https://dspace.org/

Internet regulation of harmful content affecting children

Mthethwa, Goitsemang

2015-03-19
http://hdl.handle.net/10539/17306

Downloaded from a DSpace repository. https://dspace.org/

INTERNET REGULATION OF HARMFUL CONTENT AFFECTING CHILDREN

Student Name: Goitsemang Mthethwa
Student No: 513255

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the Degree of Masters of Management in the field of ICT Policy and Regulations

March 2014

Abstract

There are many benefits for children to access the Internet including research for school projects, sharing information and downloading music or movies. However, there are also associated risks of children stumbling onto harmful Internet content including online and child pornography, as well as cyberbullying. The purpose of the study is to determine the effectiveness of the policies and regulation in addressing harmful and illegal Internet content in South Africa. The study used a phenomenological qualitative research methodology.

The conceptual framework adapted Lessig's 1998 model of Internet regulation to inform analysis of the data. Analysis used the legal, social and technology factors of effective Internet regulation. The economic factor of the framework was not used in the data analysis as it requires an in-depth investigation of price regulation, which is beyond the level of detail required to understand the foundational policy and regulatory issues.

The study established that there are gaps in legislation and regulation, in Internet safety education, and in intergovernmental collaboration to educate users. Most legislation is outdated and does not address the technological challenges in regulating the Internet. Another gap is giving service providers a greater obligation for minimising Internet risks affecting children. Furthermore there is lack of technological understanding with respect to regulating the Internet.

The study recommends the review of outdated legislation and regulation and the implementation of widespread educational programs. Regulations specifying the design of pornographic websites is recommended. Lastly service providers need to have obligations towards preventing harmful and illegal Internet content.

Declaration

I declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements of the degree of Masters of Management of Information and Communications Technology Policy and Regulation at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination at any other university.

_____

Goitsemang Mthethwa

31 March 2014

Acknowledgements

Firstly I would like to thank God for affording me the opportunity and to conduct this research.

This research would not have been possible without the help of my supervisor, Luci Abrahams, who contributed immensely in successful completion of this research by guiding, encouraging and supporting me. Without your assistance, this research would not have been possible.

I thank all the respondents for affording me time in their busy schedules and for sharing their wealth of knowledge which contributed in this research.

To my dear husband, Sibusiso Mthethwa, and my lovely children Olwethu and Zanokuhle thank you for the invaluable support and patience. I commend your incredible support through the hard times even when I stole time from our family.

A word of thanks to my mother, Rebecca Raseroka, I know how this achievement means to you, thank you for always being my pillar of strength.

Thank you to my siblings, my big family and friends for being considerate when I could not spend time with you.

Table of Contents

Chapter 1: The risks of Internet access for children and the legislation and regulations involved 1

1.1 Introduction 1

1.2. General risks of the Internet.....4

1.3 Internet risks affecting children.....5

1.3.1 Online harm from content 6
1.3.2 Harm from contact 8
1.3.3 Harm from conduct 9

1.4 Mobile Internet access and minors.....11

1.4.1 Mobile Internet access penetration 12
1.4.2 Explosion of data services 13
1.4.3 Data about minors with mobile Internet access 14

1.5 Legislation and regulations of Internet in South Africa 17

1.5.1 Legislation about cybercrime 18
1.5.2 Legislation and regulation involving e- transactions 19
1.5.3 Legislation and regulation relating to Internet content 19

1.6 Policies, legislation and regulation protecting minors on the Internet 21

1.6.1 UN Convention on the rights of the child 22
1.6.2 African Charter on the rights and welfare of the child 24
1.6.3 Optional protocol on child prostitution, child labour, child pornography ... 25
1.6.4 Palermo protocols - United Nations convention against transnational organized crime 26
1.6.5 The Constitution of the Republic of South Africa of 1996 27
1.6.6 Children's Act 38 of 2005..... 27
1.6.7 Sexual Offences Act 32 of 2007 28
1.6.8 Films and Publications Act 65 of 1996..... 28

1.7 Conclusion 29

1.8 Structure and organization of the dissertation.....30

Chapter 2: Internet content regulation, harmful content and illegal material 33

2.1 Introduction 33

2.2 Risks of Internet that affect children 34

2.2.1 Online harm from content 34
2.2.2 Harm from contact 35
2.2.3 Harm from conduct 38

2.3 Concepts of Internet content regulation 40

2.3.1 Internet content regulation and censorship defined 40
2.3.2 What to regulate 41
2.3.3 Self-regulation 42
2.3.4 Government regulation 43
2.3.5 Co-regulation 44
2.3.6 User empowerment concept 45

2.4 Censorship and content regulation in United States, Sweden and China 47

2.4.1 Content regulation in the United States *(Nanny State)* 47
2.4.2 Content regulation in Sweden *(Laissez faire)* 50
2.4.3 Content regulation in China *(Authoritative)* 52

2.5 Technology: A challenge to Internet regulation 53

2.5.1 Technology Convergence 54
2.5.2 Factors that affect rapid technology convergence 54
2.5.3 Convergence in policy and regulation 56

2.6 Technical tools to prevent harmful and illegal content 56

2.7 Conceptual framework 58

2.7.1 Legal factors 60
2.7.2 Social factors 61
2.7.3 Economic factors 62
2.7.4 Technology factors 62

2.8 Conclusion of the literature review 63

Chapter 3: Research methodology pertaining to harmful and illegal Internet content 65

3.1 Introduction 65

3.2 Research Problem 65

3.3 Purpose statement 66

3.4 Research questions 67

3.5 Research methodology 68

3.5.1 Interpretive Approach 68

3.6 Research design and population 69

3.7 Data collection and analysis 70

3.7.1 Document analysis 70
3.7.2 Advantages and limitations of document analysis 71
3.7.3 Semi- structured interviews 72
3.7.4 Advantages and disadvantages of interviews 74
3.7.5 Sampling 74

3.8 Data analysis 75

3.9 Significance of the study 77

3.10 Limitations of the research study 77

Chapter 4: Research findings of harmful and illegal Internet content 79

4.1 Introduction 79

4.2 Document analysis of policies, legislation and regulations . 80

Period A 1996-2005 – Telecoms reform era 81
4.2.1 The Constitution of the Republic of South Africa of 1996 81
4.2.2 Films and Publication Act 65 of 1996 82
4.2.3 The Telecommunication Act of 1996 85
4.2.4 ICASA Act of 2000 85
4.2.5 Electronic Communications and Transactions Act of 2002 86

4.2.6 White paper on e-Education: Transforming learning and teaching through information and communication technologies (ICTs) of 2004 89
Period B 2005-2010 – Protection of women and children and bridging the digital divide 90
4.2.7 The Children's Act 38 of 2005 90
4.2.8 Sexual Offences Act, No. 32 of 2007 92
4.2.9 Electronic Communications Act of 2005 94
4.2.10 Information Society and Development (ISAD) Plan of 2007 94
4.2.11 ICASA Code of Conduct for broadcasting service licensees of 2008 Regulation 95
Period C 2010- 2014 – Advancing into technology 96
4.2.12 Broadband Policy of 2010 97
4.2.13 Protection from Harassment Act of 2011 97
4.2.14 Internet and Cell phone Bill of 2010 98
4.2.15 National Broadband Policy of 2013 99
4.2.16 National integrated ICT Policy Green paper of 2014 99

4.3 Document analysis of broader perspectives on events of Internet risks 101

4.3.1 Findings on harmful and illegal Internet content 102
4.3.2 Findings on online grooming 103
4.3.3 Findings on cyberbullying 104

4.4 Stakeholders views and experiences on harmful and illegal Internet content 105

4.4.1 Adequacy of the policies, legislation and regulations *(Legal)* 106
4.4.2 Internet Safety Education and Awareness *(Social and technological)* 107
4.2.3 Inter-governmental and other Internet stakeholders collaboration *(Social)* 109
4.2.4 User-created harmful content *(Social)* 111

4.5 Conclusion of the findings 111

Chapter 5: Analysis of the findings on harmful and illegal Internet content affecting children 113

5.1 Introduction 113

5.2 Analysis of the findings on Policies, Legislation and Regulations 114

5.2.1 The Telecom reform era 114

5.2.2 Protection of women and children era 117
5.2.3 The technological era 118
5.2.4 Legislation about jurisdictional boundaries 119
5.2.5 Service provider's responsibility to prevent harmful and illegal Internet content..... 120

5.3 Analysis of the findings on Internet regulation principles..122

5.3.1 Harmful Internet content vs illegal Internet content 122
5.3.2 Modes of Internet regulation..... 123
5.2.5 Nanny State versus Self-Regulation..... 125

5.4 Analysis of the findings on children's experiences 126

5.4.1 Interpretation on findings on experiences of harmful Internet content 127
5.4.2 Interpretation on findings on experiences of online grooming 128
5.4.3 Interpretation of findings on experiences of cyberbullying 129

5.5 Analysis on the findings of themes on harmful and illegal Internet content affecting children 130

5.5.1 Internet safety education and awareness 130
5.5.2 Collaboration of government agencies with themselves and together with other Internet stakeholders 131
5.5.3 The dynamics of technological challenges 131

5.6 Conclusion on the Analysis 132

Chapter 6: Conclusions and Recommendations.....134

6.1 Introduction.....134

6.2 The role of the policies, legislation and regulations in preventing Internet risks affecting children.....135

6.3 User empowerment.....137

6.3.1 Empowering children 137
6.3.2 Empowering the community 139

6.4 Inclusive model of all Internet stakeholders 140

6.5 Balancing over restriction and open Internet 141

6.6 Future Research Question 141

6.7 Conclusion of the harmful and illegal Internet content affecting children 142

References 144

Appendices 155

Appendix A: Document Analysis 155

Appendix B: Research questionnaire.....155

SECTION A: Subject matter experts 157
SECTION B: Service providers 158
SECTION C: Policy makers & Regulators 159
SECTION D: Industry bodies..... 159

Appendix C: Details of Interview Respondents 160

List of figures

Figure 1: Data services coverage in Europe.....14
Figure 2: Activities of children online 17
Figure 3: Filtering mechanism 58
Figure 4: Effective regulation of harmful and illegal content 63

List of Tables

Table 1: Summary of the history of legislation of censorship in the United States 50
Table 2: Interviewees identified and interviewed 75

Glossary of terms

Blue-tooth - Wireless technology that enables communication between bluetooth-compatible devices.

Broadband - high-speed Internet access that is always on and faster than the traditional dial-up access providing provides access to the highest quality Internet services—streaming media, VoIP (Internet phone), gaming, and interactive services.

Broadcasting - is the practice of creating audio and video program content and distributing it to the mass audiences of radio, television and Internet media.

Cellphone - A long-range, electronic device used for mobile voice or data communication over a network of specialised base stations known as cell sites.

Cloud - as storing, processing and use of data on remotely located computers accessed over the internet. It involves sharing computer resources, thus giving users unlimited computing power on demand and accessing their data anywhere through the Internet.

Convergence – The tendency of different technological systems to develop towards performing similar tasks; it means that a single infrastructure can provide a collection of content or services; that a single service-provider can provide multiple services, or that content can be aired to multiple platforms.

E-mail - Electronic mail (or e-mail) means the exchange of electronic text messages and computer file attachments between computers over a communications network, such as a local area network (LAN) or the Internet.

Internet - A worldwide network of networks that all use the TCP/IP communications protocol and share a common address space. It commonly

supports services such as e-mail, the World Wide Web, file transfer, and Internet Relay Chat.

Internet filters - An Internet filter is hardware or software that restricts the information that is delivered over the Internet. Filters can greatly reduce the flow of harmful content onto your computer.

ICT- Information and Communication Technology is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.

ISP – Internet Service Provider

MXit - A social mobile or mobile instant messaging application developed in South Africa running on cellphones with GPRS/3G.

Wi-fi - is a technology that allows an electronic device to exchange data or connect to the internet wirelessly using radio waves.

WWW – The World Wide Web is a system of interlinked hypertext documents that are accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them via hyperlinks.

Chapter 1: The risks of Internet access for children and the legislation and regulations involved

1.1 Introduction

In January 2010, The African Union heads of state and government declared the Information and Communication Technology (ICT) sector as a top priority and adopted a declaration that calls on the African countries to prioritise ICTs as a vehicle for driving Africa's development agenda (DoC, 2010). Broadband and Internet access are the integral part of this priority. There are several undersea cables installed in Africa that encompasses this priority. These undersea cables include Seacom, EASSy, TEAMs, WACS, Main one and ACE which enable access to broadband and Internet to the masses of the people in Africa. The Internet has enormous benefits Madon (2000) that range from helping children with their educational materials to a scope as big as the country's economic development. However the Internet has its own risks and disadvantages. Some of the main problems relating to Internet use are exposure of children to online pornography including child pornography; cyberbullying; violent and racist websites as well as sexual solicitation perpetrated through the Internet. The Internet is defined by (Buys & Cronje, 2004) as a worldwide network of networks that all use the TCP/IP communications protocol and share a common address space. It commonly supports services such as e-mail, the World Wide Web, file transfer, and Internet Relay Chat. Having defined the Internet, it is important for the study to also define World Wide Web (WWW) also called the 'Web' which primarily is one of the methods on the Internet that children accesses harmful content. WWW or the Web is defined as a system of interlinked hypertext documents that are accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them via hyperlinks.

This study will focus on the risks of Internet access experienced by children. This is expressed in more detail by UNICEF (2011 p. v) that articulates that:

> The Internet, mobile phones and other electronic media provide children and young people with levels of access to information, culture, communication and entertainment impossible to imagine just twenty years ago. With many of their extraordinary benefits, however, come hazards. The Internet and associated technologies have made abusive images of children easier to create and distribute, and provide significant new opportunities for abusers to access and make contact with children and young people online. While ICT has not created crimes involving sexual abuse and exploitation of children, it has enhanced the scale and potential of some old and familiar ones.

Some of the characteristics of the Internet that exacerbate these issues are anonymity, and global connection without boundaries; these characteristics make it easy and possible for paedophiles and bullies to harass children with the hope of not being traced and therefore not being liable for these illegal actions.

Children are the most vulnerable people on the Internet as they have neither the emotional maturity nor the resistance to deal with online pornography, harassment or to be lured into a physical meeting with an adult pretending to be a friend on chat rooms (Preston, 2009). In this study children are defined as people under the age of 18 years. It is observed that children who are exposed to these negative activities on the Internet show signs of mental health disability although causality was not established (Mitchell & Wells; 2007 cited in Owolade & Snail, 2009). The problem is compounded by the fact that there are parents who do not have the technical expertise to monitor Internet usage nor understand the high risks that comes with it (Preston, 2009).

South African Film and Publications Board (FPB) conducted a survey of South African children; the subjects in the study were from age thirteen to just over seventeen and in randomly-selected schools in three South African cities. Reporting on the survey the FPB cited on (Chetty & Basson, 2006 p 2) observed that:

> The extraordinary opportunities offered by the Internet for enhancing our lives do not come without risks. The ease with which children may stumble across disturbing, harmful and age-inappropriate materials are too disturbing and real to ignore. The constitutional obligation to act in the best interests of the child imposes a duty on government, industry and civil society to develop mechanisms to protect children from exposure to materials which pose a risk of harm to their emotional and psychological well-being.

It is imperative that all stakeholders of the Internet work together to develop comprehensive protection mechanisms for children accessing the Internet. The Internet undermines the feasibility and legitimacy of laws based on geographic boundaries (Johnson & Post, 1996), therefore any remedy to this problem will need international collaboration.

The study examines Internet content regulation as one of possible remedies to curb harmful and illegal Internet content affecting South African children. The study will explore the risks of Internet access that affect children. Thereafter using qualitative methodology, it will interrogate South African policies, legislation and regulations that relate to Internet content; as well as investigate published academic research reports of Internet risk incidents that occurred where children were involved. Furthermore semi-structured interviews will be carried out to understand the stakeholders' views and experiences. Using the findings the study will then draw conclusions and recommend better ways to minimize the Internet risks affecting children.

1.2. General risks of the Internet

This section discusses risks that are found on the Internet in more detail. It explores the general Internet risks and how they impact children. Firstly the study defines a risk to get a perspective of what a risk involves. The concept of risk, when used in a social context, is defined as “a probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action”; furthermore, a risk can be “foreseen or unforeseen” (Xiao et al, 2012). This study explores the vulnerabilities that the Internet presents. This first section on general risk of the Internet gives a general overview of the Internet risks and thereafter it focusses specifically on risks that affect children.

There are different definitions of cybercrime available in the literature; this study will adopt Smith’s (2008 p356) definition that refers to cybercrime as crime that “encompasses all crimes involving computers, including infiltrating protected systems, espionage, identity theft, fraud, child pornography, and child exploitation”. Cybercrime can be categorised similar to the categories of common crime; for example embezzling funds using computer technology could be categorized as white-collar crimes which is generally defined as nonviolent crimes committed in the course of business activities (Shinder, 2002). These crimes are usually motivated by monetary profit and often involving theft, cheating, or fraud whilst Internet child pornographers are usually classified as sex offenders or paedophiles and regarded as violent or potentially violent criminals as Shinder (2002) articulates. The motivation and tactics of cybercriminals that do cybercrime has changed from previously large-scale events such as network worms that were mostly exhibitions of technical superiority; today, these criminals are primarily motivated by

economic incentives to turn their assets into revenue (Provos, Rajab, & Mavrommatis, 2009).

In South Africa identity theft continues to be the most prevalent cybercrime (Fick, 2009). Identity theft is mostly used to but not limited to the following offences: assume someone's identity to evade the police, to obtain credit on someone else's credentials where the criminal is not able to do that on his/her own, to gain access to bank accounts, to launder money, etc. (ibid). These general Internet risks do not have a direct impact to children but indicates the extent to which the Internet community including parents have difficulty dealing with Internet privacy. If parents are vulnerable in divulging their personal information, it is difficult to assume that they will be able to advice children on Internet risks.

As articulated the study will not focus on the general Internet risks but rather on the Internet risks that affect children.

1.3 Internet risks affecting children

The study has given a general view of Internet risks and now focuses on Internet risks that affect children. Internet content can be categorized as harmful or illegal, for example there is a difference between children accessing pornographic material (harmful) as opposed to adults accessing child pornographic material (illegal) (Akdeniz, 2001). These concepts are discussed at length in the literature review. The study focuses only focuses on the harmful content and not necessarily on illegal content accessed by adults.

Accessing illegal content on the web constitutes cybercrime. A study conducted by Livingstone and Leslie of EU Kids online referenced in

(UNICEF, 2011) has defined categories of risk and harm related to online activities. The first category is online harm from content, where a child is a passive recipient of pornographic or harmful sexual content. The second category is harm from contact, where a child is targeted as a participant by an adult or another child in activities such as sexual abuse and then disseminated for online grooming for sexual abuse, or for bullying. The third category is harm from conduct, where the child actively initiates risky or abusive behaviour towards themselves or others. The study explains the categories mentioned in more detail.

1.3.1 Online harm from content

The first Internet risk is online harm from content; this may be access of a child to online pornography and child pornography. The study looks at the definitions of pornography, online pornography, child pornography and online sexual exploitation to give a comprehensive understanding of the topic at hand. Pornography is sexually explicit material which may be verbal or pictorial or any representation that is primarily designed to produce sexual arousal in viewers (West, 2012). From West (2012) definition the study defines online pornography as any representation of sexual explicit material that is presented online including on the web.

Online child pornography is defined by International Centre for Missing & Exploited Children (2008) as including but not limited to, “any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes,” as well as the use of a child to create such representation. Online child pornography is illegal and anyone found with this material will be prosecuted by the South African law and international laws.

In recent reports by Immigration and Customs Enforcement's (ICE) (2013) an on-going investigation of child pornography launched in december 2009 was undertaken; targeted at the Dreamboard members around the world. The investigation which was carried out by the U.S. ICE, Homeland Security Investigations (HSI), along with dozens of other law enforcement agencies, as part of operation Delego saw the guilty pleas of Christopher Blackford, 28, and William Davis, 39. Blackford pleaded guilty to participating in a child exploitation contributing 84 posts to the online bulletin board that contained child pornography. He faces 20 years to life in prison, a $250,000 fine, and five years of supervised release. William Davis pleaded guilty to conspiracy to advertise child pornography where he posted advertisements offering to distribute child pornography to other members of the board. He faces 15 to 30 years in prison, a $250,000 fine, and at least five years of supervised release for his role in Dreamboard.

The reports by ICE (2013) reveals that Dreamboard was a members-only online bulletin board created and operated to promote paedophilia and encourage the sexual abuse of young children in an environment designed to avoid law enforcement detection. According to court documents, Dreamboard members traded graphic images and videos of adults molesting children. Prospective members had to create and share child pornography to gain entry into the group and to maintain membership once accepted. In their endeavour to conceal their criminal activity from detection, Dreamboard members communicated using aliases rather than their actual names and content posted on Dreamboard was encrypted with a password shared only with other members. Members also employed proxy servers to route the group's Internet traffic through other computers in an attempt to prevent law enforcement from tracing Internet activity.

