460 (9th Cir. 1988), 944 F2d 909 (9th Cir. 1991).
[247] *White v Samsung Electronics America Inc.* 989 F2d 1512 (9 Crr. 1993).
[248] See Section 3402 of the Right to Financial Privacy Act of 1978, (12 U.S.C. ch. 35, Section 3401 et seq.)
[249] Marcella and Stucki *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues* (2003) 134.
[250] See Section 3401 (1) (2) and (3) of the Right to Financial Privacy Act of 1978, (12 U.S.C. ch. 35, Section 3401 et seq.).

Financial Privacy Act.[251] The disclosure of financial records by financial institutions will not be deemed illegal if the disclosure has been authorised by the customer through consent.[252]

6.6.9. Electronic Fund Transfer Act of 1978

The Electronic Fund Transfer Act of 1978, (15 USC 1693 et seq.) (hereafter EFTA) was passed by Congress in 1980 with a single and specific application only to financial institutions.[253] Although it only applies to financial institutions, it has a bearing on e-commerce because of its provision which states that notices must be given to consumers by financial institutions before their personal information is disclosed to third parties.[254] The EFTA regulates all the electronic transactions in the banking system for example, cell phone banking, internet banking, automated teller machines (ATMs), point of sale terminal transactions and many others alike.[255]

Customers must be informed by financial institutions as to which information will be made available to a third party.[256] The EFTA also protects customer's privacy by regulating codes as means to access accounts.[257] All codes, passwords, automated teller machine (ATM) cards, Credit Cards, Debit Cards and any other means of accessing accounts should be given to customers only if requested for by way of application or if it is a renewal or replacement of an already existing card or code or password.[258] These and other provisions in the EFTA give

[251] See Section 3403 of the Right to Financial Privacy Act of 1978, (12 U.S.C. ch. 35, Section 3401 et seq.).
[252] See Section 3404 of the Right to Financial Privacy Act of 1978, (12 U.S.C. ch. 35, Section 3401 et seq.).
[253] Bergerson 'E-commerce privacy and the black hole of cyberspace' (2001) 27 (3) *William Mitchell Law Review* 1537-1538.
[254] ibid.
[255] See Section 1693 (*a*) (6) of the Electronic Fund Transfer Act of 1978, (15 USC 1693 et seq.).
[256] See Section 1693 (*c*) (9) of the Electronic Fund Transfer Act of 1978, (15 USC 1693 et seq.).
[257] See Section 1693 (*i)* of the Electronic Fund Transfer Act of 1978, (15 USC 1693 et seq.).
[258] See Section 1693 (*i*) (*a*) (1) and (2) of the Electronic Fund Transfer Act of 1978, (15 USC 1693 et seq.).

some form of security against intrusions and fraudulent invasions of privacy by protecting, private personal identifiable information.[259]

6.6.10. Privacy Protection Act of 1980

For the purposes of protecting privacy by reducing law enforcement controlled searches and seizures of books and other publishers, the USA Congress in 1980 enacted the Privacy Protection Act of 1980 (PPA).[260] Unless if a person is believed to be committing or if there is probable cause to believe that he or she has committed a criminal offence by publishing information in a broadcast, book, newspaper or any such publication, the government official is prohibited from searching and seizing such public communication.[261]

6.6.11. Cable Communications Policy Act of 1984 and the Telecommunications Act of 1996

To amend the Communications Act of 1924, the Cable Communications Policy Act of 1984, (hereafter Cable Act) was enacted by Congress.[262] The Cable Act and the Tele-Communications Act of 1996, read together protect personal identifiable information by imposing restrictions on parties who work in the telecommunications and the cable communications industries.[263] These two pieces of legislation stipulate that collection of and use of personal identifiable information should only be done if that information is necessary to perform the relevant contractual service and if the relevant data subject has given the

[259] Laosebikan 'Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws with Particular Reference to the Protection of Privacy and Data in internet Cafes and Suggestions for Appropriate Legislation in Nigeria' (unpublished LLD dissertation, University of KwaZulu-Natal, 2007) 298.
[260] Marcella and Stucki *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues* (2003) 135.
[261] ibid.
[262] ibid.
[263] ibid 139. Spratt 'An economic argument for electronic privacy' (2011) 6 (3) *I/S: A Journal of Law and Policy for the Information Society* 529.

required consent for his or her information to be collected and or used.[264] These laws are sector-specific legislation as they only apply within strictly defined industries.[265]

6.6.12. Electronic Communication Privacy Act of 1986

Since the Wiretap Act did not apply to emails, computer and other e-communications, the Electronic Communication Privacy Act of 1986, (hereafter ECPA) was enacted by the US Congress to protect privacy in all electronic communications.[266] The ECPA prohibits access to stored electronic communications (emails and computer communications) without the concerned person's consent and it also restricts the government from wiretapping transmissions of electronic data.[267]

The government is allowed by the ECPA to demand handing over of personal consumer data by the service providers.[268] Not only does ECPA cover computer communications, it also includes voice communications devices like the telephones and radio paging instruments which are not included in the Wiretap Act of 1968.[269] The ECPA has pen register and traps and trace provisions which permit tracing of telephone communications under certain circumstances.[270] The ECPA does not cover wireless phones as was confirmed in an unpublished case opinion in *United States v David Lee Smith.*[271]

The ECPA was applied in *McVeigh v Cohen et al* where the court set aside the dismissal of the plaintiff by the defendant on the basis correct procedures were not taken in accordance

[264] ibid.
[265] ibid.
[266] Sohn 'Privacy and security protection under Korean e-commerce law and proposals for its improvements' (2016) 33 (1) *Arizona Journal of International & Comparative Law* 242.
[267] ibid.
[268] ibid.
[269] See Section 2510 (*a*) of the Electronic Communication Privacy Act of 1986, 18 U.S.C. Section 2510-2522. Marcella and Stucki *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues* (2003) 135.
[270] See Section 2510 of the Electronic Communication Privacy Act of 1986, 18 U.S.C. Section 2510-2522.
[271] ibid. *United States v David Lee Smith* 978 F.2d 171 (5th Cir. 1992) at para 10.

with the ECPA when information was obtained from an electronic mail.[272] The ECPA was also enacted as a challenge to the *Smith v Maryland* case decision which pointed out that telephone toll records are not private.[273]

6.6.13. Computer Matching and Privacy Protection Act of 1988

The Computer Matching and Privacy Protection Act of 1988 (hereafter Computer Matching and Privacy Protection Act), was introduced by the USA Senate in an effort to amend the Privacy Act by bringing into balance the developed computer technology and the right to informational privacy.[274] Unlike the Privacy Act which only applies to Federal government agencies, the Computer Matching and Privacy Protection Act apply to both the Federal government agencies as well as to non-Federal matching entities.[275]

The term 'non-Federal matching entity' has been described by the Computer Matching and Privacy Protection Act to mean the local government or the state, or the agency of such a government (local or state), and any private or public organization that is participating in any matching program.[276] Agencies must give individuals an opportunity to verify the correctness of information obtained from records through the match-making programme.[277]

6.6.14. Video Privacy Protection Act of 1988

Following the Cable Communications Policy Act of 1984 which prohibited cable companies from non–consensual disclosure of customer's personal identifiable information without the customer's consent, the Video Privacy Protection Act of 1988[278] was also passed in 1988

[272] *McVeigh v Cohen et al* 983 F Supp 215 (D) DC (1998).
[273] Marcella and Stucki see Note 269 above.
[274] Iannotta 'Protecting individual privacy in the shadow of a national data base: The need for data protection legislation' (1989) 17 (1) *Capital University Law Review* 127-128.
[275] Electronic Communication Privacy Act of 1986, 18 U.S.C. Section 2510-2522. Iannotta ibid at 128.
[276] Iannotta ibid.
[277] See Section 552a (P) (1) (B) of the Computer Matching and Privacy Protection Act of 1988.
[278] Video Privacy Protection Act of 1988.

prohibiting the disclosure of customer's video rental choices without their consent.[279] When customers have selected the videos they want, their selection should be kept private under all circumstances unless consent has been given for the disclosure of such selections.[280]

6.6.15. Children's Online Privacy Protection Act of 1990

The Children's Online Privacy Protection Act of 1990, (hereafter COPPA) provides that when collecting information from children under the age of 13 years, clear notices of informational gathering practices must be provided by any website operators engaged in commercial activities and parents of these children must consent to such solicitations.[281]

When the information has been collected, even after consent has been given, parents have a right to check the information collected, reduce it in extent or quantity and to impose a restriction on that information.[282] Website operators are also mandated by COPPA to have in place, procedures that are reasonable in order to protect the confidentiality, security and integrity of personal identifiable information collected from children.[283]

6.6.16. Drivers' Privacy Protection Act of 1994

In 1993, the Congress passed the Driver's Privacy Act of 1994, which prohibits the Department of Motor Vehicles (DMV) from passing out personal information about licence holders by State motor vehicle agencies.[284] Disclosure of personal information is permitted in

[279] Bergerson 'E-commerce privacy and the black hole of cyberspace' (2001) 27 (3) *William Mitchell Law Review* 1538. See Section 2710 (*b*) (1) of the Video Privacy Protection Act of 1988.
[280] See Section 2710 (*b*) (2) (D) (ii) of the Video Privacy Protection Act of 1988 18 U.S.C. Section 2710 (2002).
[281] See Section 6502 (*b*) (i) and Section 6502 (*b*) (ii) of the Children's Online Privacy Protection Act of 1990, 15 U.S.C. Sections 6501–6506 (1990).
[282] See Section 6502 (B) (i) (ii) and (iii) of the Children's Online Privacy Protection Act of 1990, 15 U.S.C. Sections 6501–6506 (1990).
[283] See Section 6502 (D) of the Children's Online Privacy Protection Act of 1990, 15 U.S.C. Sections 6501–6506 (1990).
[284] See Section 2721 (*a*) (l) and (2) of the Driver's Privacy Act of 1994, 18 U.S.C. Sections 2721-2725 (1994). *Reno v Condon* 528 U.S. 141 (2000) at 148-151.

cases where the information relates to a motor vehicle, driver safety and or performance monitoring.[285]

In cases where the personal information is required by the Federal, State and or local agencies for reasons that relate to the motor vehicle, driver safety and performance monitoring, an exemption to disclose personal information is granted.[286]