A total of 72 individuals, including Blackford and Davis, have been charged as a result of operation Delego, which is the largest prosecution in United States history of an online bulletin board network dedicated to child sexual abuse. Fifty-seven of these individuals have been arrested; forty seven defendants have pleaded guilty for their roles in the conspiracy and an additional defendant was convicted after a trial. Fifteen of the seventy two charged individuals remain at large and are known only by their online identities. Investigations are still on-going in the effort to apprehend the remaining individuals (ICE, 2013). This case highlights how child pornography is rife and that the perpetrators will try to defeat the ends of justice by avoiding detection.

1.3.2 Harm from contact

The second category is harm from contact; one such example is online grooming. Online grooming is the process where “an individual befriends a young person for online sexual contact, sometimes with the involvement of webcams that can allow sharing of the exploitation among networks of child sex abusers, and sometimes extending to a physical meeting to commit sexual abuse” (UNICEF, 2011 p2). It is easier when you meet someone to be certain that they are who they say they are or at least the same age and gender as they say. It is more difficult on the web as it is easy to create a fake online profile. Children tend to be more naïve and trusting and are more likely to fall prey to strangers posing as children their own age (Australian Government, n.d). Potential victims can be groomed online in chat rooms, social networking sites and instant messaging (UNICEF, 2011). Children can be groomed online for sexual abuse offline.

In South Africa a case was reported where a 27 year old man Dave Coughlan was charged of raping a 15 year old girl after sexually grooming

her on social network Mxit (Smillie & Tromp, 2010). In the article Coughlan told the girl on Mxit that he was having a party and offered to pick her up, explained the mother. Initially the girl turned him down, but then later that day he showed an angry face on his profile depicting that he was angry. In their communication with the teenager the perpetrator told her that no one had pitched up for the party, but she could still come over that Saturday, and he said he could pick her up. According to the mother on Saturday night, Coughlan picked up the girl at the corner of the street where she lived and took her away. In the report it is alleged that while standing at his computer, the perpetrator came up behind the girl and placed a cloth that had strong medicinal smell over her face and she passed out.

Smillie and Tromp (2010) reported that later when the girl woke up, Coughlan was on top of her raping her. He then placed the cloth over her mouth again. "When she woke up again, the sun was up. She listened to check if he was around. It was very quiet, and then she grabbed her clothes and cellphone, and locked herself in the bathroom." It was then that she had sent the "please-call-me SMS" to her mother where her mother called the mobile number; the girl then described where she was. She was rescued by her mother and the police. The daughter was taken to a rape and trauma centre, where she was examined and evidence taken, and was given anti-retroviral medication described the mother (Smillie and Tromp, 2010). This is a typical online grooming case where an unsuspecting child became a victim.

1.3.3 Harm from conduct

The third category is harm from conduct. The examples of this category is when children create or upload their own pornographic material, physically meeting an adult met on the web, placing images of themselves or another young person on the web, and downloading abusive images of children or

bullying (UNICEF, 2011). Children can reveal their personal information such as e-mail and other online accounts with little understanding of the concept of privacy which makes them vulnerable to be tracked. When not monitored they can upload pornographic materials which may be addictive. They can also upload images of themselves or other young people online without understanding the consequences that go with this. The consequences include the fact that the image can remain in circulation all the time and there is almost no limit on how often or by whom it can be viewed or passed on (UNICEF, 2011). Internet access also provides an easy and often anonymous way for children to bully and intimidate other children or to circulate hurtful gossip or embarrassing photos or videos (Australian Government, n.d).

A practical example of harm from conduct is the reported cases of sexual abuse of children recorded on mobile phones by other children in South African schools. These cases give a perspective of how mobile phones were used by children to record and then circulate child pornography and harmful content through the web by sharing videos. At Jules High School in Johannesburg, Gauteng it is alleged that at least 10 Grade 8 pupils stood by and filmed their classmate being raped by three boys on their mobile phones; the family of the pupil feared that their daughter would be traumatised over and over again as mobile phone videos of the attack kept on circulating among pupils (Van Wyk, 2010).

Another incident was at Collegiate Girls High School in Port Elizabeth, Eastern Cape, where a group of 13 year-old girls in Grade 8 were caught sipping vodka and watching a pornographic video on a mobile phone allegedly of one of the girls having sex with her boyfriend; within only a few hours, news of the incident was plastered over social networking websites such as Twitter and Facebook; which was a shock to the parents and a great

concern to the school (Herald & Dispatch, 2010). Child specialists have warned that the trend of younger children being exposed to explicit pornographic material, and subsequently exploring their sexuality, is becoming commonplace due to the proliferation of mobile phones and a lack of gate-keeping measures by technologically unknowledgeable parents (Herald & Dispatch, 2010).

Another case was that of a boy from Mondeor and a girl from John Adamson High school who allegedly had alcohol with a friend and then had sex in the toilet, which was subsequently recorded on a mobile phone. After the school holidays, the girl discovered that the video had been widely circulated and laid a charge of rape against the boy (Harbour, 2010).

These cases are a reflection of how irresponsible children can be, firstly by recording the sexual encounters of other children and secondly disseminating these recordings on the web.

1.4 Mobile Internet access and minors

Technological advances have enabled mobile phones to access the web, perform video streaming and be used for e-mails whereas it previously could not. This convergence of technology has brought a more complex challenge to regulation. Historically mobile phones used to be telecommunication tools that only made voice calls, they now do sending and receiving of text messages, picture messaging, video material, access to e-mails, instant messaging as well as accessing the Internet. This poses a problem into the traditional methods used to prevent harmful content from being consumed by children. Technology convergence is discussed in detail in the literature review.

1.4.1 Mobile Internet access penetration

Mobile phones and devices of different kinds represent the future of Internet connectivity, especially in low and middle income nations because of the nature of mobile technology. It is more costly to dig up holes and lay cables for telecommunications than to put up mobile technology masts. Therefore mobile technology is a better option for Africa where there is more complications in the terrestrial sphere. In South Africa the number of Internet users increased dramatically in 2011 and 2012 due to both smart phones and ordinary mobile phones (Goldstuck, 2012). World Wide Worx backed by the Howzit MSN online portal conducted a study called Internet access in South Africa 2012, the findings of the study showed that South African Internet user base had grown from 6.8 million in 2010 to 8.5 million at the end of 2011. World Wide Worx forecast that the strong growth will continue in the following years; the spotlight not only being online media but also social networking and electronic services in general.

The Internet access in South Africa study by Goldstuck (2012), has revealed that a total of 7.9 million South Africans access the Internet on their mobile phones. Of these, 2.48 million access it only on their mobile phones and do not have access to computers. The remaining 6.02 million users access the Internet on their computers, laptops and tablets. However 90% of this number, which is 5.42 million also access it on their mobile phones. This means that almost 8 million South Africans sometimes or regularly access the Internet on their cell phones. The South African market is embracing this mobile penetration; not only are traditional service providers offering mobile devices and phones, banks are also offering these mobile devices and phones at competitive prices. With the dramatical increase of mobile Internet market in South Africa so is the chance of an increase in accessibility of mobile devices among children.

1.4.2 Explosion of data services

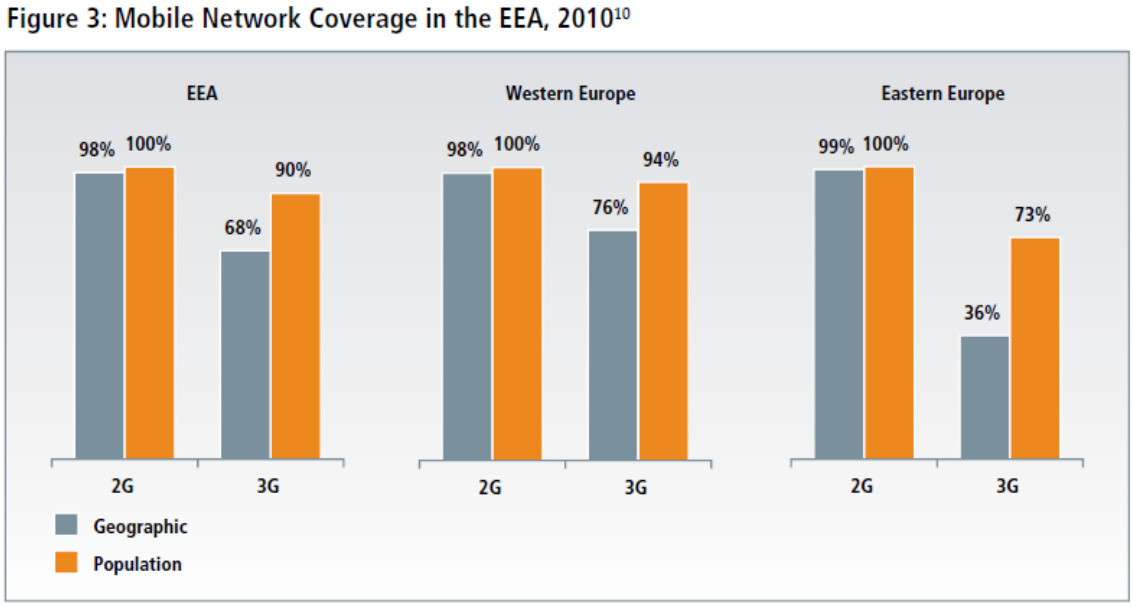
The explosion of tablets and smartphones has fundamentally changed the way people consume telecommunication services today. Traditional mobile companies such as network operators, handset manufacturers and infrastructure suppliers no longer fully define the mobile market; content and service offerings, new software and user interfaces, and easily accessible distribution channels are creating a consumer-driven mobile ecosystem with a diverse set of players (GSMA, 2011). The evolutions in smart device strategy, as well as the popularity of tablets have resulted in a significant increase in data usage as well as explosive growth in bandwidth consumption.

High volumes of data requires network resources that can be able to handle the load. The Blackberry outage that lasted for days is an example of explosive data growth that could not be handled, where a failure in on of Research in Motion's (RIM) core switches escalated when RIM's failover systems started to fail, causing significant backup of email, which created a ripple effect across the globe (Meyer, 2011). AT& T was also forced to change their unlimited usage plans to capped plans because of the iPhone and iPad which are 3G and LTE devices (Hildenbrand, 2012). These are clear indications of the kind of complexities that operators are facing today due to consumption of high volumes of data.

A network coverage analysis was conducted in Europe by GSMA in 2010. The results on the analysis is depicted on Figure 1 below. In the analysis 2G services indicates the voice and messaging services while 3G refers to the data services. Data services implies that the user will connect to the Internet to consume these services. The analysis reflect that the mobile services are universally available, with 98% geographic and nearly 100% population coverage in the European Economic Area (EEA). Furthermore there is little

difference in levels of coverage for voice and messaging (2G services) between Eastern and Western Europe, with population coverage close to 100% in almost all countries. This study indicate the increase in data services that are expected to grow even further in the years to come. The analysis of the coverage of data service does not directly affect children but reflects the fact an increase in data services will consequently increase the accessibility of children to the Internet.

Figure 1: Data services coverage in Europe



Source: GSMA (2011)

1.4.3 Data about minors with mobile Internet access

Mobile Internet connectivity poses a challenge to parents and teachers in restricting, monitoring or controlling children's access to the Internet thereby increasing the potential risks to children. These mobile phones carry with them an immediacy that simply does not exist when the device being used is in a fixed location, where supervision is easier. The filtering software that is normally installed in personal computers at home or in school labs to monitor

and prevent children's access to harmful content might become not be used in mobile phones.

Mobile phones are ubiquitous, affordable and portable making them accessible to poor populations including children. Mobile Internet penetration is growing exponentially as articulated in the sections above. As the growth of the Internet users surges so does the profile grow to include children. In a survey conducted by ITU (2011) it is indicated that younger people tend to be more online than older people, in both developed and developing countries. In developing countries, 30% of those under the age of 25 use the Internet, compared to 23% of those who are 25 years and older. However, 70% of the under 25-year olds a total of 1.9 billion are not online yet which is a huge potential if developing countries can connect schools. This statement coincides with the aforementioned statement where African Union heads of state and government declared to make the ICT sector a priority to drive African development (DoC, 2010).

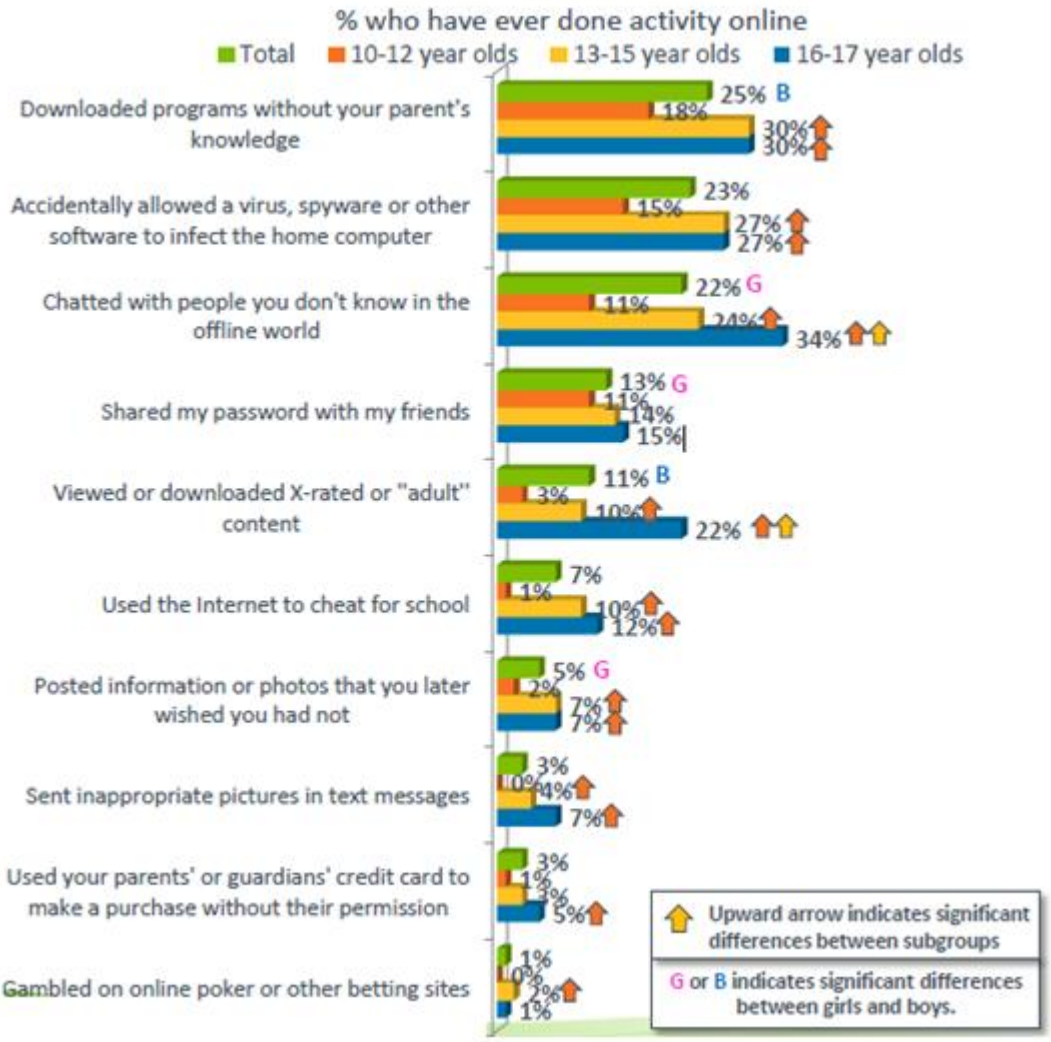
In another study conducted by (Kreutzer, 2009) on mobile phone usage in a lower income area amongst school children in South Africa, it was found that 97% of the respondents own a mobile phone and that 97% of all respondents have used the Internet through a cell phone; 83% within the study's sample do this on a typical day. The abovementioned studies highlight an important fact that more children have Internet access through mobile phones and this trend will continue to grow in years to come even in low income areas.

In order to understand the activities of children on the Internet, the study looked at a research conducted by Pieters and Krupin (2010) in the United States. The research reveals that most children go on the web to communicate; and that there are more than half of tweens and teens emailing with friends and family (66%) and/or engaging in social networking

(61%). They also use various other types of communication, such as chatting with people they do or do not know offline, instant messaging, or posting to blogs. Another popular activity among tweens and teens is for media and content downloading; more than half of children typically view or download some kind of media (video or music) online. The study further shows that half of tweens already have at least one social networking account and by the time teens reach 16-17 years of age, over 85% are engaged in social networking.

Furthermore Pieters and Krupin (2010)'s study reveals that one in ten children (11%) admit to ever engaging in some form of cyberbullying behaviour. The report shows that a much higher proportion of children seem to know someone who has experienced cyberbullying behaviours (52%). A quarter or more children say they know someone who has had mean information about them posted online, rumours spread about them online or their password hacked. One in six know someone who has been approached online by someone they don't know, had embarrassing information posted on the web, or been cyber-pranked. Figure 2 depicts that children do engage in risky behaviours and that they need to be monitored and made aware of the risks they are engaging in on the Internet.

Figure 2: Activities of children online



Source: Pieters and Krupin (2010)

1.5 Legislation and regulations of Internet in South Africa

Having looked at the risks that the Internet access poses to children, the study examines the policies, legislation and regulations of Internet content in South Africa to determine how effective they are to prevent children from accessing harmful and illegal materials. Regulation can be ex-ante or ex-post. Ex-ante regulation is regulation that deals with the prevention of

unlawful behaviour or action while ex-post regulation deals with the aftermath of the unlawful behaviour or action (Kolstad, Uclen, & Johnson, 1990). In this section the study examines legislation and regulations that regulate different facets of Internet content.

1.5.1 Legislation about cybercrime

The Electronic Communication and Transaction Act No.25 of 2002 is a legislation that regulates cybercrime. With reference to the abovementioned facts about cybercrime, managing customer's information is key towards preventing or minimising cybercrime; this according to (Flick, 2009) is called information assurance. The aspects of information assurance are confidentiality, integrity, authentication, availability and non-repudiation (ibid).

Flick (2009) articulates that information is kept confidential once the information is only accessed, used, copied by users who have been duly authorised to do so; the second aspect of data integrity means that data may not be created, altered or deleted without the proper authorisation; the third aspect of authenticity means that a user that logged on to a computer is in reality the person whose credentials (e.g. user name and password) was used; and lastly availability means that the information together with the systems needed to process the information and the security measures that protect the information are all functioning properly at the time the information is needed. This basic understanding of information assurance is important to comprehend the level of cautiousness that children accessing the Internet needs to be aware of.

1.5.2 Legislation and regulation involving e- transactions

Privacy is an integral part of e-Transactions as it plays a role in minimizing the hacking of e-Transactions. Privacy International cited in Cronjé (2009) made the statement regarding South Africa's financial sector in its 2005 world survey that "South Africa has a well-developed financial system and banking infrastructure; despite the sophistication of the financial sector, the privacy of financial information is weakly regulated by a code of conduct for banks issued by the Banking Council." The statement highlights the International perspective of how South Africa is viewed in terms of some of the problems experienced on privacy; subsequently the South African Law Reform Commission instructed a project committee to work on a draft Bill on Protection of Personal Information (Cronjé, 2009).

The ECT Act of 2002 addresses the collection of personal information in its chapter 8 but the subscription to these principles is voluntary (RSA, 2002). The RIC Act prohibits the interception of communications while one Act that has recently been enacted, The National Credit Act, makes specific provision for the regulation of personal information, although such regulation is restricted to the financial sector (Cronjé, 2009). Piracy also affects children as they explore the Internet and giving away their information on social networks.

1.5.3 Legislation and regulation relating to Internet content

ECT Act of 2002 stipulates that Internet Service Providers (ISP) who unknowingly distribute, provide access and hosting of child pornography may be exempted from liability (RSA, 2002). These ISPs are exempted if they comply with certain requirements stipulated in the Act. The exempt of liability by the ECT Act of 2002 provides "safe harbours" for the ISPs as

accountability only lies with the individual websites that has got such content. Regulation of the content becomes a challenge as the ISPs do not have to monitor the content they host for the different websites and that has a ripple effect of individual websites not complying with the law.

Films and Publication Act 65 of 1996 regulates the creation, production and distribution of certain publications and certain films by classifying them and by imposing age restrictions (RSA, 1996a). This means that any person who knowingly distributes or post the material on any website which contains a visual presentation or a description of child pornography, explicit violent sexual conduct, bestiality, explicit sexual conduct which degrades a person and which constitutes incitement to cause harm, and the explicit infliction of extreme violence which constitutes incitement to cause harm is guilty of an offense (RSA, 1996a). ISPs that knowingly hosts these materials would be considered to be distributing it and be punishable by law (Buys & Cronje, 2004). The difficulty about this Act is that it has to be proven beyond reasonable doubt that the person who has posted illegal material on the website knew that they were doing so. This Act is ex-ante and undertakes to prevent harmful and illegal content exposed to South Africans.

The ICASA Code of Conduct for Broadcasting Service Licensees does not seem to include the Internet in their clauses. This code of conduct only regulates content in the broadcasting arena as its definition of “audience” is both the viewers and listeners of television and sound, which does not include the Internet (ICASA, 2008).

Internet content regulation also deals with a very sensitive issue of freedom of expression. Given South Africa’s history of apartheid, the right to freedom of expression is not taken lightly. This constitutional right is used by many to argue that Internet content should not be regulated. One view that is

embraced by academics, theorists, journalists is that of an open Internet, free from any form of regulation (Barlow, 1996; Delacourt, 1997); this view is directly opposed by governments, some media organizations and corporations arguing for a form of regulation of the Internet (Mthimkhulu, 2010). However like all rights freedom of expression is subject to limitations when content is illegal and harmful. It is therefore important to find the balance between regulating Internet too much thereby limiting innovation and having an open Internet that anyone can commit crime on and expose vulnerable children to harmful Internet content without recourse.

Having looked at these tenets of legislation it is clear that South Africa has somewhat attempted to regulate Internet content. However regulating Internet content has become extremely complex because of convergence of technologies. Mobile phones play a vital role in promoting access to Internet for both adults and children; and yet in South Africa content contained in email, instant messages, chat SMS or MMS is not mentioned in the legislation and regulation. The other complexity is the fact that before convergence telecommunication providers and broadcasting were regulated individually and IT systems were not regulated; since the convergence between technologies has occurred all these above-mentioned sectors need to be regulated collectively. The research concern is that, it has not been tested whether existing legislation sufficiently addresses the issues in the online environment.

1.6 Policies, legislation and regulation protecting minors on the Internet

In this section the study looks at the policies, legislation and regulation that exists internationally and in South Africa on the protection of children on harmful content. The study looks at the international and national legislative

framework concerning the protection of children from any kind of harm. The discussion is about a vast array of the rights of the children but the study will concentrate on the rights that are relevant to the protection of children in terms of access to information and thereafter their rights to protection of harm.

This framework provides guidance on addressing and responding to sexual exploitation and abuse of children in the online environment, they also establish a set of legally binding obligations for States parties to take specific measures in respect to the protection of children. The framework includes definitions of offences and provisions that require punishment for criminalized behaviour, and allow for more effective prosecution of perpetrators.

1.6.1 UN Convention on the rights of the child

The UN Convention defines children as everyone under the age of 18. The convention states that “rights are things that every child should have and be able to do”; also that every child has the same rights no matter who they are, where they live, what their parents do, what language they speak, what their religion is, whether they are a boy or girl, what their culture is, whether they have a disability, whether they are rich or poor. No child should be treated unfairly on any basis; children have the rights to be alive (UN, 2009). This provision makes is relevant to the study as is highlights the importance of protecting children.

The convention also states that all adults should do what is best for children and that when adults make decisions, they should think about how their decisions will affect them. The government also has a responsibility to make sure that the rights of children are protected; they must help the family of the

child to protect these rights and create an environment where children can grow and reach their potential (UN, 2009). Here the convention provides that adults and governments both have the responsibility towards children which is relevant to the study.

The convention continues to state that children have the right to find out things and share what they think with others, by talking, drawing, and writing or in any other way unless it harms or offends other people. Children have the right to choose their own friends and join or set up groups, as long as it is not harmful to others (UN, 2009). This includes the rights to access the Internet, where most of the children make friends on social networks.

The convention articulates that children have the right to privacy. Therefore there needs to be preventative measures to ensure that children's privacy is kept at all times as they become vulnerable to paedophiles. Children have the right to get information that is important to their well-being, from radio, newspaper, books, computers and other sources. Adults should make sure that the information they are getting is not harmful, and help children find and understand the information they need. Children have the right to be protected from being hurt and mistreated, in body or mind; they have a right to be free from sexual abuse; and they have a right to protection from any kind of exploitation (UN, 2009).

The convention stipulates a lot of what Internet regulation is trying to achieve in protecting children because it places protection alongside other rights particularly relevant to the benefits the Internet brings which are freedom of expression, freedom to seek information and freedom of association (UNICEF, 2011).

1.6.2 African Charter on the rights and welfare of the child

The African charter on the rights and welfare of the child recognizes the importance of human rights without distinction of any kind such as race, ethnic group, colour, sex, language, religion, political or any other opinion, national and social origin, fortune, birth or other status (OAU, 1999). The charter recognizes the critical situation of most African children due to unique factors of their socio-economic, cultural, traditional and developmental circumstances, natural disasters, armed conflicts, exploitation and hunger, and on account of the child's physical and mental immaturity that needs special safeguards and care (OAU, 1999). The charter stipulates that a child is anyone below the age of 18. It also stipulates that all actions concerning the child taken by any person or authority should be in the best interests of the child.

All African nations need to ensure, to the maximum extent possible, the survival, protection and development of the child. Children shall be assured the rights to express their opinions freely in all matters and to disseminate their opinions subject to restrictions as are prescribed by laws. Every child has a right to privacy; children should not be subjected to unlawful interference with their privacy, family home or correspondence, or to the attacks upon their honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children’s care (OAU, 1999).

The Charter undertakes to protect the child from all forms of sexual exploitation and sexual abuse and take measures to prevent the inducement, coercion or encouragement of a child to engage in any sexual activity; the use of children in prostitution or other sexual practices; and the use of children in pornographic activities, performances and materials (OAU,

1999). The African charter does cover the protection of children and the responsibility of parents online and offline.

1.6.3 Optional protocol on child prostitution, child labour, child pornography

The protocol has been put in place to achieve the purposes of the Convention on the rights of the child. The protocol is greatly concerned about the growing availability of child pornography on the Internet and other evolving technologies. The international conference on combating child pornography on the Internet which was held in Vienna in 1999 has called for the worldwide criminalization of the production, distribution, exportation, transmission, importation, intentional possession and advertising of child pornography, and stressing the importance of closer cooperation and partnership between governments and the Internet industry (UN, 2002).

Article 3 of the protocol prohibits the sale of children, child prostitution and child pornography. It stipulates that each state party shall ensure that the acts of “offering, delivering or accepting, by whatever means, a child for the purpose of sexual exploitation; transfer of organs of the child for profit” are fully covered under their criminal or penal law, where such offences are committed domestically or transnationally or on an individual or organized basis (UN, 2002). Article 3 also stipulates the prohibition of the engagement of the child in forced labour, by improperly inducing consent, as an intermediary, for the adoption of a child in violation of applicable international legal instruments on adoption; offering, obtaining, procuring or providing a child for child prostitution and producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography should be included (UN, 2002).

What is also relevant for this study is that the protocol ensures that “States parties take all necessary steps to strengthen international cooperation by multilateral, regional and bilateral arrangements for the prevention, detection, investigation, prosecution and punishment of those responsible for acts involving the sale of children, child prostitution, child pornography and child sex tourism. States parties shall also promote international cooperation and coordination between their authorities, national and international non-governmental organizations and international organizations”. (UN, 2002).

1.6.4 Palermo protocols - United Nations convention against transnational organized crime

The purpose of this convention is to promote cooperation to prevent and combat transnational organized crime more effectively (UN, 2000). In his remarks the Secretary- General at the time Mr Kofi Annan alluded to the fact that criminal groups have wasted no time in embracing the present globalized economy and the sophisticated technology that goes with it; therefore the efforts to combat these crimes have been fragmented and the weapons used were almost obsolete. The convention gives a new tool to address these crimes as a global problem (UN, 2000).

In the convention an offence is transnational “if it is committed in more than one State; or is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State; or it is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or it is committed in one State but has substantial effects in another State” (UN, 2000). The convention binds each state to take the necessary measures, including legislative and administrative measures in accordance with fundamental principles of its domestic law, to ensure the implementation of its obligations

under the convention. All offences established in the convention will be established in the domestic law of each State entity.

As South Africa is a member of the United Nations and organization of African Unity it is bound by the prescriptions thereof and has instituted legislation to ensure these recommendations. The below sections that follow looks at the South African legislation in terms of the rights of children.

1.6.5 The Constitution of the Republic of South Africa of 1996

The Bill of Rights in the constitution provides for the protection, promotion and respect for the human rights of all South Africans. Section 28(1) stipulates that a child is anybody under the age of 18. A child's best interests are of paramount importance in every matter concerning the child (RSA, 1996b).

1.6.6 Children's Act 38 of 2005

The South African Children's Act of 2005 recognises section 28 of the Constitution of South Africa on the rights of children, United Nation's universal declaration of human, Geneva declaration on the rights of the child, the United Nation's convention on the rights of the child, the African Charter on the rights and welfare of the child and the statutes and relevant instruments of specialised agencies and international organisations concerned with the welfare of children (UNICEF, 2011).

The Act states that the Director-General must keep and maintain a national child protection register (RSA, 2005). The function of the register is to have a record of abuse or deliberate neglect inflicted on specific children, to use the information in the register in order to protect these children from further

abuse or neglect, to share information between professionals that are part of the child protection team, to determine patterns and trends of abuse or deliberate neglect of children; and to use the information in the register for planning and budgetary purposes to prevent the abuse and deliberate neglect of children and protect children on a national, provincial and municipal level (RSA, 2005). The register also contains names of people who are found to have been unsuitable to work with children to prevent them from further abuse. This means people who are found to be paedophiles will appear in this register.

1.6.7 Sexual Offences Act 32 of 2007

The South African Sexual Offences Act 23 of 2007 defines a child as anyone under the age of 18. Sexual grooming refers to the process of preparing or making a child ready to engage in a sexual act. Grooming usually takes place over a period of time (RSA, 2007). As alluded in the section of online sexual grooming the perpetrator often tries to be the child's friend by winning their trust and then progresses to solicit sexual act from a child. It is also a crime to intentionally let a child watch a sexual act.

The Act creates various pornography-related crimes which are exposure or display of child pornography to an adult with or without consent, exposure or display of pornography to children, with or without consent, using children for or benefiting from child pornography, engaging or displaying of pornography to persons who are mentally disabled, using persons who are mentally disabled for pornographic purposes or benefiting from their use (RSA, 2007).

1.6.8 Films and Publications Act 65 of 1996

The South African Films and Publication Act 65 of 1996 regulates the creation, production and distribution of certain publications and certain films

by classifying them and by imposing age restrictions (RSA, 1996a). This means that any person who knowingly distributes or post the material on any website which contains a visual presentation or a description of child pornography, explicit violent sexual conduct, bestiality, explicit sexual conduct which degrades a person and which constitutes incitement to cause harm, and the explicit infliction of extreme violence which constitutes incitement to cause harm is guilty of an offense (RSA, 1996a).

The Act criminalizes the creation, possession and distribution of child abuse images that means any image or description of a person who is under the age of 18 years or made to appear, look like or described as a person under that age, engaged in any form of sexual conduct (RSA, 1996a). The Act does not distinguish between images created by the use of real children and products of the imagination, including “virtual” child-pornography created by using sophisticated computer graphics.

1.7 Conclusion

Chapter 1 introduced the different types of risks that are found on the Internet. Those that are general risks that impact every individual and then it focused specifically on children. The study revealed that children are at risk of stumbling into harmful and illegal content of pornography and child pornography on the web. Cyberbullying was also discussed which affects children’s emotional being. Children are at risk of being groomed by older people to physically meet with them, thereby making them vulnerable to sexual exploitation. As articulated by UNICEF, (2011) the Internet does not create these crimes but exacerbates the situation.

Mobile Internet access is prominent at this stage and it is expected to grow in leaps and bounds. Furthermore the explosion of data services attracts

people to seek more Internet access on different devices that they use. This gives perspective of the growing demand to access the Internet despite all the existing risks thereby extending this demand to children.

There is the increased focus on sexual exploitation and abuse of children at the international level and the development of new global and regional human rights instruments. However as articulated by the International Centre for Missing & Exploited Children cited in UNICEF (2011), as of 2010, only 45 of the 196 countries reviewed had legislation sufficient to combat child abuse image offences, and 89 had no legislation at all that specifically addressed child pornography. Of the countries that do have legislation in place, 52 do not define child pornography in their national legislation; 18 do not provide for computer-facilitated offences; and 33 do not criminalize possession of child pornography, regardless of the intent to distribute. This means there are other countries that lack the implementation of necessary legislation. This is worrying to say the least.

South Africa has demonstrated its efforts to implement these instruments as indicated in the above-mentioned legislation. The effectiveness of these laws and regulation is what the study needs to established.

1.8 Structure and organization of the dissertation

Chapter 1 presented the background of the benefits of the Internet and why South African government is striving for Internet penetration. It also presented the Internet risks in general and those that affect children. The chapter also highlights the international and national policies, legislation and regulation in South Africa and that is concerned about the Internet.

Chapter 2 - This chapter is about literature review related to Internet risks. The chapter highlights the concepts of Internet regulation and explains further the legislation and regulations related to prevention of harmful and illegal Internet content. The level of censorship in different countries is explored to give an indication of the different levels of censorship so as to identify the level of censorship in South Africa. The conceptual framework is also addressed.

Chapter 3 - The qualitative methodology with the phenomenological approach is followed in this study, therefore this chapter presents the analysis which serves to address the number of questions concerning the research; it introduces the methodology, its approaches and the data collection analysis to be followed.

Chapter 4 - This chapter illustrates the results and findings of the research; the results from the data analysis of the policies, legislation and regulation related to harmful Internet content as well as results from published academic research reports or the encounters of children of the Internet; and semi-structured interviews. The themes identified were also presented in this chapter.

Chapter 5 – This chapter analyses and perspective on the literature review regarding the Internet regulation concepts and the factors that affect the effective Internet regulation in Chapter 2 and the findings of the research in Chapter 4.

Chapter 6 - This chapter presents the recommendations based on the findings of the research; it seeks to address the clearer perspective of the problem and provides creative solutions. This chapter also provides conclusion of the research and indicates whether the purpose of the research

to investigate the effectiveness of policies, legislation and regulation in addressing the harmful and illegal Internet content.

Chapter 2: Internet content regulation, harmful content and illegal material

2.1 Introduction

This Chapter aims to review the critical points of current knowledge around the subject matter of Internet content regulation and censorship, giving a clear understanding of the facts that this research is going to encounter. This literature review is divided into six main sections. The first section highlights the risks on the Internet that negatively affects children. These include online pornography, cyber bullying, online sexual grooming and harmful behaviour by children.

Secondly the section reviews the concepts of Internet content regulation and censorship. The study will discuss the definition of Internet content regulation thereafter it will explore in more details other Internet regulation concepts including self-regulation, co-regulation, government regulation and lastly the user education necessary to equip the Internet users.

The third review is on legislation and regulation of Internet in South Africa. Here the study discusses the policies, legislation and regulation that is in place currently internationally and locally in South Africa.

The fourth review is on censorship and content regulation in three countries which are United States, Sweden and China. These countries have been deliberately chosen to demonstrate the extent at which content regulation is applied. This section highlights countries that are more stringent in their regulations and those that are not.

The fifth review is on technology convergence. This section explains in more details what convergence is about and how it affects Internet regulation.

Lastly the study reviews the technical tools that can be deployed and used to prevent children from accessing harmful and illegal Internet content.

2.2 Risks of Internet that affect children

The risk of the Internet that affects children has been briefly explained in background of the study. In this section the study explains in detail the risks and harm related to online activities as articulated by Livingstone and Leslie referenced in UNICEF (2011). The Internet risks affecting children are categorized by the following; online harm from content, harm from content and harm from conduct.

2.2.1 Online harm from content

Online harm from content involves online pornography and child pornography. “Pornography is damaging to children because their immaturity prevents them from distinguishing between what they see in pornography and what actually happens in reality” (Preston, 2009). Online/Internet pornography is no different; the graphics on online pornography is far more striking than print or TV programmes. Online Sexual Exploitation (OSE) is defined by (Owolade & Snail, 2009) as any sexual related offence against anyone, especially children, directly or indirectly through Internet technology”. It is revealed that the average age of a child to be exposed to Internet pornography is 11 years and that the most alarming number of 90% of children has been exposed to Internet pornography while doing their homework (Longe, Chiemeke, Onifade, Balogun, & Otti, 2007). It is observed that most children do not deliberately search for these pornographic materials but it just pops up on their screens.

Furthermore in South Africa a survey to understand the exposure of children to sex material on Internet was conducted by the Film and Publication Board (FPB), it was reported that "… of the children who came across pornography on the Internet, 70% reported coming across such materials accidentally. More than half (60%) exchange addresses of pornographic websites with their friends" (Basson & Chetty, 2006), the survey also reflected that 14% of the children that are using chat rooms have had sexual advances made to them online (Owolade & Snail, 2009). Children are lured from social networks and chat rooms to have physical sexual encounters with the offenders.

Eberstadt and Layden (2010) articulate that there is evidence that children and adolescents use pornography to coerce each other into sexual behaviour, while adults also groom or coerce children by the same means. In their report Eberstadt and Layden (2010) also point out that more female adolescents tolerating emotional, physical, and sexual abuse in dating relationships, feel pressure to make out with females as a way to turn guys on, looking at or producing pornography so that their boyfriends will think they are 'open-minded' and 'cool,' and normalizing sexual abuse done to them because they see the same acts exercised in pornography."

A study focusing on juvenile sex offenders found that a disproportionate number of such offenders had been exposed to pornography as children; specifically, twenty-nine of the thirty juvenile sex offenders had been exposed to X-rated magazines or videos, and the average age of first exposure was about seven and a half years (Eberstadt & Layden, 2010).

2.2.2 Harm from contact

Harm from contact involves online sexual grooming. Online sexual grooming has the same characteristics of physical sexual grooming. The study will look at physical sexual grooming and then focus on online grooming to give a

comprehensive understanding of the topic. Minnie (2009) has a view that physical sexual grooming has five stages namely identifying and meeting the child, the friendship-forming stage, the relationship-forming stage, the molestation stage and finally, maintaining the victim and preventing disclosure. Research with abusers suggests that some have up to 200 young people on their online 'friends' lists who are at different stages of the grooming process at any given time (UNICEF, 2011).

In the first stage of identifying and meeting the child, the perpetrator will seek a place where they can meet the victim, sometimes physically in schools, malls or playgrounds; the second stage is that of friendship-forming where the perpetrator finds out what the child interests are, as well as likes and dislikes; in this case the person may try to play a counselling role by showing interest in the child's problems at home and school, thereby solidifying the bond of friendship (Minnie, 2009).

The third stage is relationship forming where the perpetrator may attempt to provide some emotional or material gain or reward that is of value to the child; their first physical contact with the child is often non-sexual touching designed to identify and test limits and to lower the child's inhibitions. This is the stage that usually the sex offender will introduce the element of secrecy into the relationship. During this stage the perpetrator might introduce pornography or sexually explicit material, as well as alcohol and drugs to the child (ibid).

Minnie (2009) explains that during the fourth stage of molestation the perpetrator through weeks, months or years of building up a superficially trusting relationship, the deception and manipulation finally pay off as they now progresses to actual sexual molestation. In the last stage of reinforcement and maintaining the victim, the grooming process does not

necessarily end, as the offender might wish to maintain further contact with the child to make sure the child remains silence about the abuse.

After a brief discussion of physical grooming the study looks at online grooming. It is understood by the study that sexual grooming can start online and end up with a physical contact. However online sexual grooming can also end up without physical contact where the perpetrator could still solicit images of a child through webcams.

Online grooming is defined by Webster, Davidson, Bifulco, Gottschalk, Caretti, Pham, & Grove-Hills (2010 p7) as “the process by which an individual befriends a young person for online sexual contact, sometimes with the involvement of webcams that can allow ‘sharing’ of the exploitation among networks of child sex abusers, and sometimes extending to a physical meeting to commit sexual abuse”. Online grooming typically happens in chat rooms, social networking sites and on instant messaging.

Staksrud (2013) articulates that there is a typical model of a grooming strategy that involves several phases. These phases are the introduction phase and the actual grooming phase. In his model Staksrud (2013) suggests that there will firstly be an introduction phase where the adult predator will start by observing, e.g. entering chatrooms as a silent non-participant, analysing the communication among other users, seeking to identify potential targets/victims so that he/she can engage in conversations with the identified target and seek to establish personal and preferably private conversations with the target.

The second phase is where the actual grooming takes place, a strategic communication, either with its final goal to meet the child and engage in sexual exploitation and/or sexual abuse, or as a goal in itself, through the

exchange of pictures, use of webcams, and explicit conversations. The grooming is intended to create a personal, trust-based relationship with the child. Children might be encouraged to place images of themselves that are of sexual in tone, which will then be followed by blackmail or threats of exposure to coerce teenagers to upload increasing numbers of explicit images (UNICEF, 2011).