6.6.17. Computer Fraud and Abuse Act of 1994

The Computer Fraud and Abuse Act of 1994, (hereafter CFAA) was first introduced in the United States of America in 1986.[287] It was later amended in 1994 and in 1996 and in 2001 through the USA PATRIOT Act.[288] The CFAA prohibits individuals from accessing Federal computers or computers belonging to a financial institution, for the purposes of obtaining personal identifiable information about some other individual.[289]

6.6.18. The Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996, (hereafter HIPPA)[290], also known as Kennedy–Kassebaum Act (a name given after its leading sponsors), deals with all the health care privacy matters of personal information.[291] The HIPPA sets out the standards that should be used when transacting healthcare information electronically.[292] Although the HIPPA apply directly to medical providers and health planers, it however also applies to

[285] See Section 2721 (*b*) of the Driver's Privacy Act of 1994, 18 U.S.C. Sections 2721-2725 (1994).
[286] See Section 2721 (*a*) (1) to (14) of the Driver's Privacy Act of 1994, 18 U.S.C. Sections 2721-2725 (1994).
[287] Computer Fraud and Abuse Act of 1986, 18 U.S.C. Section 1030 (1986). R G Smith… et al *Cybercriminal on Trial* (2004) 92.
[288] Marcella and Stucki *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues* (2003) 135.
[289] K Lee and J Light 'Law and regulation, part 1: Individual interests' in L Shyles (ed) *Deciphering Cyberspace: Making the Most of Digital Communication Technology* (2003) 305.
[290] The Health Insurance Portability and Accountability Act of 1996, 29 U.S.C. Section 1181 (1996).
[291] Plave 'Franchising: Data protection and e-commerce issues in the United States' (2006) 4 (2*) International Journal of Franchising Law* 11. A H Davis… et al 'The economics of privacy and data security' (2013) 9 (1) *Journal of Law, Economics & Policy* 465.
[292] See Section 221 and 264 of the Health Insurance Portability and Accountability Act of 1996, 29 U.S.C. Section 1181 (1996).

associated businesses and, in other instances, to companies that provide or collect health insurance information.[293]

6.6.19. Financial Services Modernization Act of 1999 (The Gramm-Leach Bliley Act (GLBA))

The Gramm-Leach Bliley Act of 1999 (hereafter GLBA) also known as the Financial Services Modernization Act of 1999, applies to the use of personal identifiable information by financial institutions and banks.[294] The GLBA permits the financial institutions to share personal information with affiliated parties without an 'opt-out' option unlike the Fair Credit Reporting Act of 1970 which demands that the financial institution must give the consumers an 'opt-out' option as well as a notice to opt out before sharing their personal information.[295] The disclosure of personal information is only limited to personal information that relates to financial institution's transactions or experiences with the consumer.[296]

The States of California, North Dakota, New Mexico and Vermont adopted the GLBA, which provides for even tougher privacy laws by forbidding entities from sharing personal information with third parties unless a consumer affirmatively by consent "opts in" to the disclosure.[297]

In *American Bankers Association v Lockyer*, (ABA v Lockyer), the ABA claimed that California's limitations on data sharing with affiliates were pre-emptied by the FCRA.[298] Due to this gap, the GLBA was amended in part by the enactment of the Privacy Act[299] to now require a business entity the sale or marketing of personally identifiable information to non-

[293] ibid. Davis… et al see Note 291 above at 468.
[294] Davis… et al ibid 526.
[295] D Medine & N D Steimer 'Recent developments in data security and data privacy' (2005-2006) 1 (1) *Journal of Payment System Laws* 275. Davis… et al see Note 290 above.
[296] ibid 276.
[297] See Section 501-510 of the Gramm-Leach Bliley Act of 1999.
[298] *American Bankers Association v Lockyer* No. 05-17163, 2008 WL 4070308 (9th Cir. Sept. 4, 2008).
[299] Privacy Act of 2005.

affiliated parties.[300] The Privacy Act of 2005 also requires financial institutions to allow its customers the opportunity to opt out of personal information sharing under a joint agreement between financial institutions of which such information is exempted from the opt-out requirement under the GLBA.[301]

6.6.20. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, otherwise known as the USA PATRIOT Act was enacted as an amendment to the FERPA. The USA PATRIOT Act amended the FERPA in 1994 to allow for the disclosure of certain records for purposes of investigation and prosecution of terrorism by the appropriate Federal authorities by giving exceptions to wiretapping.[302]

The USA PATRIOT Act amended section 2516 of the ECPA to permit interception of oral, wire and e-communications in cases relating to computer abuse and fraud.[303] The USA PATRIOT Act also amended section 2517 of the ECPA to allow law enforcement officers to disclose information (contents of oral, wire and e-communications) to Federal intelligence officials or security agents if the information relates to counter-intelligence or foreign intelligence.[304] For the purposes of protecting life and limb, the USA PATRIOT Act further amended the ECPA by authorizing the disclosure of electronic information in such circumstances.[305] Section 204 and 217 of the USA PATRIOT Act also allows for the interception of electronic communications if the information contained in the communication

[300] See Section 116 of the Privacy Act of 2005.
[301] ibid.
[302] See Section 507 of the PATRIOT Act of 2001.
[303] See Section 202 of the PATRIOT Act of 2001.
[304] See Section 203 of the PATRIOT Act of 2001.
[305] See Section 212 of the PATRIOT Act of 2001.

is classified as intelligence information[306] and if communication is done by computer trespassers.[307]

The controversial USA PATRIOT Act threatens the right to privacy.[308] It allows for searches of business records, roving wiretaps and surveillance of individuals suspected of terrorist related activities not linked to terrorist groups.[309] The USA PATRIOT Act was amended by the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 otherwise known as the USA FREEDOM Act to prohibit the National Security Agency (NSA) from continuing its unrestricted mass email data collection.[310] The USA FREEDOM Act prohibits communication companies from retaining the data from which the National Security Agency (NSA) obtains information unless if permitted by the Federal court.[311]

6.6.21. Social Security On-Line Privacy Protection Act of 2001

This prohibits computer services that are interactive from disclosing personal identifiable information to third parties without the written consent from the individual concerned.[312]

6.6.22. Social Security Number Protection Act of 2005

The Social Security Number Protection Act (HR 1078) prohibits the purchasing or selling of any individual's social security account number or social security number in a way that violates the provisions of the Federal Trade Commissions' regulations.[313] This law would

[306] See Section 204 of the PATRIOT Act of 2001.
[307] See Section 217 of the PATRIOT Act of 2001.
[308] Sohn 'Privacy and security protection under Korean e-commerce law and proposals for Its Improvements' (2016) 33 (1) *Arizona Journal of International & Comparative Law* 242.
[309] ibid.
[310] ibid.
[311] ibid.
[312] ibid 278.
[313] D Medine & N D Steimer 'Recent developments in data security and data privacy' (2006) 1 (1) Journal of Payment System Laws 278.

prevent fraud, crime, and deception, undue risk of bodily, financial and emotional harm to consumers.[314]

6.6.23. Secure and Fortify Electronic Data Act of 2011

Secure and Fortify Electronic Data Act (SAFE Data Act) is the Act that is responsible for securing people's data from private intrusion.[315]

6.7. Conclusion

In the USA, the same privacy laws that apply where the goods and or services are supplied physically also apply where goods and or services are exclusively supplied on-line.[316] This means that the sale of services and goods over the internet are treated very much the same as the sale of tangible offline services and goods.[317]

In the USA, the electronic commerce industry as discussed above is now technologically managed and State self-regulated, with very little Federal legislation.[318] Despite the increase in technology mechanisms to manage e-commerce in the USA as well as the increase in legislation, the U.S. Privacy Protection Study Commission in 1977, reported to Congress that:

> "Neither law nor technology now gives an individual the tools he needs to protect his legitimate interests in the records organizations keep about him."[319]

---

[314] ibid.
[315] Davis… et al 'The economics of privacy and data security' (2013) 9 (1) *Journal of Law, Economics & Policy* 465.
[316] Plave 'Franchising: Data protection and e-commerce issues in the United States' (2006) 4 (2) *International Journal of Franchising Law* 15.
[317] ibid 13.
[318] Reidenberg 'Restoring American's privacy in e-commerce' (1999) 17 (1) *Berkeley Technology Law Journal* 787.
[319] ibid.

The USA e-commerce is not raising new data and information privacy concerns, as these have always been there since time immemorial.[320] E-commerce is only increasing the complexity level of the electronic commerce industry between personal information and the commercial goals set by the transacting parties.[321]

On the issue of information trafficking, the USA information policy is still lagging behind despite the fact that it received public attention after the 09 September 2011 bombings (also known as the 9/11 bombings.[322] As the USA technical capabilities are advancing, so is the commercial pressure, enhancing the tracking of the Federal citizens.[323]

[320] J R Reidenberg 'E-commerce and Trans-Atlantic privacy' (2001) 38 (1) *Houston Law Review* 719.
[321] ibid.
[322] ibid.
[323] ibid.

CHAPTER SEVEN

7. CONCLUSION AND RECOMMENDATIONS

As discussed in the earlier chapters, South Africa has a myriad of legislation that deals directly and indirectly with the protection of privacy. This chapter considers the adequacy, satisfactoriness, acceptability, reasonableness and the loopholes of legislation governing electronic transactions and e-commerce in South Africa as well as the improvements that may be made by developing new legislation and or focusing on the effective implementation of existing law.

7.1. Analysis of the Regulatory Context of E-Commerce: Research Questions

Due to the unprecedented movement of the world to information technology, there has been a significant change from an industrial age to an informational age.[1] This dissertation has asked several questions on whether or not the development of information technology in business fits well into the current e-commerce legislation. To answer the crucial questions raised in chapter one of this dissertation, this chapter will seek to:

a) Establish whether there has been legislation designed or put forward by the South African legislature to address information security concerns in e-commerce transactions?
b) To determine to what extend the South African e-commerce legislation impacts on the legislature's endeavour to curb privacy protection problems in e-commerce transactions?
c) To establish how South African organizations and companies are employing policy and legal prescriptions for the purposes of enhancing identifiable private information through information security?

[1] T Almarabeh and A AbuAli 'A general framework for e-government: Definition maturity challenges, opportunities, and success' (2010) 39 (1) *European Journal of Scientific Research* 29.

d) To determine the extend to which companies (both public and private) or organizations (both public and private) in South Africa, are integrating e-commerce privacy protection legal requirements in their policy formulation as well as their policy implementation? and lastly

e) To establish whether there are intermissions in the legislation that have been enacted to address information security problems especially privacy concerns in e-commerce?

7.2. Efforts Made by South Africa in Dealing with Information Protection Issues: Privacy as a Fundamental Human Right and the Challenges Involved

7.2.1. Information Technology Security Policy Formulation

Although South Africa has a considerable amount of legislation that deals with electronic commerce transactions and with the privacy of data and its protection in electronic transactions, it is noteworthy that according to the study discussed at the 8th Annual Information Security South Africa Conference, only a handful of organizations apply the requirements stipulated by legislation in their organizational policy formulation.[2] This means that even if South Africa continues to draft and implement specific legislation on privacy protection in e-commerce, it may not improve the situation any better than it is now since organizations may still choose not to consider the legislation in their information security policy formulation.

7.2.2. Lack of Education

Among other South African statutes dealing with electronic commerce transactions (as discussed in the chapters above) is the ECTA.[3] Even though the ECTA removes legal barriers

[2] R Dagada … et al 'Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant' 1 in *Proceedings of the 8th Annual ISSA Conference*, 6 -8 July 2009, University of Johannesburg's School of Tourism and Hospitality facility, Auckland Park, Johannesburg, South Africa.
[3] Electronic Communications and Transactions Act 25 of 2002.

and also provides security information in electronic transactions for buyers and merchants, a large number of branches of engineering dealing with the use of computer IT security in any organization are not aware of this legislation.[4]

These practitioners and these experts are not familiar with the ECTA and they are unaware of the sections in it dealing with information technology security.[5] This makes it hard for them to even include the information technology security requirements provided by the ECTA and other related legislation when forming organizational information security policies.[6]

7.2.3. Lack of Necessary Expertise

Besides being unaware of information technology legislation dealing with e-commerce transactions and privacy protection, a considerable number of organizations still lack the necessary expertise to actually formulate policies to deal with e-commerce transactions and privacy protection in the workplace.[7] They buy and apply broadly generated information technology security policies of which may be irrelevant to their organization or their customers.[8] The organizations that operate in such a way are best described and characterised as not assiduous, incompetent and uncommitted in executing security mandates given them by the South African e-commerce legislation.[9]

7.2.4. Ambiguous Legislation

The 8th Annual Information Security South Africa Conference also discussed that some of the legislation used in the country to deal with e-commerce are ambiguous.[10] As was also observed in this dissertation, some legislation that is being used to date to deal with privacy

[4] See Note 2 above.
[5] ibid.
[6] ibid.
[7] ibid.
[8] ibid.
[9] ibid.
[10] At 2.

issues in e-commerce is very old and out of date. This is evidenced by the fact that the Copyright Act of 1978[11] and Merchandise Marks Act of 1941[12] are still in use despite the fact that when they were enacted, the internet was not being used for electronic commerce purposes.[13] To avoid this ambiguity, all legislation dealing with electronic transactions should be amended or repealed and replaced by new ones, since the internet is now being used for electronic commerce purposes.

7.2.5. Encryption Laws Not Effective

The capabilities that are provided by encryption in the e-commerce world are vast, especially in securing electronic transmission of personal identifiable information over the internet in transactions conducted between a retailer and a consumer.[14] The capabilities of encryption in South African e-commerce are being realised slowly because there are not many encryption laws as seen in the earlier chapters of this dissertation. Lack of encryption laws affects consumer confidence. In the British and Irish Law Education and Technology Association (BILETA) Annual Conference, it was pointed out that:

> "Fears associated with credit card detail interception over the internet coupled by the anonymity haven that the internet provides to unscrupulous merchants have done much in hampering consumer confidence. To this, the popularity that the existing payment cards have gained over the years, even before the development of electronic commerce along with the success of the card companies in managing to have their product effectively sunk in to common commercial practices have somehow played a deterrent role in simply discarding their use altogether…

[11] Copyright Act 98 of 1978.
[12] Merchandise Marks Act 17 of 1941.
[13] See Note 2 above at 2.
[14] Alexiou 'Enhancing consumer confidence in electronic commerce: Consumer protection in electronic payments' *17th BILETA Annual Conference*, April 5th - 6th, 2002. Free University, Amsterdam 2.

> By the use of public and private key encryption, Secure Socket Layers (SSL) technology has been used effectively in transmitting card payment details effectively and safely over the internet, becoming in this way the norm for secure communication of payment."[15]

7.3. Evaluation of the Success of E-Commerce Legislation: Intermissions in Existing Information Protection legislation

7.3.1. Secure Protocol Loopholes in the Electronic Communications and Transactions Act of 2002

The redundant provisions in the ECTA pose a great challenge. There are quite a few provisions in this piece of legislation, introduced for the purposes of combatting cybercrime by protecting privacy, which have been implemented since being formulated.[16] These provisions are found in chapter 8 of the ECTA and they include issues of hacking, spamming, espionage, viruses and all related cybercrimes that are supposed to be handled by cyber inspectors.[17]

Cryptography as provided by chapter 10 of the ECTA provides for information protection by hiding it through encryption which makes it impossible for an intruder to read such information.[18] This has not been implemented by most organizations dealing with personal identifiable information in e-commerce, rendering the provision useless by this lack of implementation.[19] There has not been a register provision by the director-general of

---

[15] ibid 2 and 3.
[16] B Hamann & S Papadopoulos 'Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa' (2014) 47 (1) *De Jure* 43.
[17] ibid.
[18] J Coetzee 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating electronic commerce' (2004) 15 (3) *Stellenbosch Law Review* 506.
[19] ibid.

communications for cryptography providers to facilitate encryption in organizations involved in e-commerce.[20]

Section 45 of the ECTA dealing with 'unsolicited commercial communications', has serious loopholes as consumers in e-commerce are still receiving unsolicited messages from the sellers of services, goods, and or products.[21] The ECTA provides that the seller of services, goods and or products must provide an option to opt-out and since the consumers ignore the first message, they then continue to receive other messages even though they are still unsolicited.[22]

The definition of 'commercial' found in section 45 of the ECTA is communications that form an offer to contract.[23] Just because a communication does not form an offer to contract, does not mean it is not a commercial communication because in many instances it will contain 'vague commercial features' in it that may render it an unsolicited commercial communication.[24] This shows that according to section 45 of the ECTA, spamming is not altogether illegal as the ECTA regulates rather than prohibits spamming. Spamming encourages the accessing of private personal online identifiable information available through electronic commerce, for the purposes of advertising or committing cybercrime.[25]

[20] ibid.
[21] See Section 45 (1) of the Electronic Communications and Transactions Act 25 of 2002. Hamann & Papadopoulos 'Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa' (2014) 47 (1) *De Jure* 61.
[22] W Jacobs 'The Electronic Communications and Transactions Act: Consumer Protection and internet Contracts' (2004) 16 (4) *SA Mercantile Law Journal* 561.
[23] See Section 45 (1) of the Electronic Communications and Transactions Act 25 of 2002.
[24] See Note 22 above at 561.
[25] ibid.

7.4. Proposed Law Reforms to Improve the Existing Legal Framework

7.4.1. E-commerce Across International Borders

E-commerce takes place, not just in South Africa, but across international borders.[26] E-commerce transactions taking place across international boundaries are difficult to regulate.[27] One of the challenges that emanates from this is the fact that different countries use different ways to regulate electronic commerce transactions between a buyer and a seller of services, goods and or products.[28] Although this might not be an intrinsic factor, the lack of clear regulation dealing with e-commerce taking place across international boundaries fails in creating an environment conducive for cross border online trading.[29] This is because, what may be a crime in one country may not necessarily be a crime in another country.

According to the paper released in December 2003 by the State Law Commission on the 'Privacy and Data Protection':

> "Comprehensive legislation may negatively impact on the ability of South Africa and foreign companies and to receive and send trans-border flow of personally identifiable information thereby weakening cross-border commerce and services between South Africa and its trading partners."[30]

According to the Trans-Pacific Partnership (TPP), trans-boundary e-commerce consumer protection must be incorporated at a global level to avoid it endangering consumer confidence.[31] The organization even encouraged its signatory members to come up with data

[26] United States Trade Representative '2005 National Trade Estimate Report on Foreign Trade Barriers' (2005) 563.
[27] ibid.
[28] ibid.
[29] ibid.
[30] ibid.
[31] H Krogman & N Khumalo 'Discussion Paper on E-commerce in Africa. Definitions, Issues and the Evolving International Regulatory Landscape' (2016) 28.

privacy legislation that is non-discriminatory to promote compatibility between different regimes.[32]

The Trans-Pacific Partnership stated that trans-boundary e-commerce laws will serve this purpose:

> "…adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities."[33]

7.4.2. Is There a Need for More Government Legislation on E-Commerce Transactions?

There is a risk that the e-commerce industry maybe over-regulated, since South Africa has a myriad of legislation already dealing with online business transactions and seem to be passing more legislation.[34] For policy makers, technology is a moving target.[35] Problems emanating from the use of technology in online business transactions must be addressed using flexible but effective technological solutions. The South African e-commerce legislation is out of date with the latest technology being used to do business and is thereby rendered irrelevant to the e-commerce industry.[36] On the other hand, these electronic commerce transactions should not be left to run unguarded by a policy framework.[37]

While some privacy advocates are demanding additional online privacy legislation, it has also been observed through the discussion above that these calls by the privacy advocates have been overstated as more legislation does not always progenerate better online information

[32] ibid 29.
[33] ibid 28.
[34] Alexiou 'Enhancing consumer confidence in electronic commerce: Consumer protection in electronic payments' *17th BILETA Annual Conference*, April 5th - 6th, 2002. Free University, Amsterdam 2.
[35] ibid.
[36] ibid.
[37] ibid.

privacy protection.[38] Other e-commerce sector players are of the view that before jumping to the conclusion that there is a greater need for new consumer protection laws to protect privacy in e-commerce transactions, the legislature should consider other alternatives and maybe give those alternatives a chance.[39] The BILETA Annual Conference also stated that:

> "Enhanced consumer protection legislation would on the one hand foster consumers' confidence in ecommerce, on the other hand however, it might lead to a 'knee-jerk' legislative reaction that would probably inhibit the growth of new technologies and hamper further developments.
>
> The reverse maybe true as well. Lax consumer protection legislation may have the advantage of encouraging e-payment systems' innovation allowing thus the market to develop, however, insufficient consumer protection legislation would inhibit consumers' confidence in new e-payment systems prohibiting thus this new market from reaching a critical mass of acceptance hampering thus the development of e-commerce."[40]

7.4.3. Technology-Neutral Approach

When developing rules or when regulating e-commerce activities, such regulations should not be a hindrance to the use and development of information technology in the future.[41] The technology that is developed for the purposes of dealing with privacy issues in e-commerce transactions should not in any way assume specific technology as e-commerce technology seems to be ever changing.[42]

---

[38] ibid.
[39] ibid.
[40] ibid.
[41] M D Tuba 'The technology-neutral approach and electronic money regulation in the EU: Identifying the promises and challenges for future regulation in South Africa' (2014) 47 (1) *Computer and International Law Journal of South Africa* 382.
[42] ibid.