2.2.3 Harm from conduct

This section explains several forms of harm by children. The first harm from conduct is cyberbullying. Like traditional forms of bullying, cyberbullying is when there is a deliberate and repeated aggressive behaviour by a person or group using websites, blogs, chat rooms, cell phones, instant messaging, and email with the intention of harming another person; this involves an imbalance of power that prevents the victim from challenging or ending the behaviour (Hoff & Mitchell 2009; UNICEF 2011). Bullies prefer the online method as they can remain anonymous and perceive that they will not be caught.

Cyber-bullies may post pictures of their victims online and write hate comments to embarrass them to their peers. They may also target an individual person and threaten them, making their victims to feel unsafe. This can go on for a long time before children report this to their parents or teachers. UNICEF (2011) articulates that in a research from Canada and the United Kingdom, children who are at risk of being bullied are mostly children who may be perceived to be different, such as minority ethnic groups, lesbian, gay, bisexual or transgender young people, overweight children, or those with perceived disabilities. These children are at greater risk of being bullied online than other children. Students who suffer this kind of abuse

have a negative psychological effect of anger, fear, powerlessness, depression and sadness (Hoff & Mitchell, 2009).

Cyberbullying for parents has not being as great of a concern as sexual harassment. The tragic suicide of Megan Meier, who was harassed and embarrassed through MySpace, raised awareness about cyberbullying that children need to be protected from it and it is now beginning to receive more attention (Miller, Thompson, & Franz, 2009).

Another form of harm by conduct is suicide. Internet websites and discussion forums have become an important and controversial source of information on the subject of suicide. A study by Biddle, Donovan, Hawton, Kapur & Gunnell cited in (Westerlund, 2011 p 765) indicated that “nearly 30 percent of search results for suicide-related words using different search engines consist of web pages whose content was dominated by information about suicide methods, and whose messages about suicidal acts ranged from incitement or clear encouragement to non-rejection”. These pro-suicide websites recommend suicide as a solution to life’s problems; they contain detailed descriptions of methods for achieving maximum effect, as well as suicide notes and pictures of people who have already committed suicide. Using persuasion and peer pressure to encourage suicide plans, they glorify those who succeed, giving rise to a new form of suicide pact: ‘net suicide’ (ibid).

The cases in Chapter 1 of sexual interaction, recording and dissemination of videos thereof are other examples of harmful behaviour by children. Another increasingly common behaviour by teenagers is ‘sexting’ (sharing of sexualized images or text via mobile phones).These images and text are often shared between partners in a relationship or with potential partners, but sometimes end up being shared with much wider audiences (UNICEF,

2011). Children may be harmful to themselves or other children knowingly and sometimes not knowing the consequences that come with it.

2.3 Concepts of Internet content regulation

Before the study can explore further the concepts of Internet regulation, it will first discuss what Internet content and censorship means and what needs to be regulated. The study will cover these definitions and thereafter discuss the concepts of Internet content regulation. The concepts discussed are self-regulation, government or public regulation and co-regulation or multi-stakeholder regulation.

2.3.1 Internet content regulation and censorship defined

Internet content regulation has been a topical issue since the mid-1990s with questions of whether the Internet should be regulated or not and how far should it be regulated. As Internet content has grown, so is the theory of Internet content regulation has developed. The study explores the difference between censorship and Internet content regulation; it is seen in other literature to be used interchangeably.

(Rose, 2011) describes censorship as the suppression of speech or other communication which may be considered offensive, harmful, sensitive, or inconvenient to the general body of people; this is usually determined by a government, media outlet, or any other controlling body. Furthermore (Rose, 2011) defines content regulation as basically a form of censorship to the extent that it is the regulation of any illegal or offensive content; this scheme of content regulation is designed to protect consumers and other citizens (particularly children) from exposure to inappropriate, illegal, or harmful material body. Exploring another definition of Internet content regulation (Commission of E-Business, IT and Telecoms, 2002) defines it as "… any

type of legislation by governments or regulatory authorities directed at censoring information and communication on the Internet based on its subject matter and controlling or attempting to control, access to Internet sites based on subject matter". The study adopts these definitions and will be using Internet content regulation and censorship interchangeably.

The Internet has variety of stakeholders pulling in different directions to protect their interest, those who make mega millions out of the Internet and those who are consumers with concerns of harmful content. This factor brings different arguments and perspectives on whether Internet regulation will infringe the right to speech. Another argument is that who is responsible for the well-being of children on the Internet. There is a collective view that this responsibility is shared among parents, societies, national and international governments.

One of the characteristic of the Internet's nature is to be boundary-less making Internet content regulation an international issue rather than individual countries. There must be consensus onto how to regulate the Internet.

2.3.2 What to regulate

Categories of Internet content need to be differentiated so as to understand what is being regulated. Content can be categorized as harmful or illegal, for example there is a difference between children accessing pornographic material (harmful) as opposed to adults accessing child pornographic material (illegal) (Akdeniz, 2001). Illegal Internet content is criminalized by national laws while harmful content is not. Meaning there is legal content that may offend others or that may be harmful to children. "These two categories of content poses different issues of principle and call for different legal and

technological responses" (COM (96) 487 cited in d' Udekem-Gevers & Poullet, 2001). In the forthcoming literature the study looks at specific International and South African legislation regarding the protection of children on harmful content but firstly the study discusses other concepts of Internet regulation.

2.3.3 Self-regulation

Self-regulation is when the private sector and other entities form common norms that are accepted by all stakeholders of the Internet. These norms are structured and included within the code of conduct also giving the means to enforce these rules (d' Udekem-Gevers & Poullet, 2001). Those who advocates for self-governance point out that one of its chief advantages is that the responsibility of regulation is with those who have the relevant expertise. A form of self-regulation is the establishment of hotlines that condemn certain activities contradicting the code of conduct for example online users could report child pornography (d' Udekem-Gevers & Poullet, 2001; Akdeniz, 2001). Another form of self-regulation is the formation of content monitoring and filtering schemes, developing "internationally compatible and interoperable rating and filtering schemes and measures to increase awareness of the possibilities available in choosing the appropriate content to parents, teachers, children and other consumers" (Akdeniz, 2001; Commission of E-business, IT and Telecoms, 2002).

Different initiatives of enforcing the rules have been the formation of "virtual magistrates" who are online arbitrators or mediators; where they are given the power to adjudicate on people's conflicts (d' Udekem-Gevers & Poullet, 2001). Furthermore d' Udekem-Gevers & Poullet (2001) also points out that the establishment of quality label mechanism is another form of self-regulation where the user is guaranteed a certain level of quality being given

by a website; these websites would for example be subjected to a press code.

The concept of self-regulation has had some challenges. Price and Verhulst (2004) articulate that the Internet makes it complex to understand what is included in self-regulation. The complexity is informed by the fact that the Internet industry is massive and that there is no single industry that can speak for the whole of the Internet. This difficulty in identifying a consistent self- governance structure has made it difficult to draft a broad series of guidelines that would apply across sectors and user-categories; therefore it became clear that a somewhat more detailed level of policing was required than what was possible under self-governance (ibid).

2.3.4 Government regulation

Public regulation can be the responsibility of the national government as well as international bodies. In this sphere caution should be observed in terms of freedom of speech. In South Africa the constitution outlines the rights to freedom of expression which is not taken lightly as the study has observed in the fore coming chapters. Internet regulation becomes a contentious issue as the government attempts to regulate Internet content.

Rose (2011) has broadly grouped the government policies concerning censorship and content regulation in four categories namely:

- Government policy to encourage Internet industry self-regulation and end-user voluntary use of filtering/blocking technologies.
- Criminal law penalties applicable to content providers who make content “unsuitable for minors” available online.
- Government mandated blocking of access to content deemed unsuitable for adults.
- Government prohibition of public access to the Internet.

It will be quite interesting to uncover the findings reflected in Chapter 4 of what policies has South Africa adopted.

The government's policies, law and regulations are tied to the cultural, political and economic contexts of that government (Hamilton, 2004; stated on (Dutton, Dopatka, Hills, Law, Nash, 2011)). Therefore government's policies are adapted to the circumstances of that country. Rose (2011) suggestion of self-regulation and end-user voluntary use of filtering technologies is important for the government to consider and implement, however this needs to be coupled with end-user education, including children as it is not sufficient alone. Furthermore the government need to incorporate the Internet children education into the curriculum to ensure Internet education is across all school and not only schools in the urban areas.

2.3.5 Co-regulation

Co-regulation or multi-sectoral governance is combining the efforts of all stakeholders which are not limited to governments, but include private groups including private companies, civil society - NGOs and consumer groups. Co-regulation was discussed intensely at the OECD Ministerial Conference on Electronic conference held in Ottawa on 7-9 October 1998 with the view that Internet content regulation cannot be done effectively without the combined efforts of both the private and public regulatory bodies. In order to fuse the responsibilities between public and private regulatory intervention, the "subsidiarity principle" should to be used (d' Udekem-Gevers & Poullet, 2001). Subsidiarity principle "is an organizing principle that says matters ought to be handled by the smallest, lowest or least centralized competent authority" (Carossa, 2003). This implies that the government's role should only play part where the private groups' initiatives are too enormous to be handled alone. This principle articulates that everything that

can be resolved by self-regulatory techniques must be solved by self-regulatory solutions (d' Udekem-Gevers & Poullet, 2001). Constant cooperation and dialogue between private and public regulatory bodies must be sort.

This principle is similar to what Stoker (1998) calls "light-touch approach" to regulation where the government is more of an enabler. Stoker describes governance as recognizing the capacity to get things done; which means governance does not rest on the power of government to command or use its authority. It sees government as able to use new tools and techniques to steer and guide.

Co-regulation also has its own challenges in that the different sectors usually have different set of priorities and goals. For example when it comes to an issue of privacy while all parties are clear in working together to ensure privacy, the private companies are likely to continue emphasizing profits while civil society groups would, in general, restrict profits in the name of greater individual rights. The State, too, has a somewhat difficult relationship to the private sector, particularly in many developing countries, where the individual rights have often just emerged from the shadow of heavy government regulation (wikibooks, n.d).

2.3.6 User empowerment concept

This concept has in its centre, the argument that individuals and parents are best suited to make decisions of what flows into their homes (d' Udekem-Gevers & Poullet, 2001). Parents and government both have a stake in the responsibility of children. Parents need to be made aware of the nature of risks and encouraged to improve their understanding of young people's online activities. A growing number of children are now creating and

exploring their own virtual social networks. This they do through online advertising, exposure to knowledge and information, and to political, religious, cultural or sexual ideas that may be in conflict with the view of their parents (UNICEF 2011); furthermore there are concerns that greater access and exposure to Internet can have harmful implications, including potentially diminishing parental capacity to understand children's experiences or to offer effective protection and support.

Historically in 1995 in the US there was a formation of a concept of parent empowerment as part of Internet governance; subsequent to that in June 1995 the 'information Highway Parental Empowerment Group (IHPEG) was formed by Microsoft Corporation, Netscape Communication and Progressive Networks to enable a system where parents can control what their children can have access to on the Internet (d' Udekem-Gevers & Poullet, 2001). Users especially parents, librarians and educators can configure their browsers and their search engines to avoid content they consider objectionable. This can be achieved by installing filters to block unwanted content and email (CDT, 2012). Assuming users are provided with notice and genuine choices, they can decide what software to download. They can install security software to protect against many forms of fraudulent behaviour.

There is a divide between Internet usage of children and their parents most especially in lower-income countries (UNICEF, 2011). A far-reaching response requires involving children by working directly with them in designing and implementation of information and protection strategies. Children and young people need information about risks and how to avoid them, and the mechanisms and pathways to follow if they find themselves in situations they judge to be suspicious. They need skills to make informed choices in their Internet activities and to provide each other with support

(UNICEF, 2011). This is increasingly important as Internet access becomes more private with children accessing Internet on their mobile devices.

2.4 Censorship and content regulation in United States, Sweden and China

As articulated in the aforementioned information, over the years as Internet became popular so has the issue of regulating its content accessed. Different countries have various viewpoints on how to regulate the Internet but the common theme is that most countries do not want to allow people to obtain illegal material on the Internet and they do want to protect minors from materials that are classified as harmful or unsuitable (Rose, 2011).

In this section, the study explores literature on Internet content regulation in the United States, Sweden and China. These countries have been deliberately chosen to demonstrate the different types of content regulation they have applied. The United States is regarded as a 'nanny state', while Sweden is regarded as 'laissez faire' that promotes self-regulation. China on the other hand is regarded as the more restrictive or authoritarian. This comparison gives a picture of the different types of Internet content regulation which is important to the study so as to determine the type of Internet regulation that South Africa has employed.

2.4.1 Content regulation in the United States *(Nanny State)*

The history outlined in this section gives a perspective of why the United States is called a nanny state. The nanny state is defined as a government perceived as having excessive interest in or control over the welfare of its citizens especially in the enforcement of extensive public health and safety regulations; the United States is regarded as a nanny state (Snyder, 2012).

Content regulation fall under the jurisdiction of the Federal Communications Commission which was created with the enactment of the Communications Act of 1934 (Rose, 2011). Then in 1996 the Telecommunications Act of 1996 was passed which was the first major overhaul of the United States' telecommunication law in over six decades; it opened up the market for competition and improved interconnectedness, the Act removed unnecessary regulatory barriers for entry in the market (ibid).

The Communications Decency Act (CDA) of 1996 was the first notable attempt by the United States Congress to regulate pornographic material on the Internet (Kende, 2008; Rose, 2011; Esposito, 1998). However the Act was challenged in the Reno v ACLU case where the court found the CDA to be unconstitutional and that it can drive out businesses of some non-profit sites that cannot afford age verification methods; According to the court CDA was vague and over the scope (Kende, 2008). In his article Kende (2008) mentions that the court's view was that Internet was not dangerous because it allegedly requires affirmative steps to gain access such as passwords; on top of that the Internet allegedly has warning pages that keep minors from serious adult content.

The Child Online Protection Act (COPA) of 1998 was a law put in place to restrict minors from accessing material that was deemed to be harmful to them and to address the vagueness of CDA by establishing a three part Millers' obscenity test. The Miller test is the United States Supreme Court's test for determining whether speech or expression can be labelled obscene, in which case it is not protected by the First Amendment to the United States Constitution and can be prohibited. The first two points of the Miller test are held to the standards of the community, and the last point is held to what is reasonable to a person of the United States as a whole. The national reasonable person standard of the third point acts as a check on the

community standard of the first two points, allowing protection for works that in a certain community might be considered obscene but on a national level might have redeeming value.

Miller's obscenity test applied to "for profit" entities and also covered websites (Kende, 2008; and Rose, 2011). However, the law did not take effect as a permanent injunction was put in place because it was deemed to be violating both the first and fifth amendments (Rose, 2011). The law to correct this was then established which was The Children's Internet Protection Act (CIPA); CIPA requires schools and libraries using the E-Rate discount to employ filters to prevent minors from accessing material deemed obscene, child pornography, or harmful to minors (ibid). Table 1 summarizes the United States law discussed above.

There have been events in the United States such as Wikileaks that has caused a stir on the usage of the Internet. Documents that are considered classified and confidential in the United States were leaked by Private Manning to Julian Assange, the owner of Wikileaks as reported by Poulsen & Zetter (2010). In another event in February of 2011, Secretary of State Hilary Clinton voiced her opinion that citizens should have the right to use Internet for freedom of speech and be able to explore the Internet without limitations. However, she then further expressed that the Internet should be secured from "Countries or individuals that engage in cyber-attacks. The abovementioned facts indicate that United States has evolved in the attempt to prevent harmful Internet content for a long time, it shows how the government of the United States has continually tried to regulate the Internet with other cases laws declared unconstitutional and still continuing to bring new laws of Internet regulation. This is regarded by others as being the government being excessively controlling.

Table 1: Summary of the history of legislation of censorship in the United States

Name of Statute	Effect	Year
Communications Act	This Act created the Federal Communications Commission (FCC) for the purpose of federally regulating interstate and foreign commerce in communication via telephone, telegraph, television, and radio. The Act replaced the Federal Radio Commission and the Interstate Commerce Commission.	1934
Telecommunications Act	First major overhaul of United States telecommunication law and amended the Communications Act of 1934. Objective was to open up markets to competition by removing regulatory barriers.	1996
Communications Decency Act	First attempt by the United States Congress to regulate pornographic material on the Internet. Act is Title V of the Telecommunications Act of 1996. Anti-indecency and anti-obscenity provisions were made to the Act.	1996
Child Online Protection Act	Purpose of the Act was to restrict access to minors to any material defined as harmful to such minors on the Internet. The law never took effect as it litigation led to a permanent injunction against the law in 2009	1998
Child Internet Protection Act	This is a later version of the Child Online Protection Act designed to prevent minors from accessing harmful material on the internet. It was signed into law on December 21, 2000 and upheld by the Supreme Court on June 23, 2003	2000

Source: (Rose, 2011)

2.4.2 Content regulation in Sweden *(Laissez faire)*

Another word for laissez faire is self-regulatory. Sweden is considered to be one of the leaders in terms of technological innovation, as well as in progressive policy-making, regulation and Internet freedom; it was ranked first among 61 nations, as the nation where the internet has the most significant political, social and economic impact in the World Wide Web Foundation's 2012 Web Index (Münch, 2013). In terms of policy making

Sweden is considered to be free and neutral. Sweden does not have policies requiring schools to electronically filter access to the Internet although local school authorities can approve filtering content. Filtering the Internet is seen as a form of censorship; and censorship is not something that is generally supported by the public (Moyle, 2012). The country encourages educators to use social networking sites in ways that model safe and appropriate online behaviour; with the emphasis on the concept of teachers building 'trust' with their students to emphasize the development of students as creators of knowledge rather than simply consumers of information (Downes, 2007 cited on (Moyle,2012)).

Sweden also experienced challenges while trying to implement some sort of censorship. When they were implementing Intellectual Property Rights Enforcement Directive (IPRED), the Swedish government in addition passed a legislative package that would grant the national defence radio establishment (Försvarets Radio Anstalt - FRA) extensive surveillance power over online activities, in an effort to combat 'external threats' (Münch, 2013). The laws gave the national defence intelligence agency the authority and ability to monitor all cross-border cable-based communication (phone-calls, e-mails and other Internet traffic, etc.) without a warrant - including the traffic's content - far exceeding the scope of surveillance allowed within the EU. Landes (2009) articulates that the NGOs, such as the Swedish Justice Centre and the Norwegian division of the International Commission of Jurists (ICJ), had then argued that the law violates Article 8 and Article 13 of the European Convention on Human Rights, as well as article 12 of the Universal Declaration on Human Rights, which guarantee citizens the right to privacy and their ability to hold authorities accountable for potential human rights violations.

Similar to the challenges mentioned above Moyle (2012) describes a situation where Sweden was implementing a centralised block-list which was the object of controversy. The list is issued by the authorities and subsequently implemented by ISPs by means of an automated DNS-filter, with the intention to block access to sites hosting child pornography. Moyle (2012) articulates that critics, such as internet researcher Marcin de Kaminski from the Sociology of Law department at Lund University, questioned the fact that the maintenance of the list was not transparent and that there is no third-party control of the lists content; neither is there a way to legally appeal a list entry. Amongst other things this means that the selection of sites listed may be arbitrary in some instances and that without further checks and balances the list may become a political play-ball.

The above illustrates the involvement of the public sector in legislation pertaining to censorship. Overall Sweden promotes self-regulation of Internet content.

2.4.3 Content regulation in China *(Authoritative)*

While Internet use and development was one of the most important inventions in the second half of the 20th century, China's internet use and development began a decade later after its economic reforms. Its Internet use and development grew exponentially and had outpaced other countries; by 2008 China replaced the United States as the largest Internet user of the world (Liang & Lu, 2010 and Fong, 2012). China's Internet development came with the government's tight control and regulation over Internet infrastructure, its commercial and social use, and its potential political ramifications (Liang & Lu, 2010).

The great firewall which is the predominant method of control at the infrastructure level is the restriction of access to Internet information (e.g., regulating access and content, monitoring Internet use). Liang & Lu (2010) articulate that at the national level, only government-approved agencies and businesses are permitted to establish an Internet Interconnecting Network or backbone network and to license the operation of Internet service providers at the next tier. Liang & Lu further says that the Internet service providers required to go through international gateways located in Beijing, Shanghai, and Guangzhou and are subject to governmental control and regulation; then at the next tier, all private Internet service providers are licensed through one of these Internet Interconnecting Networks and are required to install filters to block away undesirable content.

The bottom tier involves Internet users who are required to register with Internet service providers to gain Internet access. Rose (2011) articulates that in 2009, the Chinese government had required every computer sold to pre-install “Green Dam Youth Escort” software that is designed to prevent minors from harmful materials; furthermore when riots occurred in XinJiang Province of China, the government turned off the Internet for almost a year, which not only prevented citizens from communicating but prevented rioters from sharing information about where and when protests took place. These facts indicate the strict measures that China’s undergoes to censor their internet content.