A technology-neutral approach avoids e-commerce regulations from being outdated, from losing the meaning and authority as soon as they are passed due to the ever-changing technology. [43] The technology-neutral approach avoids discrimination against particular informational technology as the regulations are not specific and are framed based on values and functions.[44] In the USA case of *Diamond v Chakrabarty*, the court pointed out that an e-commerce regulatory framework must be wide-ranging and inclusive of possible technological changes that may take place.[45] The USA court in the same case also mentioned that: "law must encompass anything under the sun made by man"[46]

7.5. The Challenge Facing the South African Legislature: Comparative Legal Analysis

When accessing the efficacy of the various statutes from the three countries under review in this dissertation (that is South Africa, UK and the USA), it is apposite to note that although e-commerce legislation has developed supremely, it still needs to transform to meet the requirements of the ever-changing technology. E-commerce in the three countries mentioned above operates under different domains, as noted in this dissertation.

South African e-commerce laws as they have been discussed in this dissertation take after the UK e-commerce laws. This creates a problem for South Africa since these two countries operate under two different regimes. What works for the UK might not necessarily work for South Africa since UK is a first world country, while South Africa is a second world country.

South Africa however, has constitutional protection of privacy and informational security, unlike the UK and the USA. The UK does not have a Constitution and the USA has no express provision for the protection of privacy in its Constitution. While the USA relies on privacy protection implied in the word 'liberty' as found in its Federal Constitution, South

[43] ibid.
[44] ibid.
[45] *Diamond v Chakrabarty* 447 US 303 (1980) at 309.
[46] ibid.

Africa relies on section 14 of the Constitution of the Republic of South Africa of 1996, which provides for privacy as a fundamental human right as found in the Bill of Rights

This makes it easier for South Africa to cater for the protection of privacy in e-commerce, since information security is regarded as a fundamental human right by its Constitution.

However, although South Africa has privacy provided for as a fundamental human right in its Constitution, at a global level, there is still a lack of a systematic regulation of e-commerce transactions.[47] This makes it very difficult if not impossible for the courts to enforce privacy rights and other rights in e-commerce transactions that are conducted by South Africans with other foreign subjects.[48]

7.6. Summary and Conclusion of Findings: The Way Forward

The world is witnessing a huge revolution and rapid development in the sphere of information and communications technology. Abdulrahman Abdullah Alajaji stated that:

> "At the forefront of that revolution is the internet, which has become indispensable for providing information and communication amongst people throughout the world. It has removed geographical boundaries and even temporal differences, transforming the world into a small village as one of the main features of the era of globalisation.
>
> E-commerce is still a new phenomenon that is attracting increasing attention from many countries, which is likely to continue growing as numbers of those with access to the internet rise. As e-commerce becomes increasingly internationalised, the need to produce new well-drafted

[47] Krogman & Khumalo 'Discussion Paper on E-commerce in Africa. Definitions, Issues and the Evolving International Regulatory Landscape' (2016) 27.
[48] ibid.

> legislation governing online transactions becomes an issue of global significance.
>
> Constant advances in information and communications technology will continue to provoke international debate and discussion regarding the rules and principles that should govern the virtual world of e-commerce, challenging many aspects of existing legislation in areas such as contractual law. The emerging field of e-commerce law will need to receive increasing attention in order to maintain consumer confidence and minimise the existence of legal loopholes."[49]

7.6.1. Recommendation One: Policy Formulation by Information Technology Security Organizations

I recommend that the government should design some mechanisms to coerce IT security organizations to formulate policies that are designed to implement the requirements of legislation dealing with informational privacy protection in electronic commerce transactions. Legislation created by the South African government must address all the technological changes that have taken place over the years in e-business. The same legislation must also cater for the ever-changing electronic means of doing business. Legislation must also seek to address cross border online trading.

7.6.2. Recommendation Two: Self-regulated Industry

I recommend that the South African legislature introduce, like in the USA, technology such as the Platform for Privacy Preferences Project. The Platform for Privacy Preferences Project in the USA is an industry-led effort that enables particular websites to give e-commerce

[49] A A Alajaji 'An Evaluation of E-Commerce Legislation in GCC States: Lessons and Principles from the International Best Practices' (unpublished LLD dissertation, Lancaster University, 2016) 14, 18 and 19.

customers their privacy practices in machine readable standardised format, which can be retrieved and interpreted by a consumer's computer automatically.[50] If the site's policy that is found on that particular website is not in line with what the consumer wishes, a warning is issued automatically and the consumer is warned and can decide on whether to visit the site or not.[51]

Again, as shown by the American 1998 annual Federal Trade Commission (FTC) studies, self-regulation through privacy policies was evident in 14% of all the commercial websites which had a privacy notice or a privacy statement.[52] The percentage rose from 14% in 1998 to 66% in 1999 and ultimately to 88% in 2000.[53] Self-regulation-plus-administration-pressure approach led to this increase as well as to internet privacy technology innovations.[54]

7.6.3. Recommendation Three: Coded E-Commerce Legislation

I also recommend that the South African government introduce coded legislation to deal only with e-commerce matters in order to avoid over-regulating the industry instead of the scattered system of threat-and-industry-specific privacy protection. This will also enable information technology security practitioners and experts to find it easy to incorporate the requirements of these legislation when making organizational IT policies.

The South African government must not just write e-commerce policy objectives into legislation, but must also ensure the legal framework so enacted is providing adequate incentives. This requires the government not only pass e-commerce regulations but also to supervise the implementation of such. It should ensure that the existing e-commerce laws and

[50] R W Hahn & A Layne-Farrar 'Is more government regulation needed to promote e-commerce?' (2002) 35 (1) *Connecticut Law Review* 201.
[51] J R Reidenberg 'Restoring American's privacy in e-commerce' (1999) 17 (1) *Berkeley Technology Law Journal* 787.
[52] P P Swire 'Trustwrap: The importance of legal rules to electronic commerce and internet privacy' (2003) 54 (1) *Hastings Law Journal* 863.
[53] ibid 863 and 864.
[54] Ibid 864.

industry practices are followed. There must be a balance between the very need to combat crime through transaction reporting of consumer identification and the consumer's right of privacy and data protection.

7.6.4. Recommendation Four: Extra Privacy Protection Mechanisms

The government can also come up with measures to strengthen its monitoring systems to ensure compliance with the rules/laws enacted to deal with privacy protection, especially in electronic commerce transactions.

7.6.5. Recommendation Four: Creating Awareness

This dissertation would not be complete, if it did not address the issue of awareness. Finally, I recommend that the South African government devise more ways to enhance their awareness campaigns. In addition to the legislation that has been implemented, those that are yet to be implemented and those that will need to be amended to address privacy concerns in e-commerce in South Africa, should be communicated to the general public who should also be educated on how to handle their private online personal identifiable information when doing online doing online transactions.

BIBLIOGRAPHY

BOOKS

1. Aldermann, E & Kennedy, C *The Right to Privacy* New York: Random House (1997).
2. Buys, R & Cronje, F (eds) *Cyberlaw @ SA II: The Law of the Internet in South Africa* 2 ed Pretoria: Van Schaik (2004).
3. Chaffey, D *E-Business and E-commerce Management: Strategy, Implementation and Practice* 4 ed New York: Financial Times Prentice Hall (2009).
4. Chakrabarti, R *The Asian Manager's Handbook of E-commerce* New Delhi: Tata McGraw-Hill Publishing Company Limited (2002).
5. Classen, L 'E-commerce and value added tax' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed Pretoria: Van Schaik (2012).
6. Cupido, C 'Electronic Communications regulation' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed Pretoria: Van Schaik (2012).
7. Currie, I & De Waal, J *The Bill of Rights Handbook* 5 ed Cape Town: Juta (2005).
8. De Waal, J & Currie, I *The Bill of Rights Handbook* Kenwyn: Juta (1998).
9. Dickie, J *Internet and Electronic Commerce Law in the European Union* Oxford: Hart Publishing (1999).
10. Fitzgerald, B. … et al. *Internet and E-commerce Law: Technology, Law and Policy* Sydney: Lawbook Co. (2007).

11. Goodburn, D & Ngoye, M 2004: 'Privacy and the internet' in R Buys & F Cronje (eds) *Cyberlaw: The Law of the Internet in South Africa* 3 ed Pretoria: Van Schaik (2004).

12. Grayling, A C *Liberty in the Age of Terror: A Defence of Civil Liberties and Enlightenment Values* Michigan: Bloomsbury (2009).

13. Grist, S 'The definition dilemma of e-commerce' in S A Becker (ed) *Electronic Commerce: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications* New York: Information Science Reference (2008).

14. Jay, R *Data Protection Law and Practice* 3 ed London: Sweet & Maxwell (2007).

15. Kalakota, R & Whinston, A *Electronic Commerce a Manager's Guide* 3 ed New York: Addison-Wesley Professional (1997).

16. Lee, K and Light, J 'Law and regulation, Part 1: Individual interests' in Shyles L (ed) *Deciphering Cyberspace: Making the Most of Digital Communication Technology* Thousand Oaks, California: Sage Publications (2003).

17. Lloyd, I *Information Technology Law* 5 ed New York: Oxford University Press, (2008).

18. Lloyd, I J *Information Technology* Law 7 ed London: Oxford University Press (2014).

19. Malecki, E J & Moriset, B *The Digital Economy: Business Organization, Production Processes and Regional Developments* London: Routledge (2007).

20. Manzoor, A *E-Commerce: An Introduction* Saarbrücken: LAP Lambert Academic Publishing (2010).

21. Marcella, A J and Stucki, C *Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues* Toronto: John Wiley & Sons Inc. (2003).

22. Morgan, R and Boardman, R *Data Protection Strategy: Implementing Data Protection Compliance* 2 ed London: Sweet & Maxwell (2012).