2.5 Technology: A challenge to Internet regulation

Technology is one of the biggest factor that affect the validity and sustainability of policies, legislation and regulation. In this section the study explores the challenges that technology brings to Internet regulation.

2.5.1 Technology Convergence

As already articulated in the study, in the past years regulation was based on both telecommunication, which includes electronic systems used for communication between individuals or groups and broadcasting, which included creating audio and video program content and distributing it to the mass audiences of radio, and television separately. IT services which refers to hardware and software used to store, retrieve, and process data were not regulated. Presently these boundaries have become increasingly indistinguishable because of technology convergence. It is imperative for the study to understand this concept as it impacts Internet regulation and how consumers consume ICT services.

Convergence relates to the tendency of different technological systems to develop towards performing similar tasks; it means that a single infrastructure can provide a collection of content or services; that a single service-provider can provide multiple services, or that content can be aired to multiple platforms (RSA, 2014). As a result of this technology convergence, industries are adapting and new industries are emerging to deliver enriched user experiences for consumers, enterprises, and the private sector (Huang, Guo, Xie, & Wu, 2012). For example, newspapers now offer both audio and visual content online, and the major broadcaster are now offering textual services online.

2.5.2 Factors that affect rapid technology convergence

There are several factors that are driving technology convergence, which are cloud, broadband, and device technologies. Cloud, in its simplistic term means storing and accessing data and programs over the Internet instead of your computer at home or a server at work (Griffiths, 2013). Another

definition given by RSA (2014) describes cloud computing as storing, processing and use of data on remotely located computers accessed over the internet. It involves sharing computer resources, thus giving users unlimited computing power on demand and accessing their data anywhere through the Internet. The user can access all cloud services without making major capital investments. On the other hand the sharing aspect of the cloud computing allows cloud service providers to spread their development and maintenance costs over many users, resulting in lower costs and better service quality compared to on-premises IT services.

Broadband is another factor that affect the rapid technology convergence. Cloud services requires a lot of bandwidth for users to be able to access and store data in remote computing devices. This is where broadband plays a major part. (Huang, Guo, Xie, & Wu, 2012) articulates that more than 50 countries have invested in national broadband projects that lay solid foundations for bandwidths adequate to drive ICT convergence. In South Africa the implementation of undersea cables including Seacom, EASSy, TEAMs, WACS, Main one and ACE as well as the Broadband policy are fundamental in proving broadband access.

The last factor that affect rapid technology convergence is the devices. There are many devices that accesses the Internet including smart phones, tablets, laptops, and wi-fi devices which allow users to send and download music and images, to use the Internet to purchase products, and to pay retailers and financial institutions electronically among other things. These devices enable users to use the cloud anywhere they are situated making it a preferable way of using the Internet.

2.5.3 Convergence in policy and regulation

Technology convergence is of particular interest to policy makers and regulators as it changes the nature of services, allowing an operator who was licensed under one category to be able to do things that would have required different category licences in the past. This is seeing as corporate convergence where a single company can provide mobile services, broadband, digital television, cloud, tablets and new media technologies whereas traditionally there would be a separation between broadcasting and telecommunication companies.

As articulate in RSA (2014) current policies and law are based on a traditional structure that was premised on distinct broadcasting, telecommunications and IT markets. These markets were based on the existent of distinct industries around telephony, point to multipoint broadcasting services, and mobile telephony services. Presently there are still separate policy and regulatory approaches for broadcasting, radio-based communications and telecommunications and they do not take into account the changes that have taken place.

2.6 Technical tools to prevent harmful and illegal content

This section looks at the technical tools that can be deployed and used to aid in preventing harmful internet content to be accessible to minors. The tools that are mentioned in this chapter are not comprehensive; therefore there might be other tools that are not mentioned below.

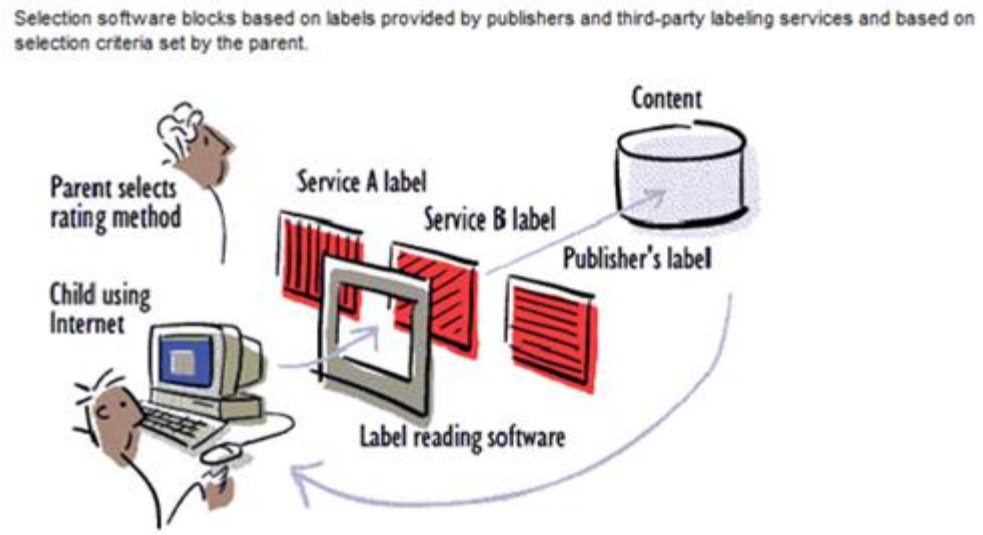
At the entry point of the technical tools filtering can be based on ratings (labelling) and/or on classification into uniform resource locator (URL) lists (d' Udekem-Gevers & Poullet, 2002). Classified URL list consist of all blacklisted

or “Not for children” URLs. In this study rating and classification refer to the same concept. Platform for Internet Content Selection (PICS) is a commonly used rating system that allows users to choose label source independently of their filtering software (ibid). A label is described as “… either a single document or a group of documents” that can be named with a URL including FTP and Gopher (Resnick & Miller, 1996). Labelling can be done by a content provider or by a third party. If the content is not labelled, parents can prohibit access to the content. Figure 3 illustrates how labelling can allow only labelled content. Furthermore Watney (nd) articulates that the filtering technology distinguishes between filtering options for end users and filtering options for non-end users; where end users filters may be utilised to block access to content on particular websites. Filters may also be used to deny access to interactive sites (such as e-mail and chat rooms), Usenet newsgroups, file downloading, and peer-to-peer connections.

Another tool suggested by (Preston, 2009) is called Internet community ports concept. This mechanism allows parents and schools to choose what their community is exposed to by choosing the zone they would like to belong to. In this concept the user purchases community ports service where Internet content is sorted according to what the user chooses. This means that anyone who does not choose anything is purchasing all ports on the Internet. The Internet has got over sixty five thousand ports but there is a few that are used the usual being port 80 (Preston, 2009). Age appropriate content can be channelled through other free ports thereby being specific to a certain community (family orientated content). This concept will not work without being backed up by law. Therefore there should be law that imposes civil and criminal penalties against a person who has placed inappropriate content on the Community Port. (Preston, 2009) suggests that in this way parents can lodge a civil case against an individual or group who contravene such a law.

There are many filtering tools in the market and there is no perfect one. Therefore “no particular technology or method provides a perfect solution, but when used in conjunction with education, acceptable use policies and adult supervision, many technologies can provide improved safety from inadvertent access from harmful to minors materials” (Commission on Child Online Protection, 2000 cited in d’ Udekem-Gevers and Poullet, 2002).

Figure 3: Filtering mechanism



Source : Resnick & Miller (1996)

2.7 Conceptual framework

The study has discovered that the literature and facts gathered to understand harmful and illegal Internet regulation are all encompassed in Lessig’s 1998 model of Internet regulation. Therefore to present these concepts in a more systematic format the study has derived the conceptual framework from Lessig’s 1998 model of Internet regulation.

Bercowitz, Madsen, & Wulff (nd) describes Lessig’s 1998 model of Internet regulation in four modes of regulating behaviour in the physical world; which

can be applied to the Internet. In his model Lessig describes the major forces that allows regulation of the Internet as social norms, the market, the architecture and the law. According to Lessig's 1998 model of Internet regulation law regulates by sanctions imposed ex post for example if someone steals a car, they are likely to go to jail. Law what regulators use.

The second mode of regulating behaviour is the social norms. Social norms also regulate; they are the understandings or expectations about how someone ought to behave. This is enforced not through some centralized norm enforcer, but rather through the understandings and expectations of just about everyone within a particular community (Bercowitz et al, nd). Examples of norms would be what clothes to wear when going to an interview.

The third mode of regulating behaviour is the market. The market regulates by price. The example of a market is that it limits the amount that someone can spend on clothes; through the device of price, the market sets opportunities, and through this range of opportunities, it regulates.

Lastly the mode of regulation is the architecture. The architecture force is described by Lessig as the basic constraints of the world; in the physical world we often overlook architecture since it is largely fixed. The example is that there is no need for regulation that prohibits one walking through a locked door. However, in the virtual world it becomes more fluid where some networks requires identity authentication while other allows anonymity (Bercowitz et al., nd). The study will regard architecture as technology.

Based on Lessig's 1998 model of Internet regulation the study has derived four factors that will effectively relate harmful and illegal content namely legal (policies, legislation and regulation); economic (price); social (government, parents, schools, etc); and technology (convergence) as depicted in Figure 4

below. The factors of effective governance work as a collective; none of the factors below will achieve effectiveness individually without the others. The factors of this conceptual framework are discussed individually below.

2.7.1 Legal factors

The legal factors governing the Internet is policies, legislation and regulation. The legal factor allows for the protection of children in ex-ante and ex-post. Ex-ante laws are represented by laws such as but not limited to the Films and Publications Act 65 of 1996; this Act classifies content of films and publications so as to prevent the adult classified content to be exposed to children. Broadcasters are able to then warn the viewers of the classification of movies in the event of broadcasting and they broadcast adult content movies at the certain time of day which is at night. Ex-post laws are represented by laws such as but not limited to the Sexual Offences Act, No. 32 of 2007; this law provides for the recourse of those who has been sexually violated including finding guilty those who have committed the sexual act to children.

This factor assures that the perpetrators of online grooming and child pornography can be prosecuted and be jailed. It also allows for the person who feels harassed to get a restraining order against a harasser in terms of parents protecting their children from such interactions. Internet is boundary-less meaning a website situated in another country can be accessed by South African children. Jurisdiction laws plays a very important part on the Internet. South African laws allows for its courts to have jurisdiction in other countries where the perpetrator is a South African or where the perpetrator has committed crime in South Africa.

2.7.2 Social factors

Social norms guide behaviour and therefore function as a factor that affects the effectiveness of regulating harmful and illegal Internet content. Lessig (1998) is quoted by Bercowitz et al (nd) as articulating that regulation is ineffective if nobody is willing to enforce it. As the example given above where it is considered harsh to use capital letters in an email, the person receiving the email can be offended and raise it with the sender of the e-mail.

The social factor comprises all the stakeholders of the Internet which includes children, parents, teachers, caregivers, schools, government agencies including policy makers and regulators, and non-profit organizations, Internet and Content service providers, mobile companies and how they behave. The service providers normally subscribe to code of conduct in the representative body that they have affiliated to. For credibility of these organizations the ECT Act of 2002 provides the representative body must be capable of monitoring and enforcing its code of conduct. Parents as well as teachers has a role to play in laying the foundation of discipline to children. An example is when parents monitor what the children accesses on the Internet by installing filters on the computers at home and also restricting access on the Internet at unsupervised times, the same goes for teachers.

The vulnerability of children in the Internet needs to be mitigated by all stakeholders working together. Not only is it a responsibility of parents and government to protect their children but that of other Internet stakeholders such as Internet service and content service providers. These providers needs work to put measures in place such as but not limited to educating users of the Internet risks affecting children.

2.7.3 Economic factors

Economic factors plays equally important part of regulating harmful and illegal Internet content. Price is of access to broadband and prices on cell phones and other devices plays a role in regulating who accesses the Internet. The prices of cell phones have dropped significantly and therefore the study can see more proliferation of these devices. Furthermore ICASA is forcing mobile service providers to cut termination rates, this will bring prices of communication down from a user perspective. Government has universal access policies and initiatives to bring computers at schools and provide for discounts on broadband access. Therefore these initiatives encourage more Internet penetration.

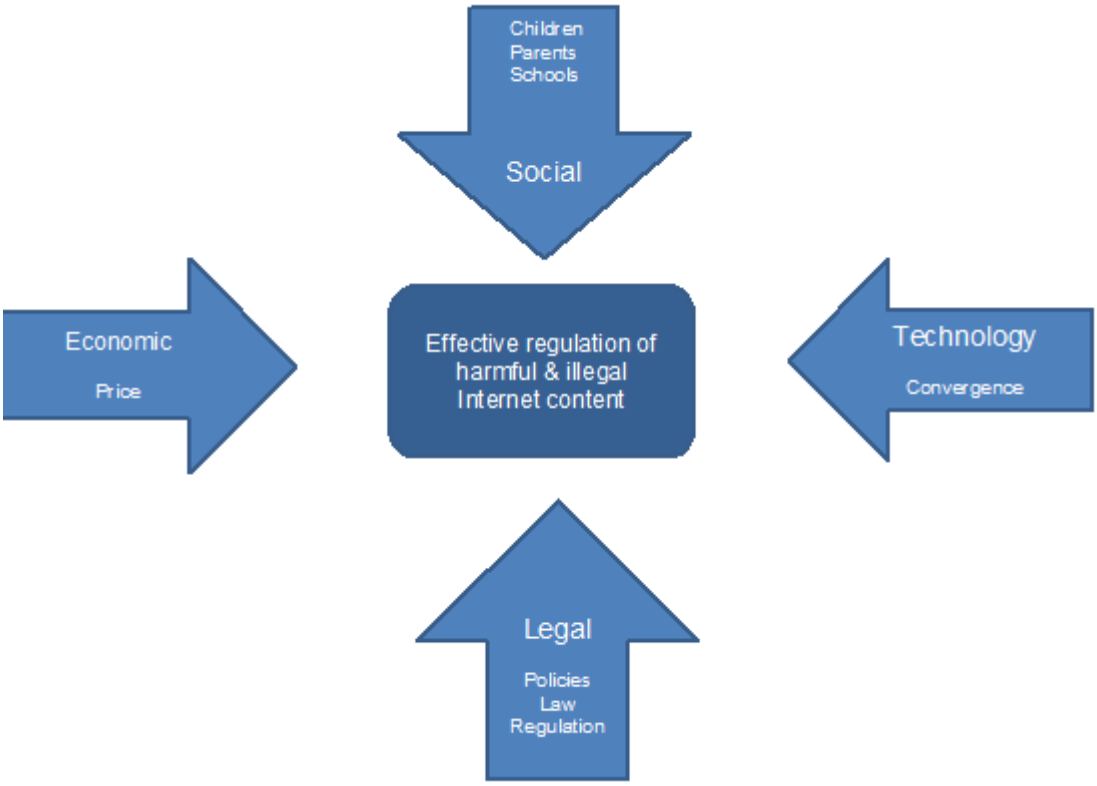
It is to be noted that the study will not use the economic factor in its data analysis as requires an in-depth understanding of price regulation which is beyond the level of detail required to understand the foundational policy and regulatory issues.

2.7.4 Technology factors

Internet has evolved dramatically in the past years. Devices that access Internet has increased, mobile phones taking the lead in these devices as they became cheaper with time. Although mobile phones started being used primarily for voice calls nowadays it is also used for several activities including text messages, sharing pictures and video clips, e-mail, for chat rooms, instant messages, accessing of websites and blogs, and social networking sites or applications. This convergence complicates the regulation of sectors that were separate which now can provide all services which traditionally could not provide. This evolution has caused gaps in the policies and regulation. The Internet is so dynamic which requires dynamic

laws and regulations as well as dynamic Internet safety education as and when the changes happen.

Figure 4: Effective regulation of harmful and illegal content



2.8 Conclusion of the literature review

This chapter reviewed the literature on risks of Internet that affect children. The study has highlighted few of these hazards which are online pornography, cyberbullying, online sexual grooming and harmful behaviour by children. It is imperative that these issues are not taken lightly and that all stakeholders with interest Internet and children work together to prevent these issues that affect children. These issues are not only South African issues but also involves the international bodies; therefore international collaboration is of paramount importance to put prevention measures in place.

The chapter also reviewed literature on the concepts of Internet content regulation and addresses the different methods of content regulations. This brings to light the fact that not every content that is harmful to children is illegal. This section gives an understanding of Internet content regulation together with legal and illegal content. It highlights the types of Internet regulation that is self-regulation, government or public regulation, co-regulation and a few countries were reviewed to check what they have opted for one of these regulations according to how they approach content regulation..

Technology convergence was covered to give an understanding of the challenges that the policy makers have to deal with and that adaptation of the legislation and regulations need to occur as technology changes. The technical tools to be used to filter Internet content were also covered to give perspective of parents and children can use to minimize access to harmful content.

Lastly this chapter presented a conceptual framework that was used by the study to investigate the effectiveness of the policies, legislation and regulations. It provided for four factors that affect which were legal, social, economic and social factors. The research design and methodology that this study engaged is presented in the following chapter.

Chapter 3: Research methodology pertaining to harmful and illegal Internet content

3.1 Introduction

This chapter focuses on the research methodology and design of this study. Data collection and analysis are also discussed in this chapter. The research question and its sub-questions will be examined in this chapter. The research methodology to be conducted is qualitative research. The purpose of this research is to examine the effectiveness of the South African regulation and legislation with regard to Internet content today. The data collection methods used will include semi-structured interviews as well as document analysis. Semi- structured interviews will be conducted to gather the understanding of the stakeholders of the Internet in South Africa while document analysis will be used to focus on examining the legislation and regulations that addresses internet content. Furthermore document analysis will be used on published academic research reports of events that occurred pertaining to the Internet risks affecting children; this is so that the study can have perspective of what children encounter.

3.2 Research Problem

It is quite clear that there are benefits for children to have access to the Internet including being able to do research and school work, socializing with their peers on social network and being able to communicate worldwide and share information. With all these benefits in mind one of South Africa's national priority is to enable all South Africans to have access to electronic communications including the Internet. With this access South Africa will benefit from economic development and growth which will enable other social benefits as envisaged in the Broadband Policy (RSA, 2010) and the amended Broadband Policy (RSA 2013).

However it is equally disturbing to realize how vulnerable children are on the Internet platform including but not limited to cyberbullying, online pornography and child pornography, self-harming websites, online grooming and innocently exposing personal information that will be used for criminal activities. Therefore it is imperative to ensure that children are protected from harmful and illegal Internet content and most of all from paedophiles that are scouting them on the Internet. Mobile devices are increasingly the choice for accessing the Internet as compared to the personal computers at home and at school. This among others reasons is because the net can be accessed anywhere and at any time of the day. This defeats the measures of monitoring and filtering harmful and illegal Internet content at home.

While there is literature on how other countries are regulating Internet content, it is not clear whether South Africa is effectively addressing illegal and harmful Internet content. South Africa cannot regulate Internet content in isolation; it will need to coordinate its efforts with the international bodies to ensure a united approach that is aligned with international standards.

3.3 Purpose statement

The purpose of the study is to explore the South African policies, legislation, and regulation that addresses the harmful and illegal Internet content affecting children. Thereafter the study will analyse the effectiveness of the policies, legislation, and regulations concerned in order to conclude on the findings of the study.

The study will firstly investigate by analysing the existing legislation and regulations that governs illegal and harmful Internet content in the present era of technological innovation to determine if it is relevant and indeed addresses the harmful and illegal Internet content. Secondly the measure of

effectiveness will be achieved by critically examining statistics from published academic research reports on the events that occurred where children were subjected to the Internet risks, and lastly use interview findings to understand the perspectives of the subject matter experts with regard to the topic at hand.

The outcome of the research is to explore any evidence that suggests the effectiveness of the legislation and approaches. Where there are gaps, the study will attempt to identify and suggest best practice approaches for effective legislation and regulation on harmful and illegal Internet content affecting children.

3.4 Research questions

The main research question for this study is as follows:

> To what extent does South Africa's legislation and regulation address illegal and harmful Internet content relating to children?

In order for the researcher to answer the main question, the following sub-questions will be answered using the adapted model from Lessig's 1998 model of Internet regulation:

1. To what extent does the policies, legislation and regulations address cybercrime affecting children? (*legal*)
2. How do various technologies, particularly mobile affect Internet content regulation? (*technology*)
3. What are the roles of the Internet stakeholders in relation to Internet content regulation? (*social*)

4. What lessons can we learn from particular cases of Internet abuse affecting children? (*social*)

3.5 Research methodology

The study will use a qualitative research methodology. The goal of qualitative research is defined as describing, understanding or explaining human and institutional behaviour. The researcher endeavours to have an understanding for events, actions and processes in the context of their natural setting as described by (Babbie & Mouton, 2001). Merriam (2009) also articulates the same fact by explaining that qualitative researchers are more interested in understanding the meaning people have constructed, that is, how people make sense of their world and the experiences they have in the world. Cresswell (2003:199) also adds to the definition of qualitative research and articulates that fact that the researcher is the primary instrument in data collection rather than some inanimate mechanism; that the data that emerge from a qualitative study is reported in words rather than in numbers and lastly that the focus of qualitative research is on participants' perceptions and experiences. Qualitative research methodology is appropriate for this study as the research questions requires an analysis of the processes and regulations and lastly the social context with respect to Internet multi-stakeholder relationships and exposure of children to harmful and illegal content.