23. Neethling, J. … et al. *Neethling's Law of Personality* 2 ed Durban: LexisNexis (2005).

24. Nel, S 'Freedom of expression, anonymity and the internet' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed Pretoria: Van Schaik (2012).

25. OECD *Measuring the Information Economy* Berlin: OECD Publications (2002).

26. OECD *OECD Glossary of Statistical Terms* Berlin: OECD Publications (2008).

27. OECD *OECD Guide to Measuring the Information Society 2011* Berlin: OECD Publications (2011).

28. Papadopoulos, S 'An introduction to cyberlaw' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed Pretoria: Van Schaik (2012).

29. Papadopoulos, S 'Online consumer protection' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed Pretoria: Van Schaik (2012).

30. Qin, Z … et al. *E-Commerce Strategy* 2 ed Hangzhou: Zhejiang University Press (2014).

31. Qin, Z *Introduction to E-commerce* Beijing: Springer Science & Business Media (2010).

32. Riordan, J *The Liability of Internet Intermediaries* New York: Oxford University Press (2016).

33. Robinson, B E *Financial Privacy & Electronic Commerce: Who's in My Business* New York: Writers Club Press (2000).

34. Schniederjans, M J. … et al. *E-Commerce Operations Management* 2 ed Singapore: World Scientific Publishing (2013).

35. Shim, J. … et al. *The International Handbook of Electronic Commerce* 3 ed New York: Routledge (2000).

36. Smith, G J H *Internet Law and Regulation* 4 ed London: Sweet & Maxwell (2007).

37. Smith, R G. … et al. *Cybercriminal on Trial* Cambridge: Cambridge University Press (2004).

38. Snail S & Papadopoulos S 'Privacy and data protection' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed Pretoria: Van Schaik (2012).

39. Snail, S & Papadopoulos S 'Privacy and data protection' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed Pretoria: Van Schaik (2012).

40. Snail, S 'Electronic contracting in South Africa (e-contracts)' in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III: The Law of the Internet in South Africa* 3 ed Pretoria: Van Schaik (2012).

41. Sparrow, A *The Law of Virtual Worlds and Internet Social Networks* Surrey: Gower Publishing Limited (2010).

42. Stewart, M *Encyclopaedia of Developing Regional Communities with Information and Communication Technology* New York: Information Science Reference (2005).

43. United Nations *'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998'* New York: United Nations Publications (1999).

44. Van der Merwe, D P *Information and Communications Technology Law* Durban: LexisNexis (2008).

45. Wang, F F *Law of Electronic Commercial Transactions – Contemporary Issues in the EU, US and China* London: Routledge (2010).

JOURNAL AND NEWSPAPER ARTICLES

1. Abhilash, C M 'E-commerce law in developing countries: An Indian perspective' (2002) 11 (3) *Information & Communication Technology Law* 200-270.

2. Alhorr, H S. …et al 'E-commerce on the global platform: Strategic insights on the localization-standardization perspective' (2010) 11 (1) *Journal of Electronic Commerce Research* 1-10.

3. Allen, A L 'Associational privacy and the First Amendment: NAACP v Alabama, privacy and data protection' (2011) 1 (1) *Alabama Civil Rights & Civil Liberties Law Review* 1-13.

4. Allison, S 'The concept of "Personal Data" under the data protection regime' (2009) 48 (1) *Edinburgh Student Law Review* 48-65.

5. Almarabeh T and AbuAli A 'A general framework for e-government: Definition maturity challenges, opportunities, and success' (2010) 39 (1) *European Journal of Scientific Research* 29-42.

6. Ananthapur, R 'India's new data protection legislation' (2011) 8 (2) *Script-ed Journal* 193-203.

7. Balz, S D & Hance, O 'Privacy and the internet: Intrusion, surveillance and personal data' (1996) 10 (2) *International Review of Law Computers & Technology* 219-234.

8. Banisar, D & Davies, S 'Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments' (199) 18 (1) *Journal of Computer and Information Law* 1-112.

9. Bergerson, S R 'E-commerce privacy and the black hole of cyberspace' (2001) 27 (3) *William Mitchell Law Review* 1527-1555.

10. Beyleveld, D 'Data protection and genetics: Medical research and the public good' (2007) 18 (1) *King's Law Journal* 276-289.

11. Bharwaney, M and Marwah, A 'Personal data privacy in the digital age' (2013) 43 (3) *Hong Kong Law Journal* 801-834.

12. Border, A C 'Untangling the web' (2012) 35 (2) *Suffolk Transnational Law Review* 363-392.

13. Burchell, J 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* 1-26.

14. Cardonsky, L B 'Towards a meaningful right to privacy in the United Kingdom' (2002) 20 (2) *Boston University International Law Journal* 393-412.

15. Cassim, F 'Formulating specialised legislation to address the growing spectre of Cybercrime: A comparative study' (2009) 12 (4) *Potchefstroom Electronic Law Journal* 36-79.

16. Charlesworth, A 'Legislating against computer misuse: The trials and tribulations of the UK Computer Misuse Act 1990' (1993) 4 (1) *Journal of Law and Information Science* 80-93.

17. Chong, H 'Validity of Delone and Mclean's e-commerce model in B2C student loan industry' (2010) 19 (1) *Journal of International Technology and Information Management* 60-100.

18. Chong, W K & Suling, J C 'United Nations convention on the use of electronic communications in international contracts: A new global standard' (2006) 18 (1) *Singapore Academy of Law Journal* 116-202.

19. Coetzee, J 'The Electronic Communications and Transactions Act 25 of 2002: facilitating electronic commerce' (2004) 15 (3) *Stellenbosch Law Review* 501-521.

20. Collins, V 'Privacy in the United Kingdom: A right conferred by Europe?' (1994) 1 (3) *International Journal of Law and Information Technology* 290-304.

21. Corbitt, B J. …et al 'Trust and e-commerce: a study of consumer perceptions' (2003) 2 (1) *Electronic Commerce Research and Application* 203-215.

22. Davis, A H … et al 'The economics of privacy and data security' (2013) 9 (1) *Journal of Law, Economics & Policy* 461-487.

23. Dimond, B 'Rights to information access under the Data Protection Act' (2005) 14 (14) *British Journal of Nursing* 774-776.

24. Din, N M & Jamaluddin, M Z 'Building a trusted environment for e-business: Malaysian perspective' (2003) 1 (1) *Journal of ICT* 33-44.

25. Dunkel, Y F 'Medical privacy rights in anonymous data: Discussion of rights in the United Kingdom and the United States in light of the source informatics cases' (2001) 23 (41) *The Loyola of Los Angeles International and Comparative Law Review* 41-79.

26. Eiselen, S 'Fiddling with the ECT Act - electronic signatures' (2014) 17 (6) *Potchefstroom Electronic Law Journal* 2805-2820.

27. Eleftheriou, D … et al 'Data protection and e-commerce in the United States and the European Union' (2006) 40 (2) *The International Lawyer* 393-402.

28. Esselaar, P and Miller, J 'Towards electronic commerce in Africa: A perspective from three country studies' (2002) 2 (1) *The Southern African Journal of Information and Communication* 1-10.

29. Fafinski, S ‘Access denied: Computer misuse in an era of technological change’ (2006) 70 (1) *The Journal of Criminal Law* 424-442.

30. Faria, J A E ‘E-commerce and international legal harmonization: Time to go beyond functional equivalence?’ (2004) 16 (1) *SA Mercantile Law Journal* 529-555.

31. Flaherty, D H ‘On the utility of constitutional rights to privacy and data protection’ (1991) 41 (1) *Case Western Reserve Law Review* 831-855.

32. Flaherty, S ‘Surveillance societies’ (1992) 2 (1) *Hastings Law Journal* 1334-1343.

33. Francois, L R ‘E-commerce: the legal framework’ (2000) 1 (1) *De Rebus* 1-30.

34. Gangeshwer, D K ‘E-Commerce or internet marketing: A business review from Indian context’ (2013) 6 (6) *International Journal of u- and e- Service, Science and Technology* 187-194.

35. Geist, M 'When dot-coms die: The e-commerce challenge to Canada's bankruptcy law' (2002) 37 (1) *Canadian Business Law Journal* 1-50.

36. Glatt, C ‘Comparative issues in the formation of electronic contracts’ (1998) 1 (1) *International Journal of Law and Information Technology* 34-68.

37. Guo, M ‘A Comparative study on consumer right to privacy in e-commerce’ (2012) 3 (1) *Modern Economy* 402-407.

38. Haenggi, S ‘The right to privacy is coming to the United Kingdom: Balancing the individual's right to privacy from the press and the media's right to freedom of expression’ (1999) 531 (1) *Journal of International Law* 531-579.

39. Hahn R W & Layne-Farrar A ‘Is more government regulation needed to promote e-commerce?’ (2002) 35 (1) *Connecticut Law Review* 195-213.

40. Hamann, B & Papadopoulos, S 'Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa' (2014) 47 (1) *De Jure* 42-62.

41. Henschel, R F & Cleff, E B 'Information requirements and consumer protection in future m-commerce: Textual information overload or alternative regulation and communication?' (2007) 1 (1) *International Journal of Intercultural Information Management* 58-73.

42. Ho, B C & Oh, K B 'An empirical study of the use of e- security seals in e-commerce' (2009) 33 (4) *Online Information Review* 655-671.

43. Hofman, J 'The moving finger: Sms, on-line communication and on-line disinhibition' (2011) 8 (1) *Digital Evidence and Electronic Signature Law Review* 179-183.

44. Iannotta, M W 'Protecting individual privacy in the shadow of a national data base: The need for data protection legislation' (1989) 17 (1) *Capital University Law Review* 117-141.

45. Jacobs, W 'The Electronic Communications and Transactions Act: Consumer *Protection and Internet Contracts'* (2004) 16 (1) *SA Mercantile Law Journal* 556-567.

46. Jansen, J 'A new era for e-commerce in South Africa' (2002) 416 *De Rebus* 16-21.

47. Jobodwana, Z N 'E-commerce and mobile commerce in South Africa: Regulatory challenges' (2009) 4 (4) *Journal of International Commercial Law and Technology* 287-298.

48. Kosta, E 'Construing the meaning of "Opt-Out"- An analysis of the European, U.K. and German data Protection legislation' (2015) 1 (1) *European Data Protection Law* 16-31.

49. Le Roux, F 'E-commerce: The legal framework' (2000) 392 *De Rebus* 25-28.

50. Lightner, N J 'What users want in e-commerce design: Effects of age, education and income' (2003) 46 (1) *Ergonomics* 153-168.