3.5.1 Interpretive Approach

The study is using an interpretive approach. Neuman (2011 p88) defines interpretive approach as a systematic analysis of socially meaningful action through a direct detailed observation of people in natural settings in order to arrive at understandings and interpretations of how people create and

maintain their social worlds. Babbie & Mouton (2001 p28) explains the interpretive approach as understanding people not primarily as biological organisms by firstly and foremost as conscious, self-directing, symbolic human beings. These two definitions of interpretive approach fits the study being conducted as the main aim is to understand and interpret how behaviour can be regulated in the Internet environment. This approach evaluates reality according to how people who experience it on an ongoing basis understand it (Babbie & Mouton, 2001, p. 29). It is therefore associated with qualitative methods that seek to understand rather than measure.

3.6 Research design and population

The function of a research design is to ensure that the evidence obtained enables us to answer the initial question as unambiguously as possible. Leedy and Omrod (2004) describe a range of research designs namely case study, ethnography, phenomenological study, grounded theory study, and content analysis. It is essential that the correct research design is chosen to ensure it answers the research problem or question at hand (Babbie & Mouton, 2001).

The research design for this study is phenomenological study. Welman and Kruger (1999, p. 189) cited in (Groenewald, 2004, p. 5) articulates that “the phenomenologists are concerned with understanding social and psychological phenomena from the perspectives of people involved”. The study more closely displays the characteristics of a phenomenological study, where the researcher tries to understand the “perceptions, perspectives, and understandings” of the Internet stakeholders and then after the policies, legislation and regulations; with this understanding the research is able to determine and then conclude on the effectiveness of the policies, legislation and regulations that relates to harmful and illegal Internet content.

3.7 Data collection and analysis

The data collection will be conducted using two sources of data which is primary and secondary. The primary data relies on interviews that will be conducted to generate ideas that will form a natural setting, face-to-face or telephonic. The secondary data relies on the important documents accessed through libraries and resource centres such as the legislation, published academic research reports, policies, corporate reports and industry websites. The combination of methodologies in the study of the same phenomenon which in this case is qualitative methodology is called triangulation (Denzin, 1970, referenced by Bowen, 2009). By triangulating data, the researcher attempts to provide 'a confluence of evidence that breeds credibility' (Eisner, 1991 referenced by Bowen, 2009). By examining information collected through different methods, the researcher can corroborate findings across data sets and thus reduce the impact of potential biases that can exist in a single study. These two data collection methods are discussed below:

3.7.1 Document analysis

Firstly the researcher started with Document analysis. Document analysis was used to interrogate the legislation and regulations that govern the Internet content and are related to children protection. The legislation that was examined are Electronic Communications Act No. 36 of 2005, Children's Act 38 of 2005, Sexual Offences Act 23 of 1957, as amended, Films and Publications Act 65 of 1996 as amended, and the ICASA amendment Act 3 of 2006. In the process of analysis other legislation that were deemed necessary to be examined were The Protection of Harassment Bill, Information society and development Plan, Broadband Policy of 2010 and Broadband Policy of 2013, and Internet and Cellphone Bill of 2010. This helped the researcher to gain more insight into the subject matter before conducting interviews. It was imperative that the researcher is

knowledgeable about the subject matter before proceeding to the interview data collection method. The study will highlight both the significance and the weaknesses of the legislation and regulations that South Africa has at present. As discussed in the study, technology has advanced in a rapid manner which requires the legislation and regulation that governs this technological environment to evolve and be updated at the same time.

The researcher also used document analysis to determine the effectiveness of the said legislation by interrogating the surveys, and published academic research reports that reflect indicators for statistics such as the number of cyberbullied children, the number of children that has sexually being groomed on the Internet, number of children that accidentally stumble on pornographic materials on the Internet, the awareness of parents and family and statistics about Internet safety education.

Bowen (2009) defines document analysis as a systematic procedure for reviewing or evaluating documents that are both printed and electronic material. Document analysis requires that data be examined and interpreted in order to elicit meaning, gain understanding, and develop empirical knowledge (Corbin & Strauss, 2008; Rapley, 2007). There are advantages and disadvantages of using document analysis, the study explores them below:

3.7.2 Advantages and limitations of document analysis

Document Analysis is efficient as it consumes less time than the other research methods, it requires data selection, instead of data collection. Documents are available in the public domain and are more accessible on the Internet. Document Analysis is also cost-effective as it is less costly than other research methods because the data contained in documents have

already been gathered; what remains is for the content and quality of the documents to be evaluated. Document analysis is stable because the researcher's presence does not alter what is being studied (Merriam, 2009); therefore documents are then suitable for repeated reviews. Documents also provide broad coverage; they cover a long span of time, many events, and many settings (Yin, 1994).

Document analysis also has its limitations. Documents are produced for some purpose other than research; they are created independent of a research agenda; consequently, they usually do not provide sufficient detail to answer a research question. Yin (1994) has articulated that access to documents may be deliberately blocked making it difficult for the researcher to retrieve them. Another important limitation of document analysis is biased selectivity; this means that an incomplete collection of documents suggests 'biased selectivity'. These are potential flaws rather than major disadvantages; given its efficiency and cost-effectiveness in particular, document analysis offers advantages that clearly outweigh the limitations (Bowen, 2009).

3.7.3 Semi- structured interviews

After doing thorough document analysis, the researcher will proceed with interviews to investigate the role of the different stakeholders in Internet content regulation. Babbie (2001) suggests that interviews should be used as the primary source of data collection for qualitative research methodologies as they generally produce fewer incomplete answers. The study is interested in the interviewee's point of view therefore qualitative research interview will be conducted. Qualitative research interview seeks to cover both a factual and a meaning level, though it is usually more difficult to interview on a meaningful level (Kvale,1996). (Maree, Creswell, Ebersohn, Eloff, Ferreira,

Ivankova, Jansen, Nieuwenhuis, Pietersen, Plano Clark, & van der Westhuizen, 2007) defines interviews as “a two-way conversation in which the interviewer asks the participant questions to collect data and to learn about the ideas, beliefs, views, opinions and behaviours of the participant”. Semi-structured interview method will be used. In the semi-structured interviews the participants may propose solutions or provide insight into events, but their focus is mainly on their own perceptions of the event (Maree, 2007).

When choosing interviewees, the researcher considered a sample that best represents the diverse Internet stakeholders. The population to be interviewed is listed in Table 2 below. The interviewees were selected to give different perspectives of the subject matter, this was determined as follows: Regulator A (13/01/2014) of ICASA gave perspective as a policy maker of the challenges encountered in formulating the regulation and regulating harmful and illegal content; Regulator B (13/01/2014) of Films and Publication Board gave similar perspective as ICASA on its challenges. Policy maker A (14/01/2014) of Department of Communications gave perspective of how Internet risks affect children at school and to understand measures in place to prevent these risks; Policy maker B (31/01/2014) gave perspective of how schools are involved in the curbing Internet risks and how Internet policies, legislation and regulation are received and used in school. Service provider A (16/01/2014) of Telkom Internet gave perspective as an Internet Service Provider of the responsibilities they hold as a Service provider to prevent access to harmful and illegal Internet content as well as to understand if there are any strides made to combat this content; Subject expert A (16/01/2014) of Snail Attorneys @ Law Inc is a subject matter expert in the field of the Internet law, the respondent gave perspective in what the policies, law and regulations provide and to identify the gaps. Subject expert B (20/01/2014) of Convergence Partners is also a subject

matter expert in Internet law and gave similar perspective as Respondent G (16/01/2014). Subject expert C (03/02/2014) of Mxit together with Subject expert D of Childline (04/02/2014) gave perspective of what children experiences in the Internet in their daily lives.

3.7.4 Advantages and disadvantages of interviews

The advantage of the semi-interview method is that the interviewer will be able to probe deeper into the response given by the respondents which will allow the interviewees to be able to express their deepest thoughts thereby imparting information that is beyond the interviewee's formal roles and positions. It allows the interviewer to probe the interviewee on the answers that they have given to get complete answers and also clarify any ambiguities. The main limitation of interviews is that they can be very time-consuming to setup, interview, transcribe, analyse, write feedback, and reporting.

3.7.5 Sampling

Sampling is a process used to select a portion of the population of the study. (Maree et al, 2007). In choosing a sampling method for informant selection, the researcher first considered whether to study the entire population, and if not, how to sample the population efficiently, how many people will be involved? What level of organization would be sampled—individual or community? What sampling technique should be used to assure the sample is representative and the data collected replicable, solid and relevant as articulated by (Alexiades, 1996; Bernard 2002) reference in (Tongco, 2007).

The researcher considered the question "To what extent does South Africa's legislation and regulation address illegal and harmful Internet content relating

to children?" The question is specific to the Internet community and regulations and laws that govern Internet content therefore the researcher chose purposive sampling. Purposive sampling will be used to select the legislation and regulations to be reviewed and the population to be interviewed. Tongco (2007) defines purposive sampling as a technique that is a deliberate choice of an informant due to the qualities the informant possesses. Also called judgment sampling, it is a non-random technique that does not need underlying theories or a set number of informants (ibid). The population to be interviewed is displayed in Table 2.

The interview guide will be used to interview the population selected. The interview will be conducted with open-ended questions. A tape recorder will be used. When analysing the interview responses the researcher will read through the interview responses and look for patterns or themes among the participants. If a variety of themes is discovered, the researcher will group them in any meaningful way, for example as by type of participant.

Table 2: Interviewees identified and interviewed

Respondent	**Company/ Institution**	**Focus**
Regulator A	ICASA	Regulator
Regulator B	Films and Publication Board	Regulator
Policy maker A	Department of Communications	Policy Maker
Policy maker B	Department of Education	Policy Maker
Service provider A	Telkom Internet	Internet Service Provider
Subject expert A	Snail Attorneys @ Law Inc	Subject Matter Expert
Subject expert B	Convergence Partners	Subject Matter Expert
Subject expert C	Mxit	Content Provider
Subject expert D	Childline	Subject Matter Expert

3.8 Data analysis

Data Analysis is defined by Centre for teaching, researching and learning (n.d) as " a process of organizing and interrogating data in ways that allow

researchers to see patterns, identify themes, discover relationships, develop explanations, make interpretations, mount critiques, or generate theories". Based on the questions the researcher would have asked in the interview together with document analysis done, the researcher will be able to develop themes and deriving meaning from the data. Creswell (2009) suggests that qualitative research needs to be interrogated in the following manner for the researcher to get the meaning of the data, which is

- Research is often conducted in the field, allowing direct interaction with the people being studied in their context.
- Researchers collect data themselves by examining documents, observing behaviour or interviewing participants.
- Multiple sources of data are preferred over a single source; this requires the researcher to review all data, make sense of it and organize it into categories or themes that cut across all sources.
- Researchers often build their patterns, categories and themes from the bottom up (inductive analysis).

The steps suggested by Cresswell (2009) were followed in the analysis of the findings of this study. The conceptual framework that was adapted from Lessig's 1998 model of Internet regulation was used as a basis of analysing the data. The themes identified are adequacy of the policies, legislation and regulations; Internet safety education and awareness and lastly intergovernmental and other Internet stakeholders' collaboration. The themes were also derived from the conceptual framework. The findings of these themes are presented in Chapter 4 and the analysis is presented in Chapter 5.

3.9 Significance of the study

It is established in the study that children are the most vulnerable people on the Internet (Preston, 2009). Considering this factor the significance of the study is to attempt to give guidance to policy makers, regulators and the private sector on how to enhance Internet content regulation. The study recommends the prescription regulation among other things on pornographic websites. Furthermore the study will highlight the desperate need of national education about Internet risks and prevention for children, parents, schools and caregivers. Ultimately South Africa will work towards effective Internet content affecting children.

3.10 Limitations of the research study

The scope of this research is limited to harmful and illegal Internet content against children in South Africa. Illegal Internet content that does not affect children, for example electronic funds transfer fraud, sales and investment fraud, electronic money laundering and tax evasion and policies that are not related to cybercrime will fall out of the scope of this study. Although it is in the interest of this study to investigate other forms of cybercrime, the researcher deliberately excluded these dimensions in the research study because it would broaden the area of study and therefore weaken the focus.

Furthermore, the policies, legislation, and regulations selected for data analysis might not be comprehensive but gives a holistic representation of the subject matter at hand. In the conceptual framework there are four factors that lead to the effective Internet regulation that affect children. These factors are legal, social, economic and technology. The economic factor of the framework was left out in the data analysis as it requires an in-depth

investigation of price regulation, which is beyond the level of detail required to understand the foundational policy and regulatory issues.

The researcher could not interview children and parents to get a first-hand information on how they experience harmful and illegal internet content, this is due to the fact that the researcher needed to get permission from the ethics committee and due to time constraints the permission was not sought. The researcher acknowledges that the study would benefit from the interviewing parents and children; however this will raise issues of ethics for the research.

Lastly considering that the environment being researched is very dynamic, data could change and be outdated in a short space of time.

Chapter 4: Research findings of harmful and illegal Internet content

4.1 Introduction

The study is examining the effectiveness of the policies, legislation and regulations that govern harmful and illegal content that affect children. This chapter presents the findings that ensued from the data collection methodologies performed. Purposive sampling was used to select the policies, legislation and regulations to be examined, furthermore this type of sampling was used to select the interviewees based on the role they play in the Internet environment.

In addition to the themes explored, other factors affecting harmful and illegal content emerged during the course of the data collection. The themes and issues emerging from the interviews and document analysis are; the adequacy of the policies, legislation and regulations, Internet safety education and awareness, collaboration of government agencies with themselves and together with other Internet stakeholders.

Document Analysis was the first data collection to be implemented so that the information gathered could help with structuring the interview questionnaires to get the most meaningful information. The study looked at three timeframes where policies, legislation and regulation that relates to children and ICT sector emanated from. The study concentrated on understanding the focus of the policy makers at that time period. This was realised by looking at Period A which will interrogate policies, legislation and regulations written on the years 1996 - 2005. Period A is the period where telecom reform was initialized with the purpose of bringing affordable access to communications services and accelerated development to meet the needs of a modern economy (Gillwald, 2005). In the initial period of telecoms

reform, there are intentions of introducing privatization, competition and regulatory reform. Then the study looked at Period B with policies, legislation and regulations that was written between the years of 2005 – 2010, this period is where policy makers were focused on legislation and regulations that relates to the wellbeing of women and children as well as concentrating on bridging the digital divide. Lastly Period C is where the study reviewed policies, legislation and regulations from the years 2010 - 2014. This period is the advancing period where the focus is based on broadband among other priorities. The study's first focus was on legislation that talks to children's welfare and thereafter it focussed on ICT sector specific legislation.

The second document analysis was conducted to interrogate different materials such as surveys and published academic research reports to establish the effectiveness of the legislation.

After the completion of document analysis, the study conducted semi-structured interviews. The interview guide was setup to specifically address questions that are relevant to a particular interviewee. The questions posed to the interviewee seek to gather as much information and encouraged the interviewee to elaborate in their answers.

4.2 Document analysis of policies, legislation and regulations

Document analysis was performed on the policies, legislation and regulations that are deemed to be concerned with the Internet. The questions in Appendix A were posed to every policy, legislation and regulation that was analysed for the study to understand how risks on the Internet were addressed.

Period A 1996-2005 – Telecoms reform era

This period marks the beginning of democracy in 1994, a period where a foundation was created. Period A sees the introduction of telecom reforms by introducing privatization, completion and regulatory reform. The introduction of the telecom reform was to bring affordable access to communications services and accelerated development to the South African society (Gillwald, 2005).

4.2.1 The Constitution of the Republic of South Africa of 1996

The Convention on the Rights of the Child (CRC) was finalized in 1989 but it took two decades for the real work of developing the legislative, administrative and other measures to ensure recognition of children's rights (UNICEF, 2007). The CRC specifically required states parties to take all appropriate legislative, administrative and other measures to ensure realization of the rights of the child (UNICEF, 2007). Section 28 of the South African constitution (1996b) which is also referred to as Children's charter includes a specific section dedicated to the rights of children which is in line with CRC (UNICEF, 2007). The study notes that South Africa did not adopt a comprehensive law on children until 2006, with enactment of Children's Act 38 of 2005.

Under the Bill of Rights, Section 28 (1) (f) of the South African constitution (1996b) states that "every child has the right to not to be required or permitted to perform work or provide services that place at risk the child's well-being, education, physical or mental health or spiritual, moral or social development;" (RSA, 1996b). This provides that children should not be used or provide services of child pornography. The constitution does not mention exposure of children to internet child pornography and any other

pornography nor does it touch on the Internet harmful content. But looking at Section 28 (2) of the South African Constitution (1996b) where it states that “a child’s best interests are of paramount importance in every matter concerning the child. These provisions can be seen to include and address exposure of children to Internet child pornography and any other online pornography as well as any Internet harmful content. This should also address cyberbullying. It will be difficult to only use the constitution in prosecuting an individual as it is not explicit in explaining the best interest of a child. This will need to be proven that when a child is exposed to pornography, which is not illegal is not in the best interest of that child.

4.2.2 Films and Publication Act 65 of 1996

The Films and Publications Act 65 of 1996 was established in 1996 however has been amended in 1999, 2004 and 2009. The objective of the Act as in chapter 2 is “to regulate the distribution of certain publications and the exhibition and distribution of certain films, in the main by means of classification, the imposition of age restrictions and the giving of consumer advice, due regard being had to the fundamental rights enshrined in the Constitution of the Republic” (RSA, 1996a).

It is important for the study to consider the definitions in the Films and Publications Act 65 of 1996 that are relevant to this study; which are defined below. Chapter 1 of the Act defines "film" as any sequence of visual images recorded on any substance, whether a film, magnetic tape, disc or any other material, in such manner that by using such substance such images will be capable of being seen as a moving picture. This definition of film can be interpreted to include any videos that can be accessed through the Internet.

The Act also provide that any publication is classified as X18 if it contains a visual presentation, simulated or real, of explicit sexual conduct which, in the case of sexual intercourse, includes an explicit visual presentation of genitals. Furthermore RI8 publications are classified to protect children in the relevant age group against harmful or disturbing material in the publication which shall only be distributed to persons older than 18 years of age, or older than a specified younger age; that it shall only be distributed in a sealed and, if necessary, opaque wrapper which shall also, if applicable, bear the notice referred to in clause.

Schedule 1 of the Act classified a film as XX if it contains a scene or scenes, simulated or real, of a person who is, or is depicted as being, under the age of 18 years, participating in, engaging in or assisting another person to engage in sexual conduct or a lewd display of nudity; explicit violent sexual conduct; bestiality; explicit sexual conduct which degrades a person and which constitutes incitement to cause harm; or the explicit infliction of extreme violence or the explicit effects of extreme violence which constitutes incitement to cause harm. Furthermore a film shall be classified as X18 if it contains a scene or scenes, simulated or real, judged within context, of explicit sexual conduct which, in the case of sexual intercourse, includes an explicit visual presentation of genitals.

Chapter 7 of the Films and Publications Act 65 of 1996 provides that any person who knowingly distributes or advertises for distribution a publication classified as XX, X18, R18 or F18 in conflict with any condition imposed by the Board in terms of section 18(4)(b),shall be guilty of an offence. The provision of this Act address the exposure of children to child pornography, online pornography and any inappropriate and harmful website contents. The Act also provides for any person who knowingly possess, or produces, or

imports or distributes certain publications of films prohibited like child pornography shall be guilty of an offence.

The Act also addresses cyberbullying and websites that advices children to commit suicide by stipulating that any person who knowingly broadcasts, exhibits in public or distributes a film which, judged within context incites to imminent violence; or advocates hatred that is based on race, ethnicity, gender or religion, and which constitutes incitement to cause harm, shall be guilty of an offence.

The Act provides that any person found guilty of a contravention of section 25(a), (b) or (c), 26(1)(a), (b) or (f), 26 (4), 27(1), 28 or 29 may be sentenced to a fine or to imprisonment for a period not exceeding five years, or where the court convicting such person finds that aggravating factors are predominant, both such fine and such imprisonment. The Act however it does not address online sexual grooming.