51. Lorber, S 'Data protection and subject access requests' (2004) 179 (1) *International Law Journal* 179-190.

52. Mann, J 'Privacy at work in the United Kingdom' (2002) 1 (1) *International Business Lawyer* 150-154.

53. McDougall, C 'An introduction to the Data Protection Act 1998 and the Freedom of Information Act 2000: Part I' (2002) 7 (1) *Judicial Review* 199-205.

54. Medine, D & Steimer, N D 'Recent revelopments in data security and data privacy' (2006) 1 (1) *Journal of Payment System Laws* 263-280.

55. Mitton, A 'Data protection and web 2.0: Whose data is it anyway?' (2007) 3 (1) *Convergence* 94-98.

56. Mtuze, S L S & Matanzima, S 'Without prejudice - cyber security in Africa: Cyber law.' (2014) 14 (9) *Electronic Journal of Commerce* 88-89.

57. Nemat, R 'Taking a look at different types of e-commerce' (2011) 1 (2) *World Applied Programming Journal* 100-104.

58. Olinger, H N. … et al 'Western privacy and/or ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007) 39 (1) *The International Information & Library Review* 31-43.

59. O'Reilly, K 'South African law coming to grips with cyber-crime: News' (2013) 530 *De Rebus* 14-15.

60. Pistorius, T 'Contract formation: A comparative study of legislative initiatives on select aspects of electronic commerce' (2002) 25 (1) *Comparative & International Law of South Africa* 100-200.

61. Pistorius, T 'Formation of internet contracts: Contractual and security issues' (1999) 11 (1) *SA Mercantile Law Journal* 270-300.

62. Pitiyasak, S 'Electronic contracts: Contract law of Thailand, England and UNCITRAL compared' (2003) 9 (1) *Computer and Telecommunications Law Review* 16-30.

63. Plave, L 'Franchising: Data protection and e-commerce issues in the United States' (2006) 4 (2) *International Journal of Franchising Law* 3-26.

64. Prinsloo, I J 'How safe are South African schools?' (2005) 25 (1) *South African Journal of Education* 5-10.

65. Reid, P ''Regulating' Online data privacy' (2004) 2 (3) *Script-ed Journal* 489-504.

66. Reidenberg, J R 'E-commerce and Trans-Atlantic privacy' (2001) 38 (1) *Houston Law Review* 717-749.

67. Reidenberg, J R 'Restoring American's privacy in e-commerce' (1999) 17 (1) *Berkeley Technology Law Journal* 771-792.

68. Roos, A 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2008) 11 (4) *South African Law Journal* 400-436.

69. Rothchild, J 'Protecting the digital consumer: The limits of cyberspace utopianism' (1999) 74 *Indiana Law Journal* 893-989.

70. Rotman, L I 'The fiduciary regulation of e-commerce' (2004) 29 (1) *Queen's Law Journal* 739-788.

71. Satapathy, C 'Legal framework for e-commerce' (1998) 33 (29) *Economic and Political Weekly Journal* 1906-1907.

72. Schulze, C 'Electronic commerce and civil jurisdiction, with special reference to consumer contracts' (2006) 18 (1) *SA Mercantile Law Journal* 31-44.

73. Shahriari, S. ... et al 'E-commerce and it impacts on global trend and market' (2015) 3 (4) *International Journal of Research - Granthaalayah* 49-55.

74. Shumba, T 'Towards an SADC community sales law: Lessons SADC may learn from the proposal for a Common European Sales Law (CESL)' (2015) 27 (3) *SA Mercantile Law Journal* 383-588.

75. Snail, S 'Cyber crime in South Africa - Hacking, cracking, and other unlawful online activities' (2009) 1 *Journal of Information, Law & Technology* 1-13.

76. Snail, S 'Electronic contracts in South Africa - A comparative analysis' (2008) 2 (1) *Journal of Information, Law & Technology* 1-24.

77. Snail, S L 'An overview of South African e-consumer law in the context of the Electronic Communications and Transactions Act (part 2)' (2007) 15 (1) *Juta's Business Law* 54-59.

78. Snail, S L 'South African e-consumer law in the context of the ECT Act (part 1)' (2007) 15 (1) *The Quarterly Law Review for People in Business* 40-46.

79. Sohn, K H 'Privacy and security protection under Korean E-Commerce law and proposals for its improvements' (2016) 33 (1) *Arizona Journal of International & Comparative Law* 229-248.

80. Solzhenitsyn, A & Ward, C 'The Privacy Act of 1974: An overview and critique' (1976) 4 *Washington University Law Review* 667-718.

81. Sorieul, R … et al 'Establishing a legal framework for electronic commerce: The work of the United Nations Commission on International Trade Law (UNCITRAL)' (2001) 35 (1) *The International Lawyer* 107-122.

82. Spratt, J 'An economic argument for electronic privacy' (2011) 6 (3) *I/S: A Journal of Law and Policy for the Information Society* 513-554.

83. Stoop, P 'SMS and e-mail contracts: Jafta v Ezemvelo KZN Wildlife' (2009) 21 (1) *SA Mercantile Law Jpournal* 1-144.

84. Suh B & Han I 'The impact of customer trust and perception of security control on the acceptance of electronic commerce' (2003) 7 (3) *International Journal of Electronic Commerce* 135-161.

85. Sun, T 'The roles of trust and experience in consumer confidence in conducting e-commerce: a cross-cultural comparison between France and Germany' (2011) 35 (3) *International Journal of Consumer Studies* 330-337.

86. Swales, L 'Protection of personal information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' (2016) 28 (1) *SA Mercantile Law Journal* 49-84.

87. Swire, P P 'Trustwrap: The importance of legal rules to electronic commerce and internet privacy' (2003) 54 (1) *Hastings Law Journal* 847-873.

88. Taylor, E 'UK schools, CCTV and the Data Protection Act 1998' (2011) 26 (1) *Journal of Education Policy* 1-15.

89. Tuba, M D 'The technology-neutral approach and electronic money regulation in the EU: Identifying the promises and challenges for future regulation in South Africa' (2014) 47 (1) *Computer and International Law Journal of South Africa* 372-400.

90. Turn, R 'Privacy Protection and Security in Transnational Data Processing Systems' (1980) 16 (1) *Stanford Journal of International Law* 67-86.

91. Turner, M … et al 'E-commerce Directive - UK implementation. Electronic Commerce (EC Directive) Regulations 2002 - Worth the wait?' (2002) 18 (6) *Computer Law & Security Report* 396-403.

92. Ulrich, C 'Consumer protection in e-commerce: Germany and the United States' (2000) 4 (5) *Journal of Internet* 1-22.

93. Van Zyl, S P 'Determining the place of supply or the place of use and consumption of imported services for value-added tax purposes: Some lessons for South Africa from the European Union' (2013) 25 (4) *SA Mercantile Law Journal* 534-554.

94. Wade, A E 'A new age of privacy protection: A proposal for an international personal data privacy treaty' (2010) 42 (1) *The George Washington International Law Review* 659-685.

95. Walden, I 'Anonymising personal data' (2002) 10 (2) *International Journal of aw and Information Technology* 224-237.

96. Wang, M 'Review of the signature regulations: Do they facilitate or impede intentional electronic commerce?' (2006) 14 (1) *Association for Computing Machinery* 548-552.

97. Warren, S D & Brandeis, L D 'The right to privacy' (1890) 4 (5) *Harvard Law Review* 193-220.

98. Wijnhoven, F 'The importance of information goods abstraction levels for information commerce process models' (2002) 3 (2) *Journal of Electronic Commerce Research* 40-49.

99. Wilkinson, T 'Is anyone listening to me? Bartnicki v Vopper' (2003) 63 (2) *Louisiana Law Review* 589-607.

100. Woolman, S 'Coetzee: The limitations of Justice Sach's concurrence' (1996) 12 (1) *South African Journal on Human Rights* 99-124.

101. Worku, G 'Electronic-banking in Ethiopia - practices, opportunities and challenges' (2003) 1 (2) *Journal of Internet Banking and Commerce* 1-15.

LAW COMMISSION PAPERS, CONFERENCE PAPERS and OTHERS

1. Computers and Privacy, White Paper Cmnd 6353, (HMSO: London 1975).
2. Computers: Safeguards for Privacy Cmnd 6354, (HMSO: London 1975).
3. Kontogeorgou, P & Alexiou, M G 'Enhancing Consumer Confidence in Electronic Commerce: Consumer Protection in Electronic Payments' *17th BILETA Annual Conference*, April 5th - 6th, 2002. Free University: Amsterdam, (2002).
4. Krogman, H & Khumalo, N: Discussion Paper on E-commerce in Africa. Definitions, Issues and the Evolving International Regulatory Landscape: Global Economic Governance (GEG) Africa, (2016).
5. Report of the Committee on Data Protection Cmnd 7341, (HMSO: London 1978).
6. South Africa Department of Communications 'A Green Paper on Electronic Commerce for South Africa' Government Printer, (2000).
7. South Africa Department of Communications 'Discussion Paper on Electronic Commerce' Government Printer, (1999).
8. South African Law Reform Commission Privacy and Data Protection (Project 124 Discussion Paper 109), Pretoria: SALRC (2005).
9. The South African Law Reform Commission: Privacy and Protection (Discussion paper 109/2015, Project 124) Pretoria: SALRC (2006).
10. Victorian Law Reform Commission Discussion Paper: Privacy Law: Options For Reform (Discussion paper 1/2001, Project 1), (2001).

THESES

1. Aladwan, A A ‘Cyber-Consumer protection framework for prevention of online deceptive advertising’ (unpublished LLM thesis, Curtin University, 2012).

2. Alajaji, A A ‘An evaluation of e-commerce legislation in GCC states: Lessons and principles from the international best practices’ (unpublished LLD dissertation, Lancaster University, 2016).

3. Cleff, E ‘Mobile advertising: A comparative regulatory overview’ (unpublished LLM thesis, Arhus School of Business, 2005).

4. Huffmann, J ‘Consumer protection in e-commerce: An examination and comparison of the regulations in the European Union, Germany and South Africa that have to be met in order to run internet services and in particular online-shops’ (unpublished LLM thesis, University of Cape Town, 2004).

5. Laosebikan, F O ‘Privacy and technological development: A comparative analysis of South African and Nigerian privacy and data protection laws with particular reference to the protection of privacy and data in internet cafes and suggestions for appropriate legislation in Nigeria’ (unpublished LLD dissertation, University of KwaZulu-Natal, 2007).

6. Mtuze, S L S ‘A comparative review of legislative reform of electronic contract formation in South Africa’ (unpublished LLM thesis, University of South Africa, 2015).

7. Nagalingam, S G ‘The enforceability of computer contracts’ (unpublished LLB thesis, University of Pretoria, 2000).

8. Pluckhahn, P '(E-commerce) data protection in the European Union and South Africa. A comparative study' (unpublished LLM thesis, Aarhus University, 2010).

9. Roos, A 'The law of data (privacy) protection: A comparative and theoretical study' (unpublished LLD dissertation, University of South Africa, 2003).

INTERNET ARTICLES

1. 'A Guide For Business to the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013) 31 July' at 4 available at http://webarchive.nationalarchives.gov.uk/20121212135622/http:/www.bis.gov.uk/files/file14635.pdf, accessed on 28 June 2017.

2. 'A Guide to UNCITRAL Basic facts about the United Nations Commission on International Trade Law' (2013) at 1 available at http://www.uncitral.org/pdf/english/texts/general/12-57491-Guide-to-UNCITRAL-e.pdf, accessed on 03 February 2017.

3. 'CLOUT case 1230 – UNCITRAL' available at https://www.uncitral.org/clout/clout/data/zaf/clout_case_1230_leg-2892.html, accessed on 06 February 2017.

4. 'The UK's E-Commerce Regulations' available at https://www.out-law.com/page-431, accessed on 27 June 2017.

5. 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998' available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html, accessed on 03 February 2017.

6. 'UNCITRAL Model Law on Electronic Commerce' United Nations Commission on International Trade Law available at http://www.uncitral.org/uncitral/en/commission/sessions/29th.html, accessed on 19 January 2017.

7. 'UNCITRAL model Law on Electronic Signatures' United Nations Commission on International Trade Law available at http://www.uncitral.org/uncitral/en/commission/sessions/29th.html, accessed on 30 January 2017.

8. 'UNICITRAL Model Law on Electronic Signatures' United Nations Commission on International Trade Law available at http://www.uncitral.org/uncitral/en/commission/sessions/29th.html, accessed on 19 January 2017.

9. 'What is the OECD?' About the OECD available at https://usoecd.usmission.gov/mission/overview.html, accessed on 28 December 2016.

10. "TRUSTe Oversight" available at http://www.truste.com, accessed on 16 February 2017.

11. Commissioner's Office (UK) 'Direct Marketing' available at https://ico.org.uk/media/fororganizations/documents/1555/direct-marketing-guidance.pdf, accessed on 25 July 2017.

12. Dagada, R. …et al 'Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant?' available at http://uir.unisa.ac.za/handle/10500/2660, accessed on 17 February 2017.

13. Deloitte & Touche Legal 'Electronic Communications & Transaction Bill 2002. (South Africa)' (2002), available at http://www.doc.pwv.gov.za/, accessed on 20 December 2016.

14. Deloitte & Touche Legal 'Electronic Communications & Transaction Bill 2002. (South Africa)' (2002), available at http://www.doc.pwv.gov.za/, accessed on 13 February 2017.

15. Federal Trade Commission 'Privacy Online: A Report to Congress' June 1998 available at https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf, accessed on 31 July 2017.

16. UNCITRAL Conventions available at http://www.uncitral.org/uncitral/en/uncitral-texts/electronic-commerce/2005Convention.html, accessed on 06 February 2017.

17. UNCITRL 'About UNCITRAL' available at www.uncitral.org/ uncitral/ en/about_us.html, accessed on 30 January 2017.

18. Zantsi, N & Eloff, M 'Guide to South African law' (2003), available at http://icsa.cs.up.ac.za/issa/2003/Publications/001.doc/, accessed on 13 February 2017.

19. Zantsi, N & Eloff, M 'Guide to South African law' (2003), available at http://icsa.cs.up.ac.za/issa/2003/Publications/001.doc/, accessed on 20 December 2016.

TABLE OF CASES

SOUTH AFRICA

1. *Bernstein v Bester* 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC).
2. *Boerne v Harris* 1949 (1) SA 793 (A).
3. *Comair Ltd v Minister for Public Enterprises* 2014 (5) SA 608 (GP).
4. *Esterhuizen v Administrator, Transvaal* 1957 (3) SA 710 (T).
5. *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A).
6. *Harksen v Lane* 1998 (1) SA 300 (CC).
7. *Helen Suzman Foundation v Judicial Service Commission* 2017 (1) SA 367 (SCA).
8. *Heroldt v Wills* 2013 (2) SA 530 (GSJ).
9. *Hyundai Motor Distributors (Pty) Ltd v Smit* 2001 (1) SA 545 (CC).
10. *In re: Certification of the Constitution of the Republic of South Africa* 1996, 1996 (10) BCLR 1253 (CC).
11. *Jafta v Ezemvelo KZN Wildlife* (2009) 30 ILJ 131 (LC).
12. *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 (4) SA 293 (A).
13. *Jooste v National Media Ltd* 1994 (2) SA 634 (C).
14. *Khumalo & v Holomisa* 2002 (8) BCLR 771; 2002 (5) SA 401 (CC).
15. *Lampert v Hefer* 1955 (2) SA 507 (A).
16. *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC).
17. *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 (CC).
18. *National Media Ltd ao v Jooste* 1994 (2) SA 634 (C).
19. *National Media Ltd v Jooste* 1996 (3) SA 262 (A).
20. *National Media Ltd. v Bogoshi* 1998 (4) SA 1196 (SCA).

21. *NM v Smith (Freedom of Expression Institute as Amicus Curiae)* 2007 (7) BCLR 751 (CC).
22. *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 (2) SA 244 (C).
23. *Phoenix Shipping Corporation v DHL Global Forwarding SA (Pty) Ltd* (AC70/2011) [2012] ZAWCHC 11; 2012 (3) SA 381 (WCC) (24 February 2012).
24. *S v Bailey* 1981 (4) SA 187 (N).
25. *S v Hammer* 1994 (2) SACR 496 (C).
26. *S v Harper* 1981 (2) SA 638 (D).
27. *S v Howard* (unreported Case no. 41/ 258 / 02, Johannesburg regional magistrate's court).
28. *S v Makwanyane* 1995 (3) SA 391 (CC); 1995 BCLR 665 (CC).
29. *S v Manuel* 1953 (4) SA 523 (A).
30. *S v Van den Berg* 1991 (1) SACR 104 (T).
31. *Sihlali v South African Broadcasting Corporation Ltd* (J700/08) [2010] ZALC 1; (2010) 31 ILJ 1477 (LC); [2010] 5 BLLR 542 (LC) (14 January 2010).
32. *Spring Forest Trading CC v Wilberry (Pty) Ltd t/a Ecowash* 2015 (2) SA 118 (SCA).
33. *Spring Forest Trading v Wilberry* [2014] ZASCA 178; 2015 (2) SA 118 (SCA), 725/13.
34. *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 (4) SA 549 (T).
35. *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T).
36. *Lymbery v Jefferies* 1925 AD 236.
37. *Stoffberg v Elliot* 1923 CPD 148.

UNITED KINGDOM

1. *A v B 1 All ER* 449 (QB 2001).
2. *Argyll v Argyll* [1965] 2 W.L.R. 790 (Chancery Div.).

3. *Attorney General v Guardian Newspapers* (No2) [1990] 1 AC 109.

4. *Attorney General v Guardian Newspapers Ltd.* No. 2, 1 A.C. 109 (H.L. 1990).

5. *Campbell v Mirror Group Newspapers Ltd* [2004] 2 All ER 995 (HL).

6. *Christie v United Kingdom* (1994) 7S-A DR 119.

7. *Douglas v Hello! Ltd* [2001] Q.B. 967, 997 (Eng. C.A.).

8. *Francome v Mirror Group Newspapers Ltd* [1984] 1 WLR 892.

9. *Golder v United Kingdom* (1975) 1 EHRR 524.

10. *Halford v United Kingdom* [1997] IRLR 471.

11. *Hunter v Mann* [1974] 1 QB 767.

12. *Kaye v Robertson* [1991] FSR 62.

13. *Lord Ashburton v Pape* [1913] 2 Ch 469.

14. *Malone v Metropolitan Police Commissioner* (No2) [1979] 2 All ER 620.

15. *Michael John Durant v Financial Services Authority* [2003] EWCA Civ 1746; [2004] FSR 28.

16. *Morison v Moat* [1851] 9 Hare 241.

17. *Murray v Big Pictures (UK) Ltd* [2008] EWCA.

18. *Prince Jefri Bolkiah v KPMG* [1999] 1 All ER 577.

19. *R v Dep't of Health ex parte Source Informatics Ltd., 1 All E.R.* 786, (C.A. 2000), rev'g 4 All E.R. 185 (Q.B. 1999).

20. *Regina v Gold & Schifreen* [1988] 2 All ER 186 (HL).

21. *Saltman Engineering v Campbell Engineering* [1948] 65 RPC 203.

22. *Terrapin v Builders' Supply Co (Hayes) Ltd* [1967] RPC 375.

23. *Thomas Marshall (Exporters) Ltd v Guinle* [1978] 3 WLR 116.

24. *Tolley v J.S. Fry & Sons Ltd* [1931] AC 333.

25. *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461.

UNITED STATES OF AMERICA

1. *Alana Shoars v Epson America, Inc.* No. SWC112749 (L.A. Super. Ct. 1990).
2. *American Bankers Association v Lockyer* No. 05-17163, 2008 WL 4070308 (9th Cir. Sept. 4, 2008).
3. *Bartnicki v Vopper* 532 U.S. 514 (2001).
4. *Bechhoefer v U.S. Department of Justice Drug Enforcement Admin* 209 F3d 57 (2d Cir. 2000).
5. *Bowers v Hardwick* 478 U.S. 186 (1986).
6. *Cape Pubs. Inc. v Bridges* 423 So 2d 426 (1982 Fla App).
7. *Carson v Here's Johnny Portable Toilets Inc.* 698 F2d 831 (6th Cir. 1983).
8. *Chrysler Corp. v Brown* 441 U.S. 281 (1979).
9. *Department of Justice v Reporters Committee for Freedom of the Press* 489 U.S. 749 (1989).
10. *Diamond v Chakrabarty* 447 US 303, (1980).
11. *Dietemann v Time Inc* 284 F. Supp. 925 (1968).
12. *Doe v Bolton* 410 U.S. 179 (1973).
13. *Eisenstadt v Baird* 405 U.S. 438 (1972).
14. *Florida Star v B. J. F.* 491 U.S. 524 (1989).
15. *Goodyear Tire & Rubber Co. v Vandergriff* 52 Ga. App. 662, 184 S.E. 452 (1936).
16. *Griswold v Connecticut* 381 U.S. 479 (1965).
17. *Hirsch v S.C. Johnson & Sons Inc.* 90 Wis. 2d 379, 280 NW2d (1979).
18. *John W. Carson v Here's Johnny Portable Toilets Inc.* 698 F2d 831 (6th Cir. 1983).
19. *Katz v United States* 389 U.S. 347 (1967).
20. *Kerby v Hal Roach Studios* (1942) 53 Cal App 2d 207.
21. *Lawrence v Texas* 539 U.S. 558 (2003).