The freedom house South Africa (2013) articulate that in “September 2012, the Constitutional court upheld a 2011 Gauteng High Court judgment ruling the 2009 amendments to the Films and Publications Act 65 of 1996 as unconstitutional, based on the conclusion that the pre-screening of publications (including internet content) would affect the value of news and be an unjustifiable limitation on freedom of expression”. The amendments to the Films and Publications Act 65 of 1996 were passed in an attempt to regulate child pornography and hate speech, this raised concerns that certain types of controversial content could be subject to prepublication censorship. The amendments required every print and online publication not recognized by the press ombudsman to submit potentially “pornographic” or “violence-inciting” materials to the Film and Publications Board (FPB) for approval and imposed criminal penalties for noncompliance. Exemptions were provided for

artistic and scientific speech, but the FPB had the discretion to grant or deny these exemptions. Movies and games were classified before their release, though the FPB could not classify publications or websites until it first received a complaint from the public (Freedom House South Africa, 2013). This is a demonstration of how censorship of content and freedom of speech are issues that requires balance when regulating.

4.2.3 The Telecommunication Act of 1996

Looking at the ICT specific sector legislation the study analyses the Telecommunication Act of 1996. The aim of this Act included to make new provision for the regulation of telecommunication activities other than broadcasting, to establish an independent South African Telecommunications Regulatory Authority and a Universal Service Agency (RSA, 1996c). The Act concentrates on licencing of among others the telecommunications service providers where it specifically mentions Telkom and the mobile telecommunications services providers Vodacom, Mobile Telephone Networks (MTN) and Cell C. This Act does not address any of the questions that the study is trying to address.

4.2.4 ICASA Act of 2000

The Independent Communications Authority of South Africa (ICASA) Act of 2000 preamble stipulates that it recognizes that technological and other developments in the fields of broadcasting and telecommunications are causing a rapid convergence of these fields. This preamble is important for the study because as the study endeavours to investigate how Internet content can be regulated, the study needs to acknowledge the convergence of the fields of broadcasting and telecommunication. The Act's objective is to

establish an independent authority to regulate broadcasting in the public interest and to ensure fairness and a diversity of views broadly representing South African society, and to regulate telecommunications in the public interest. This Act sets the scene in how the authority will be established and how it will regulate the ICT industry which is of interest to this study. The Act also sets the foundation of regulating both the broadcasting and telecommunication environment by one body which is ideal as the technological dynamics of convergence emerges. However the Act does not address exposure to Internet child pornography, online pornography, online sexual grooming, inappropriate website content and cyberbullying.

4.2.5 Electronic Communications and Transactions Act of 2002

The main aim of Electronic Communications Transaction Act of 2002 (ECT) includes “to provide for the development of a national e-strategy for the Republic and to promote universal access to electronic communications and transactions” (RSA, 2002). In these two objectives, the Act promotes the use of electronic communications and transactions by the South African community and provides that the government must drive the e-strategy and universal access to enable e-communications.

Chapter 2 Part 1(6) of the ECT Act of 2002 in respect of “universal access, the national e-strategy must outline strategies and programmes to provide Internet connectivity to disadvantaged communities; foster the adoption and use of new technologies for attaining universal access; stimulate public awareness, understanding and acceptance of the benefits of and Internet connectivity and electronic transacting” (RSA, 2002). It is quite clear that the ECT Act of 2002 promotes universal access of electronic communications by all South Africans including disadvantaged communities. Relevant to this study is the access to Internet universally by all South Africans.

Chapter 2 part 2 (6) of the ECT Act of 2002 further provides for the provision or securing support services for such facilities and infrastructure to assist with the efficient execution of electronic transactions; and rendering assistance and advice to such persons and communities on ways to adopt and utilise electronic transactions efficiently (RSA, 2002). On the other hand the Act does not address nor mention any of the questions of exposure to children to Internet child pornography, Internet pornography, any harmful or inappropriate Internet content by children including cyberbullying. It is clear that while the ECT Act of 2002 was promoting the use of electronic communications it did not tackle all the consequences of using the electronic mediums.

The Act has a section on cybercrime including unauthorised access to, interception of or interference with data, computer related extortion, fraud and forgery. In this section the Act concentrates on breaking security codes of passwords to access electronic information that the person is not authorised to access. It does not mention the accessing illegal content in this case online child pornography.

The other section which is on interest to this study is chapter 11 section 73 of the ECT Act of 2002; the section provides that " a service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control, as long as the service provider does not initiate the transmission; performs the functions in an automatic, technical manner without selection of and does not modify the data contained in the transmission" (RSA, 2002). In this case the Act provides that the Internet service providers (ISP) will not be liable for any child pornography content that will be stored or transmitted from their electronic systems if they did not know about it.

Furthermore the Act provides that there is no general obligation for the service providers to monitor the data which it transmits or stores and to actively seek facts or circumstances indicating an unlawful activity (RSA, 2002).Therefore the accountability for ISPs to monitor this unlawful content is not addressed. However this limitation of liability to ISPs only applies if the ISP is a member of representative body where its members are subject to a code of conduct and where the representative body is capable of monitoring and enforcing its code of conduct (RSA, 2002).

The Act provides for a turndown notification to the service provider in case of an unlawful activity. The turndown notification must be in writing and must contain the details of the complainant (RSA, 2002). However the owner of the website can change from one service provider to the next with the same content making it difficult and cumbersome for the complainant for execute the turndown notification to different service providers.

The other challenge is that on the Internet the website with unlawful activity can be from anywhere in the world. Section 90 of the Act provides that a court in the Republic trying an offence in terms of this Act has jurisdiction where-

(a) The offence was committed in the Republic;

(b) Any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;

(c) The offence was committed by a South African citizen or a person with permanent residence in the Republic or by any person carrying on business in the Republic; or

(d) The offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

This provision of the Act covers all Internet transgressions that can happen in South Africa or outside the country but affects the country.

4.2.6 White paper on e-Education: Transforming learning and teaching through information and communication technologies (ICTs) of 2004

While conducting interviews, Respondent D (31/01/2014) suggested that the study look at the e-Education white paper as part of regulations related to access to ICT by schools. The objective of the e-Policy is for every South African learner in the general and further education and training bands to be ICT capable in terms of use ICTs confidently and creatively to help develop the skills and knowledge they need to achieve personal goals and to be full participants in the global community by 2013 (DoE, 2004).

The White Paper defines e-Education as a use of ICTs to accelerate the achievement of national education goals and connecting learners and teachers to each other; the intention of e-Education is to connect learners and teachers to information and ideas via effective combinations of education and technology in support of educational reform (DoE, 2004).

The White Paper articulates that e-education is not more than developing computer literacy and the skills necessary to operate various types of information and communication technologies. It is the ability to apply ICT skills to access, analyse, evaluate, integrate, present and communicate information; create knowledge and new information by adapting, applying, designing, inventing and authoring information; and function in a knowledge society by using appropriate technology and mastering communication and collaboration skills (DoE, 2004).

The White paper goes into detail on how to achieve the goals for e-Education however it does not mention the risks that comes with ICTs and how it will address them.

Period B 2005-2010 – Protection of women and children and bridging the digital divide

Period B is the period policy makers were focused on legislation and regulations that relates to the wellbeing of women and children as well as concentrating on bridging the digital divide. In the 10 years post building the foundation, the focus moved from a telecom reform to more pertinent issues of cybercrime and children and sexual offences. It is to be noted that the Films and Publications Act of 1996 was subsequently amended in 2009 to bring more focus on the technological changes including the Internet content. As mentioned above some of these amendments were contested and found to be unconstitutional.

4.2.7 The Children's Act 38 of 2005

The Children's Act 38 was enacted in 2005. Section 9 of the Children's Act 38 of 2005 provides that the best interests of a child are of paramount importance in every matter concerning the child (RSA, 2005a). When analysing the Children's Act with regard to the questions stipulated above Chapter 1 (f) of the Children Act provides that children needs to be protected from children from discrimination, exploitation and any other physical, emotional or moral harm or hazards (RSA, 2005a). It is highlighted in the literature that exposure of children to harmful internet content may cause them emotional and psychological harm. Chapter 1 (i) of Children's Act 38 of 2005 provides in general the protection, development and well-being of children.

To answer one of the question that stipulates “to what extend does the legislation address cyberbullying” in Chapter 1 (1) of The Children’s Act 38 of 2005 “abuse”, in relation to a child is defined as any form of harm or ill-treatment deliberately inflicted on a child, and includes (c) bullying by another child (RSA, 2005a). The legislation does not specifically mention cyberbullying but cyberbullying is another form of bullying that happens on the Internet. This type of bullying is prominent and it is easy to carry out as the victim may not know who is bullying them. According to the Children’s Act 38 of 2005 that will constitute abuse. Chapter 1 (e) of the Children’s Act 38 of 2005 also defines exposing or subjecting a child to behaviour that may harm them psychologically or emotionally as abuse (RSA, 2005a). It can be interpreted that exposure of children to harmful internet content and other forms of harm on the Internet constitute to abuse.

Chapter 2 of the Children’s Act 38 of 2005 sets out the general principles and states that all proceedings, actions or decisions in a matter concerning a child must recognise a child’s need for development and to engage in play and other recreational activities appropriate to the child’s age (RSA, 2005a). The Act highlights that the child needs to be engaged in play and other activities that are appropriate to their age. Internet pornography is inappropriate to children therefore the Act provides that this Internet content should not be exposed to children. The Act also sets out the responsibility of both parents and the State in relation to the child.

Section 12 (1) of the Children’s Act 38 of 2005 provides that every child has the right not to be subjected to social, cultural and religious practices which are detrimental to his or her well-being (RSA, 2005a). The exposure of children to Internet child pornography, online pornography and inappropriate website content will be detrimental to children therefore the Act addresses this two questions. Although the Act is explicit on protecting the children to

what is detrimental to them, it must be proven in court that the exposure to the risks on the Internet was detrimental. Online sexual grooming is not mentioned on the Children's Act 38 of 2005 but it is also covered by the general principles on chapter 2 of the Children's Act 38 of 2005.

4.2.8 Sexual Offences Act, No. 32 of 2007

The Sexual Offences Act 32 of 2007's aim includes "enacting comprehensive provisions dealing with the creation of certain new, expanded or amended sexual offences against children and persons who are mentally disabled, including offences relating to sexual exploitation or grooming, exposure to or display of pornography and the creation of child pornography…to address the particular vulnerability of children and persons who are mentally disabled in respect of sexual abuse or exploitation" (RSA, 2007). Chapter 3 of the Sexual Offences Act 32 of 2007 specifically talks to sexual offences against children.

Part 2 (18) of this chapter provides that a person who supplies, exposes or displays to a child an article which is intended to be used in the performance of a sexual act, child pornography or pornography, a publication or film, or perform a sexual act or self-masturbation with the intention to encourage, enable, instruct or persuade or to diminish or reduce any resistance or unwillingness of a child to perform a sexual act; or commits any act with or in the presence of child and arranges or facilitates a meeting or communication with the child in any part of the world, with the intention of performing a sexual act is guilty of offence of sexual grooming of the child (RSA, 2007). The Act also provides that anybody who facilitates sexual grooming with a child is guilty of the offence of promoting the sexual grooming of a child (RSA, 2007).

Section 19 provides that a person who unlawfully and intentionally exposes or displays or causes the exposure or display of any image, publication, depiction, description or sequence of child pornography or pornography; and any image, publication, depiction, description or sequence containing a visual presentation, description or representation of a sexual nature of a child, which may be disturbing or harmful to, or age-inappropriate for children, as contemplated in the Films and Publications Act 65 of 1996, or in terms of any other legislation; or (c) any image, publication, depiction, description or sequence containing a visual presentation, description or representation of pornography or an act of an explicit sexual nature of a person 18 years or older, which may be disturbing or harmful to, or age-inappropriate, for children, as contemplated in the Films and Publications Act of 1996, or in terms of any other law, to a child, with or without the consent of a parent or a guardian, is guilty of the offence of exposing or displaying or causing the exposure or display of child pornography or pornography to a child (RSA, 2007).

Section 21 and 22 of Chapter 3 provides that any person who compelling or cause a child to witness sexual offences, sexual acts or self-masturbation and any person who exposes or displays genital organs, anus or female breasts to children ("flashing") is guilty of a sexual offence (RSA,2007).

The Act is very comprehensive and addresses most of the questions that were asked in Appendix A for document analysis. The Act answers the questions of whether the legislation addresses sexual grooming, exposure to child pornography and pornography and any inappropriate content. Even though the Act does not specify the Internet, it references on the Films and Publications Act of 1996 which includes the Internet in its definition of film. The Act does not address bullying or cyberbullying.

4.2.9 Electronic Communications Act of 2005

The objective of the Electronic Communications (EC) Act of 2005 is to provide for the regulation of electronic communications in the Republic in the public interest (RSA, 2005b). This objective is important to the study as it regulates the electronic communications in the public interest, including the children's interest. The Act does not address any of the questions posed which is, does the legislation address exposure to internet child pornography, online pornography, online sexual grooming, inappropriate website content and cyberbullying.

What is quite interesting is that Chapter 13 section 73 of the EC Act of 2005 provides that the Internet services, provided to all public schools as defined in the South African Schools Act of 1996 and all public further education and training institutions as defined in the Further Education and Training Act of 1998, must be provided at a minimum discounted rate of 50% off the total charge levied by the licensee providing Internet services to such institutions (RSA, 2005b). This provision intends to make Internet services affordable to schools therefore encouraging increased access to school children. This Act does not address any of the issues that affect children on the internet but encourages Internet penetration in schools. The encouragement of Internet penetration needs to encompass how to deal with the Internet risks that comes with it.

4.2.10 Information Society and Development (ISAD) Plan of 2007

In response to the World Summit on the Information Society (WSIS) plan of Action for countries to develop plans that outline how the Information Society building was to unfold, South Africa developed the Information Society and Development (ISAD) Plan. The vision of this plan is "to establish South Africa

as an advanced Information Society in which Information and ICT tools are key drivers of economic and societal development" (PNC, 2007). The main goal of the policy is to ensure that every learner in both general and further education and training will be ICT capable by 2013. This would broaden the participation and increase the competitiveness of the South African economy and increase the capacity of government to deliver using e-services (PNS, 2007).

In the ISAD Plan there is strategic imperatives set out by the PNC (2007) which includes enabling policy and regulatory environment as well as strengthening the capacity of the regulator; providing ubiquitous access to ICT infrastructure and services at affordable prices; to restructure education curriculum to address the needs of the knowledge economy, to develop a sustainable, science, technology and research sector and to increase awareness of the benefits of ICTs to all, especially persons with disability, women, youth, children.

The ISAD Plan is comprehensive in the intentions of connecting all South Africans including children into the digital world. However it does not address any of the risks that come with ICT.

4.2.11 ICASA Code of Conduct for broadcasting service licensees of 2008 Regulation

This regulation refers to the Electronic Communications Act of 2005, where broadcasting is defined as "any form of unidirectional electronic communications intended for reception by the public to any broadcasting service, whether conveyed by means of radio frequency spectrum or any electronic communications network or any combination thereof" (RSA, 2005b). The key word being unidirectional meaning moving or operating in

one direction. The study acknowledges that the Internet is not unidirectional but rather bidirectional as it allows data flow in the opposite direction.

Section 5 of this regulation provides that the broadcasting service licensees must not broadcast material which is harmful or disturbing to children at times when a large number of children is likely to be part of the audience. Unlike the Internet, broadcasting have watershed time where certain content intended for adults can be broadcasted between 21h00 and 05h00 (ICASA, 2008). Furthermore section 7 provides that broadcasting service licensees must not broadcast material which contains a scenes, simulated or real, of any of child pornography, bestiality, sexual conduct which degrades a person in the sense that it advocates a particular form of hatred based on gender and which constitutes incitement to cause harm, explicit sexual conduct, explicit extreme violence or explicit infliction of domestic violence (ICASA, 2008).

The study observes that this regulation covers harmful content affecting children but only concentrating on broadcasting which to a large extend does not include the Internet.

Period C 2010- 2014 – Advancing into technology

Period C is where the policy makers were advancing into technology. We see the policy maker focusing on broadband and how benefits it will bring to the South African society. The Protection from Harassment Act illustrates the understanding that harassment can come in different formats including the Internet.

4.2.12 Broadband Policy of 2010

The broadband policy of South Africa's objective is "to facilitate the provisioning of affordable, accessible, universal access to broadband infrastructure to citizens, business, communities and the three spheres of government, and to stimulate the usage of broadband services in order to promote economic development and growth and act as an enabler for further social benefits" (RSA, 2010). The government wrote this policy to rapidly drive access to broadband as a major benefit to the country like for economic growth. The policy does not address exposure to Internet child pornography, online pornography, online sexual grooming, inappropriate website content and cyberbullying.

4.2.13 Protection from Harassment Act of 2011

The Protection from Harassment Act of 2011 affords the victims of harassment an effective remedy against harassment by providing protection orders against harassment, a person who breaches a protection order may be criminally charged and, if found guilty, held liable to a fine or imprisonment (RSA, 2011). This is to ensure the rights that are enshrined in the South African Constitution which includes the right to equality, privacy, dignity, freedom and security of a person, which incorporates the right to be free from all forms of violence, and the rights of children to have their best interests (RSA, 1996b). A protection order may be applied at court by any person who is a victim of harassment, it is worth noting that a child may apply for a protection order with or without the assistance of their parents or guardian (Snail, 2013).

In the act of harassment is defined as any person who directly or indirectly engages in a conduct that the harasser knows or ought to know causes harm

or inspires the reasonable belief that harm may be caused to the complainant or a related person by unreasonably engage in verbal, electronic or any other communication aimed at the complainant or a related person, by any means, whether or not conversation ensues. Section 1(b) of the Act continues to add to the definition of harassment as any person who directly or indirectly engages in a conduct that the harasser knows or ought to know amounts to sexual harassment of the complainant or a related person. This Act addresses cyberbullying, it covers harassment of a complainant electronically.

4.2.14 Internet and Cell phone Bill of 2010

The controversial Internet and cell phone bill was proposed in 2010. This draft bill makes it illegal for Internet and mobile phone service providers in the South Africa to distribute or permit the distribution of pornography, so as to ensure protection for children and women. The Bill suggested that Internet service providers be tasked with filtering content.

Critics included women's and LGBTI movements; in their objection they said that firstly the bill was drafted by an organisation JASA that is known to be anti-choice and homophobic; secondly the "Bill equates women with children, and takes a protectionist approach to the rights of women" (Shackleton, 2010). Women's and LGBTI movements feared JASA would not promote access to information about lesbian sexuality or abortion (ibid). Neither the Deputy Minister, Mr Gigaba, nor the Bill has details as to how the total ban could be effected in a country where the internet and cell phone content is not controlled by the state, and where freedoms of expression and access to information are considered central to human rights. This bill has had a revision in 2011 which still saw the ISPs and mobile service providers liable for the distribution of pornography. This brings controversy as it implies that

adults who would want to access pornography will be prevented by the ISPs and mobile service providers. The bill has not being passed by parliament.

4.2.15 National Broadband Policy of 2013

The objective of the National Broadband Policy 2013 is to connect South Africa by creating opportunities, ensuring inclusion. The policy has adopted four central strategies which are digital readiness, digital development, building the digital future and lastly realising digital opportunity. The intended outcomes of digital readiness include to enable regulatory and administrative environment that facilitates broadband rollout; digital development strategy's intended outcome include having a high capacity future-proof network capacity procured for key public sector broadband needs at more affordable rates; while building the digital future strategy intent to enable economies of scale in medium density and low income areas through government investment and guarantees in network extensions; and lastly realising digital opportunity strategy intended outcome includes to promote growth through enabling economic infrastructure and associated industrial development (RSA 2013). The strategies and objective of the Broadband Policy 2013 also does not address exposure to Internet child pornography, online pornography, online sexual grooming, inappropriate website content and cyberbullying.

4.2.16 National integrated ICT Policy Green paper of 2014

The Green Paper articulates that the policy recognize the need to protect children from potentially harmful content. Mobile technology, broadband, digital television, smartphones, the cloud, tablets and new media technology are all recent developments in the market. These changes have far reaching implication for any new policies and legislation.

In terms of cybersecurity the green paper focuses on ECT Act of 2002 and the provisions of it. It stipulates the finalization of the national cybersecurity policy in which issues of the protection of critical databases and critical infrastructure protection is fragmented. The cybersecurity concentrates on data protection, identity theft, online gambling and related activities and collection, preservation and production of e-evidence

The Green Paper recognises the need to redefine broadcasting, EC Act of 2005 have a technology neutral definition of broadcasting. The regulator noted that in the future, on demand services, including those available over the public internet “may substitute for traditional television broadcasting” and therefore require some form of regulation but stated that this would require a legislative amendment to permit the regulation of content services distinct from broadcasting services under certain circumstances. The green paper acknowledges that it needs to consider the approach to broadcasting-like services delivered over the Internet.

There is a section of content standards and protection of children. In this section the green paper articulates that there is currently a co-regulatory approach to the development and enforcement of South African broadcasting content standards.