22. *Lochner v New York* 198 U.S. 45 (1905).

23. *Loving v Virginia* 388 U.S.1 (1967).

24. *McGregor v Greer* 748 F Supp 881(DC 1990).

25. *McIntyre v Ohio Elections Commission* 514 U.S. 334 (1995).

26. *McNamara v Freedom Newspapers, Inc.* 802 S.W.2d 901 (Tex. App. 1991).

27. *McVeigh v Cohen et al* 983 F Supp 215 (D) DC (1998).

28. *Melvin v Reid* 112 Cal.App. 285, 297 P. 91 (1931).

29. *Midler v Young & Rubicam* 849 F2d 460 (9th Cir. 1988), 944 F2d 909 (9th Cir. 1991).

30. *Miller v Motorola, Inc.* 202 Ill. App.3d 976 (Ill. App. Ct. 1990).

31. *Moore v City of East Cleveland* 431 U.S. 494 (1971).

32. *Moore v East Cleveland* (1977) 431 US 494, 52 LEd 2d 531, 97 SCt 1932.

33. *Motschenbacher v R J Reynolds Tobacco Co.* 498 F2d 821 (9th Cir. 1974).

34. *National Association for the Advancement of Colored People v Alabama ex. Rel. Patterson* 357 U.S. 449 (1958).

35. *New Jersey v T.L.O.* 469 U.S. 325 (1985).

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

37. *Olmstead v United States* 277 U.S. 438 (1927).

38. *Parenthood v Casey* 505 U.S. 833 (1992).

39. *People v Shinkle* 128 Ill.2d 480, 486, 132 Ill.Dec. 432, 539 N.E.2d 1238 (1989).

40. *Pierce v Society of Sisters* 268 U.S. 510 (1925).

41. *Rakas v Illinois* 439 U.S. 128 (1978).

42. *Reno v American Civil Liberties Union* 521 U.S. 844 (1997).

43. *Reno v Condon* (2000) 528 US 141.

44. *Roe v Wade* 410 U.S. 113 (1973).

45. *Shibley v Time, Inc.* 341 N.E.2d 337 (Ohio Ct. App. 1975).

46. *Skinner v Oklahoma* 316 U.S. 535 (1942).

47. *Smith v Maryland* 442 U.S. 735 (1979).

48. *Sutton v Providence St Joseph Medical Center* 192 F 3d 826 (9th Cir. 1999).

49. *Tobey v NLRB* 40 F3d 469 (Dc Cir. 1994).

50. *United States Department of Justice v Reporters Committee for Freedom of the Press* 489 U.S. 749 (1989).

51. *United States v David Lee Smith* 978 F.2d 171 (5th Cir. 1992).

52. *United States v Jones* 132 S. Ct. 945, 949 (2012).

53. *United States v Miller* 425 US 435 (1976).

54. *Watchtower Society v Village of Stratton* 536 U.S. 150 (2002).

55. *Whalen v Roe* 429 U.S. 589 (1977).

56. *White v Samsung Electronics America Inc.* 989 F2d 1512 (9 Crr. 1993).

57. *Zablocki v Redhail* 434 U.S. 374 (1978).

SWEDEN

1. *MS v Sweden* (1999) 28 EHRR 313.

FINLAND

1. *Z v Finland* (1998) 25 EHRR 371.

NETHERLANDS

1. *X & Y v The Netherlands* (1986) 8 EHRR 235.

CANADA

1. *Hunter v Southam* [1984] 2 SCR 145.
2. *R v Duarte* [1990] 1 SCR 30.

3. *R v Dyment* [1988] 2 RCS 417.

STATUTES

SOUTH AFRICAN

1. Broadcasting Act 4 of 1999.
2. Competition Act 89 of 1998.
3. Constitution of the Republic of South Africa, 1996.
4. Consumer Protection Act 68 of 2008.
5. Copyright Act 98 of 1978.
6. Electronic Communications Act 36 of 2006.
7. Electronic Communications and Transactions Act 25 of 2002.
8. Employment Equity Act 55 of 1998.
9. Financial Intelligence Centre Act 38 of 2001.
10. Independent Communications Authority of South Africa Act 13 of 2000.
11. Interim Constitution of South Africa Act 200 of 1993.
12. Merchandise Marks Act 17 of 1941.
13. National Credit Act 34 of 2005.
14. Prevention of Organised Crime Act 121 of 1998.
15. Promotion of Access to Information Act 2 of 2000.
16. Protection of Personal Information Act 4 of 2013.
17. Protection of Personal Information Bill B9 of 2009.

18. Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.
19. Regulation of Interception of Communications and Provision of Communication-related Information Amendment Act 48 of 2008.
20. Statistics Act 66 of 1976.
21. Telecommunications Act 103 of 1996.

UNITED KINGDOM

1. Access to Health Records Act of 1990.
2. Access to Medical Reports Act of 1988.
3. Adoption Act of 1976.
4. Broadcasting Act of 1996.
5. Children and Young Persons Act of 1933.
6. Computer Misuse Act 1990.
7. Consumer Credit Act of 1974.
8. Copyright, Designs and Patents Act of 1988.
9. Crime and Disorder Act 1998.
10. Criminal Justice Act of 1988.
11. Data Protection Act of 1984.
12. Data Protection Act of 1998.
13. Electronic Commerce (EC Directive) Regulations 2002.

14. European Convention on Human Rights of 1953.

15. European Union Directive on Privacy and Data Protection 95/46/EC (EU Directive).

16. Human Rights Act of 1998.

17. International Covenant on Civil and Political Rights of 1976.

18. Magistrates' Courts Act of 1980.

19. Police Act of 1997.

20. Privacy and Electronic Communications (EC Directive) Regulations 2003.

21. Protection from Harassment Act of 1997.

22. Regulation of Investigatory Powers Act of 2000.

23. Rehabilitation of Offenders Act of 1974.

24. Sexual Offences Amendment Act of 1976.

25. Telecommunications Act of 1984.

26. Telecommunications Regulations of 1999.

27. The Health and Social Care Act of 2001.

28. Theatres Act of 1968.

29. The Interception of Communications Act of 1985.

UNITED STATES OF AMERICA

1. Alaska Constitution (1972).

2. Arkansas, Ark. Code Ann. Section 4-110-101.

3. CA Civil Code Section 1798.83 of 2005.

4. California Assembly Bill 1950.

5. Communications Act 2003.

6. Communications Decency Act of 1996.

7. Computer Fraud and Abuse Act of 1986.

8. Computer Fraud and Abuse Act of 1994.

9. Computer Matching and Privacy Protection Act of 1988.

10. Connecticut, Conn. Gen. Stat. Section 36a-701.

11. Delaware, Del. Code Ann. tit. 6, Section 12B1-01.

12. Driver's Privacy Act of 1994.

13. Electronic Communication Privacy Act of 1986.

14. Electronic Freedom of Information Act of 1996.

15. Electronic Fund Transfer Act of 1978.

16. European Communities Act of 1973.

17. Family Educational Rights and Privacy Act of 1974.

18. Federal Trade Commission Act of 1914.

19. Financial Services Modernization Act of 1999.

20. Florida, Fla. Stat. Section 817.5681.

21. Forgery and Counterfeiting Act of 1981.

22. Freedom of Information Act of 1996.

23. Georgia, Ga Code. Ann. Section 10-1-910.

24. Health Insurance Portability and Accountability Act of 1996.

25. Illinois, 815 ill. comp. stat. Section 530/1.

26. Indiana, Ind. Code Section 4-1-10-1.

27. Louisiana, La Rev. Stat. Ann Section 51:3071.

28. Maine, Me. Rev. Stat. Ann. tit. 10, Section 1346.

29. Minnesota, Minn. Stat. Section 325E.61.

30. Montana, Mont. Code Ann. Section 30-14-1701 et seq.; Section 33-19-321.

31. Nevada, Nev. Rev. Stat. Section 603A.010.

32. New Jersey, N.J. Rev. Stat. Section 56:8-161.

33. New York Constitution (1938).

34. New York, N.Y. Gen. Bus. Law Section 899-aa.

35. North Carolina, N.C. Gen Stat., Section 75-65(a).

36. North Dakota, N.D. Cent. Code Section 51-30-02.

37. Ohio, Ohio Rev. Code Section 1349.19(B) (1).

38. Pennsylvania, Pa. Cons. Stat. Section 3(a).

39. Privacy Act of 1974.

40. Privacy Act of 2005.

41. Privacy Protection Act of 1980.

42. Rhode Island, R.I. Gen. Laws Section 11-49.2-7(a).

43. Right to Financial Privacy Act of 1978.

44. Secure and Fortify Electronic Data Act of 2011.

45. Social Security Number Protection Act of 2005.

46. Social Security On-Line Privacy Protection Act of 2001.

47. Telecommunications Act of 1996.

48. Tennessee, Tenn. Code. Ann. Section 47-18-2107.

49. Texas, Tex. Bus. & Com. Code Section 48.103(b).

50. The Cable Communications Policy Act of 1984.

51. The Unsolicited Communications Order of 2005.

52. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015.

53. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

54. Washington, Wash. Rev. Code Section 19.255.010.

55. Wiretap Act of 1968.

INTERNATIONAL CONVENTIONS

1. African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.

2. The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention).

3. The United Nations Commission on International Trade Law (UNCITRAL Model Law on Electronic Commerce) 1996 [MLEC].

4. The United Nations Commission on International Trade Law (UNCITRAL Model Law on Electronic Signatures) 2001 [MLES].

5. The United Nations Convention on the Use of Electronic Communications in International Contracts 2005 [UNECIC].