The EC Act requires ICASA to develop a code of conduct for broadcasters and stipulates that all broadcast licensees must adhere to this unless they are a member of a body which has proved to the satisfaction of the authority that its members subscribe and adhere to a code of conduct enforced by that body (RSA, 2005b). Such a self-regulatory code and the mechanisms to enforce compliance to it have to be approved by ICASA in terms of the law.

Broadcasters have established their own self-regulatory body in line with the above provisions of the Act. The codes developed by both ICASA and the broadcasting complaints commission of SA are very similar. Both focus on protection of children and providing viewers and listeners with sufficient information about programme content to make decisions about what to watch or listen to through advisories. Content delivered over other platforms is currently regulated via a range of different bodies in line with FP Act. Convergence raises a number of new issues in relation to ensuring audience expectations regarding classification of audio-visual content and protection of children.

Given the volume of content that will be available over different platforms and channels, many countries around the world are considering ways to strengthen self-regulatory and co-regulatory arrangements. There is also an increased focus on media literacy to equip audiences and parents with information on tools available to protect in particular children from accessing harmful content (RSA, 2014).

Technology convergence is of interest to policy makers and regulators as it changes the nature of services, allowing an operator who was licensed under one category to be able to do things that would have required in a different category licences in the past (ibid).

4.3 Document analysis of broader perspectives on events of Internet risks

The materials that were interrogated were published academic research reports and newspaper websites. Apart from the policies, legislation and regulation this section addresses other published academic research reports that gives perspective of what happens in the daily lives of children in South Africa with regards to their encounter of harmful and illegal Internet content.

4.3.1 Findings on harmful and illegal Internet content

The report mentioned above by Chetty and Basson (2006) surveyed 943 children between 13-17 years in randomly selected schools in Cape Town, Durban and Johannesburg. In the report, 64 percent of young boys and girls were exposed to pornographic digital images shared on digital mediums. Seventy per cent of surveyed students reported that they came across pornographic images on digital mediums "accidentally". The report also reveals that while more boys claimed not to be bothered by pornography they encounter online, most girls felt disgusted.

In another report by FPB (2008) to investigate the impact of sexual abuse through ICT, which surveyed South African students, between the ages of 10 to 12-years old (grade five to seven) and 13 to 15-years old (grade eight to nine) living in Johannesburg, Durban and Cape Town; the study conducted 604 total questionnaires and 37 completed interviews. It was found that 22 per cent of surveyed participants were exposed to internet content of sexual nature and nudity. 14 per cent of the participants who had been exposed to "distressing content" had "sexual advances" made to them. Furthermore, 12 per cent of surveyed individuals indicated that this "distressing content" was via cell phones.

Young people Research Unit (YRU) (2011) at the University of South Africa (Unisa) surveyed 1000 young South Africans aged 12 to 25-years old. In the report 30.8 per cent of the participant were faced with an "unwanted discussion about sex" online, and 12.6 per cent had been "asked to do something sexual" online. The report also found that 20.2 per cent of respondents had come across a website with photos of naked people and of people having sex, and that 18.6 per cent of participants had received emails and instant messages with advertisements and/or links to X-rated websites.

The researches mentioned above indicate the extent of South African children exposed to harmful and illegal content and access on the Internet. In attempting to tackle the harmful and illegal Internet content the South African government is also faced with challenges of balancing the censorship with freedom of speech as mentioned above where the Constitutional court upheld the judgement of declaring the amendments to the Films and Publications Act as unconstitutional (Freedom house organization, 2013) on the fore-mentioned case against the FPB.

4.3.2 Findings on online grooming

UNICEF (2012) articulates that there is no laws that reprimands false online registration by the South African online community. The non-existence of such laws allows certain risks to occur. Firstly children under age can gain access to Mxit or other online websites which have age restrictions and secondly pedophiles and adults can do false registration online with the intention of disguising as children to groom unsuspecting children (UNICEF, 2012).

A study conducted by UNICEF (2011) has found that 42 per cent of young people talk to strangers on Mxit every day and 33 per cent doing so at least once a week. In another study conducted in the Nelson Mandela Bay by de Lange and von Solms (2011), 1,594 students at three primary and three secondary schools, who ranged across grades six to 12 completed a questionnaire regarding their online habits. They study revealed 40 per cent of students had met someone in person after having chatted online. Thirty per cent of students reported meeting a stranger in person who differed significantly from what they anticipated.

In 2008 a Pretoria a businessman obtained an interdict against a Durban woman after she became obsessive and manipulative with his 17-year-old matric daughter whom she had met on MXit chatroom (Versluis, 2008). In September 2007, Ganesh had allegedly asked that she meets with the girl at the shopping centre, which the girl did and missed school; the two then went to Ganesh's uncle where the girl stayed overnight. Before they were able to get on a plane to Durban to go to Ganesh's house, the police arrived at the uncle's house.

Another example is the case mentioned above reported by (Smillie and Tromp, 2010) where a 15-year old girl was drugged and raped by a 27-year old man she met on Mxit. Another similar case reported on IOL by Geduld (2011) reveals that three men allegedly raped a 20-year old, who communicated with one of the alleged perpetrators on Mxit before meeting with them.

The study and the cases presented highlights the point that online grooming is widespread making children vulnerable to be victims of sexual exploitation.

4.3.3 Findings on cyberbullying

In a study mentioned above researched by de Lange and Rossouw von Solms (2011) in Nelson Mandela among 1 594 primary and secondary school learners indicated that 36 percent of the respondents had experienced some form of cyberbullying. In a separate study, The Centre for Justice and Crime Prevention (2009) reported that among 1 726 young people between the ages of 12 and 24 years being surveyed, 46.8 percent of the respondents had experienced some form of cyberbullying, including verbal telephone harassment.

Cases of cyberbullying among South African children had been reported in the news outlets had unveiled cases of cyberbullying among South African children and young people. Edwards (2008) had reported on New24 that in Springs, Gauteng, and the mother of a 16-year-old girl obtained a peace order in terms of section 384 of the Criminal Procedure Act, 1955 against another 16-year-old girl at her daughter's school after the other girl apparently regularly humiliated the woman's daughter on MXit. The daughter's name also appeared on MXit 'slut list', which contained the names of girls from various schools in Springs, including their addresses, telephone numbers and schools. The mother filed for and obtained a peace order in order to protect her daughter from cyberbullying, and prevent the perpetrators from continuing their actions.

In another case that mentioned by Badenhorst (2011) in February/March 2006, three high school boys aged 15- to 17-years-old were charged with crimen injuria after publishing an alleged defamatory image of the deputy principal of their school. One of the boys created the defamatory image electronically by attaching the heads and faces of the principal and deputy principal on to a picture of two naked men sitting next to each other in a sexually suggestive and intimate manner. The boy took the school badge from the school website and used it to obscure the men's genitals. He then sent the image to a friend's mobile phone, who forwarded it to other learners at the school. One of the accused printed the image and placed it on the school's notice board.

4.4 Stakeholders views and experiences on harmful and illegal Internet content

As articulated in Chapter 3 purposive sampling was used to select the interviewees based on the role they play in the Internet environment. The

interview questions were setup in a way that is relevant to what interviewees specialized in. The open-ended questions were intended to gather as much information as possible from the interviewee by giving the opportunity to have the elaborative responses.

The study will express the interview findings with the themes in mind, these themes are the adequacy of the policies, legislation and regulations; Internet safety education and awareness; and intergovernmental collaboration and other Internet stakeholders. They are presented as follows:

4.4.1 Adequacy of the policies, legislation and regulations *(Legal)*

The policies, legislation and regulations that govern harmful and illegal Internet content affecting children is South Africa is adequate (Subject expert A, Subject expert B, Regulator A, Regulator B and Policy maker A). South Africa is a signatory to international treaties such as the Budapest Convention and the SADC Model Law. The Budapest Convention remains the only international agreement that addresses cybercrime and is aimed at harmonizing national laws and establishing international cooperation against cybercrime (DoC, 2014). The country has aligned their policies, legislation and regulation with the international agreements which is a signatory to. Subject expert A (16/01/2014) articulated that in some instances South Africa has copied the international legislation which validates the country's policies, legislation and regulations. The issue that South Africa is facing is more on the implementation of these laws rather than the laws being inadequate (Subject expert A, 16/01/2014).

Policy maker B (31/01/2014) has indicated that the policies are governing at a macro level and there is a need for a policies to be translated and managed in a micro level including but not limited to home, playground, classroom, church and night clubs. The assumption is policy is the answer

but this problem requires more than that legislation is extremely limited in terms of schools, classrooms and school governing bodies (Policy maker B, 31/01/2014). There are a lot of contentious issues with governance of mobile devices in schools. The National Association of governing bodies called for the banning of mobile phones at schools on the pretext that it encourages the proliferation of pornographic material (Tubbs, 2012). Not everyone agreed with this notion, the Governing Body Foundation (GBF) believed that a blanket ban on cellphones in schools could be counter-productive (ibid). Other argued that the mobile phones are useful as educational tools. We need effective mechanisms not only policies (Policy maker B, 31/01/2014). Policy maker B (31/01/2014) and Subject expert B (20/01/2014) articulated that there is no knowledge of the technologies in general for the policy makers in order to ensure that they make good policy.

South Africa is part of the UN Convention on the rights of the child, African Charter on the rights and welfare of the child, Palermo Protocols - United Nations Convention against Transnational Organized Crime

4.4.2 Internet Safety Education and Awareness *(Social and technological)*

It is shared by many respondents that Internet safety and awareness is not enough in the schools, at home and in various places like churches. Parents together with government need to play a big role in educating their children about the risks on the Internet but most of the parents are oblivious to these risks. Some of the parents are more worried about the time the children spent on the Internet and the bills they would run rather than the risks of stumbling into pornographic material or being exposed to cyberbullying and the other Internet risks revealed in the study (Ofcom, 2014).

Parents are the policy makers at home and they must want to protect their kids (Regulator A (13/01/2014); Regulator B (13/01/2014); Policy maker B (31/01/2014). There are lots of children who do not have parents in their homes but has guardians and the community playing the role of parents. The prevalent finding about Internet safety was that not only children need to be educated about Internet safety but also the parents, caregivers, teachers and communities. All respondents had a view that there is little or no knowledge of the risks on the Internet that affects children.

Schools play a major role in Internet safety education and awareness. Schools need to be equipped to educate children about the risks on the Internet most importantly as other schools are requiring children to bring tablets to school for learning purposes (Policy maker B (31/01/2014); Subject expert A (16/01/2014); and Policy maker A (14/01/2014). Not only do we see the proliferation of mobile phones, there are different devices that access the Internet.

Policy maker B (31/01/2014) and Subject expert C (03/02/2014) has stressed the fact that there are parents, caregivers, and teachers that are old and are not familiar with the technology and that there is not enough work done with parents; and where there are attempts to educate parents it is only in functional school governing bodies. Otherwise in general there is not a lot that is done for parents. There is also often power play between teachers and parents in the SGBs where they are functional.

The study has observed that it is important for children to be aware of organizations such as childline which is a non-profit organization that provides counselling to abused and traumatized children and their families and also provides training of other professionals who work with children and

those in child protection units. Subject expert D (04/02/2014) articulated that their organization have a capacity of two people for counselling in a province.

4.2.3 Inter-governmental and other Internet stakeholders collaboration *(Social)*

It was a general feeling by all respondents that government agencies has got different campaigns in tackling the awareness of harmful and illegal Internet content to children.

Google has partnered with Center for Media Literacy, Common Sense Media, ConnectSafely, Enough Is Enough, Family Online Safety Institute, GetNetWise, Internet Keep Safe Coalition, Internet Safety Coalition, National Center for Missing and Exploited Children, CyberTipline, NetSmartz411, National Cyber Security Alliance (NCSA), OnGuardOnline.gov, StopBadware, Stop. Think. Connect, and WiredSafety to form a google family safety centre in 2010. In South Africa the google family safety center partnered with UNICEF was launched in 2012. The center aims to educate the communities about Internet safety.

The latest campaign of by FPB is the Safety Internet Day 2014 held on the 11th of February 2014 (Subject expert C, 03/02/2014). The campaign was only held in Gauteng. The objective of the campaign was to:

- To educate children, parents and care-givers on the existence of child-pornography and the associated dangers and risks to children exposed and involved in the creation, possession and distribution of child-pornography and pornography in general.
- To promote responsible usage and self-regulation whilst using new media cyber-networks and communications technology by children.

- To promote understanding amongst children and parents on the reasons and meaning of the classification tools utilized by the FPB for Film, Games and publications.
- To raise the public profile of cyber-safety and the campaign against child pornography as a means to mobilize the active participation of the stakeholders and interested parties who may be in a position to bring change with their support to the Campaign.
- To promote and advise children, parents and care-givers of the reporting channels for cases of Child-Pornography and related incidents.

This campaign is the collaboration of the google family safety, Mixit, department of communications, Nelson Mandela Children's Fund, Parent's Corner, Media Monitoring Africa, Childline SA, Department of Women, Children and People with disabilities, UNICEF South Africa and FPB. It is not known by the study if the objectives of the campaign were reached.

Mxit has used techniques such as moderation by human intervention where the employees would monitor chat rooms to determine content that is age appropriate for its user base (Subject expert C, 03/02/2014). It has a user base of less than 18 years but also has a user base of 18 plus years. They also has automatic filters that detect age inappropriate content. People also have an opportunity to report bad behaviour. Mxit also report crimes to SAPS where there is online grooming. Mxit has used the advantage of their 6.5 million subscribers to advertise and put broadcast messages on the about the risks of the internet. In this effort they shared information about cyberbullying and meeting strangers online. They get thousands of user comments for the broadcast messages sent.

Telkom Mobile and Telkom Internet are in a process of productising a parental control (Service provider A, 16/01/2014). The parental control will be done on a network level and which is aimed at restricting what the children accesses as set by a parent buying the product.

4.2.4 User-created harmful content *(Social)*

Another finding that was discovered in the interviews was that children can also create their own harmful content. Policy maker B (31/01/2014) has alluded to the fact that children take videos and images of themselves or their friends in compromising circumstances where they are naked or having sex and then share this information with each other. This information sharing not only happens on sms and e-mail but they also use Bluetooth technology.

4.5 Conclusion of the findings

The study reviewed and analysed a considerable amount of legislation, as well as applicable policies and regulations. The study has found that there are a number of policies, legislation and regulations that addresses the intention of the government to bridge the digital divide but most do not addresses risks affecting children on the web.

The findings of this study from sources such as other published academic research reports, and online newspapers has indicated that children are experiencing Internet risks and that sometimes the risks became realities of sexual exploitation and general wellbeing of children was compromised. This is concerning as the Internet community and the government has the responsibility to protect children. The stakeholders from the policy and regulatory environment and Internet Service Providers agreed that while some policy, legislation and regulation was merely adequate, significant

further policy and regulatory decision-making is required to guide, educate and give tools to prevent Internet risks to children, parents, caregivers and schools. Another finding was that there is the lack of intergovernmental collaboration and also collaboration with the private sector. There is work that still needs to be done in South Africa to improve the prevention of Internet risks that affect children.

Chapter 5: Analysis of the findings on harmful and illegal Internet content affecting children

5.1 Introduction

The purpose of this study is to critically analyse the regulatory environment in order to determine the effectiveness of the policies, legislation and regulations that govern harmful and illegal Internet content in order to pre-empt the actions to be taken to prevent risk of harmful Internet content to children. The definition of risk as articulated in Chp1 of the study is the probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action. The study allowed the researcher to understand what the policies, legislation and regulations entailed in terms of prevention and recourse of harmful and illegal Internet content affecting children.

It further gave a perspective of children experiences and risks they face on a daily basis while on the Internet. This chapter provides an analysis of the findings and themes presented in Chapter 4 and aligns the findings with the literature reviewed in Chapter 2. The study used the conceptual framework adapted from Lessig's 1998 model of Internet regulation to analyse the data. The analysis will follow the same order as the findings so as to make this discussion logical to follow. This analysis addresses three major themes that were identified during the research and corresponds with the four sub-questions that are presented in Chapter 3.

5.2 Analysis of the findings on Policies, Legislation and Regulations

The findings of policies, legislation and regulations display the different eras that reflects what the country's ICT issues were, consequently what the country focused on at that particular time. Looking at these eras as a whole the government has made strides to address the interest of children. These developments were to protect children but not necessarily specific to the Internet. The question that the study has is that were these strides enough to alleviate the risks that children experiences on the Internet. It is also evident on this chapter that there is a conflict between the desirability of regulating content and the disadvantages that comes with it. These disadvantages are apparent when they are seen to be interfering with other rights like freedom of speech. The study will debate these two opposing rights as the analysis of the findings are presented.

5.2.1 The Telecom reform era

In the beginning of the period of telecom reform from 1996 to 2005 the focus on regulation was not much on the Internet but on the telecommunication industry. It is to be noted that the Internet penetration in South Africa had not progressed to the levels that it is seen to be at the present moment. The end of the apartheid era was officially in 1994 when the democratic government was elected. This informed the focus of the government at this time. The focus was about the rights of all South Africans as seen in the Constitution as well as to establish universal services so that all South Africans can benefit from telecommunications and broadcasting services.

Internet was the least of the government's worries and that is seen in the policies and the legislation that were established at that time. However this

period laid the foundation that was necessary to provide converged regulations. In this period ICASA was formed which is the body that regulates the then telecommunications and broadcasting industries. This step was very important; as the literature reflect technological convergence of services, there is a need to have one authority that has the responsibility to tackle both the broadcasting and telecommunications issues *(legal)*.

The challenges that the regulator faces in the present moment is that of corporate convergence as articulated in the literature where a single company can provide mobile services, broadband, digital television, cloud, tablets and new media technologies allowing an operator who was licensed under one category to be able to do things that would have required different category of licences in the past *(technological)*.

This era provided for law that regulated electronic transaction and e-commerce as seen in the ECT Act of 2002. The Act has a section on cybercrime that concentrates on unauthorised access to information systems, computer related extortion, fraud and forgery *(legal)*. The Act does not address accessing of harmful Internet content to children or even illegal Internet content in this case online child pornography.

Child pornography has always been illegal as articulated in the Child Care Act 74 of 1983 (RSA, 1983). However in terms of harmful Internet content there was a gap. Another law provided in this era was for regulating films and publications; the Act focused on the classifications of movies and publications in the broadcasting arena *(social)*. Unlike the Internet, broadcasting is regulated with less challenges as it provides for classifications of films and when those films can be aired. X-rated movies can be aired at night when it is presumed that most of the children are asleep. While there might be children that are awake at midnight, most of the

children are asleep. On the other hand Internet provides all content all the time with no time limit.

As the years progressed there were subsequent amendments made on the Films and Publication Act of 1996 that encompassed the elements of harmful and illegal Internet content. Subject expert A has stated that this law among others do tackle the risks of access to Internet by children however he said the implementation thereof is lacking. Subject expert A articulated that there are few police that have an understanding of how to deal with cases where a child has been exposed to explicit and sexual Internet content; furthermore they have no idea how to preserve evidence in those situations *(legal)*.

The government introduced the e-Education policy with its objective being to ensure that all South African learners can use ICTs confidently and creatively to help develop their skills and knowledge and to be able to participate in the global community (DoE, 2004). The policy however fails to address any risks that comes with the access and use of the ICT. It is the opinion of Policy maker B that the policy is addressing issues of access at a macro level and there is no connection of implementation at the micro level. This means the while the government has good intentions to connect children in schools as revealed in the policy *(micro level)*, teachers are not equipped on Internet safety and how to prevent harmful content *(micro level)*.

This era had no focus on the Internet risks that children experiences. Furthermore there were no regulations that the study came across on ICT issues.

5.2.2 Protection of women and children era

This period was the era where women and children welfare was at the centre of government concerns among other issues. In the period of 2005 to 2010 the study determines that there was more focus on women and children's protection. There is an establishment of the Children's Act. The children's Act recognises section 28 of the Constitution of South Africa on the rights of children. It is generic in the protection of children and it is inclusive to the risks that children may experience on the Internet *(social)*.

Sexual offences Act after repealing and replacing many provisions under the Sexual offences Act explicitly provides for the protection of women and children on any form of sexual violation whether in a physical or Internet format *(social)*. The Sexual offences Act does indeed cover the protection of children against the exposure to Internet pornography and child pornography. Other legislation can learn from the Sexual offences Act.

The study also observes that in this era the government put focus on the establishment of the information society where all South Africans including children will be included in the education of the use of ICT services and devices. The study observes the establishment of the ISAD plan as a vehicle to fulfil this role. This plan does not address in any way the risks associated with ICT services. It is the opinion of the study that every initiative that is addressing broadband access must not just stop at that, but have to provide for the education of all users on the Internet risks and how to prevent them *(social)*.

The study observes that while there were legislation that addressed the risks of Internet access and content, there is no consistency in the legislation in addressing Internet risks that affects children which is a shortfall.

5.2.3 The technological era

The technological era is the time where priority of access to ICT services had intensified, and therefore the risks of Internet access were highlighted. The Broadband Policy (2010) was introduced to facilitate the provisioning of affordable, accessible, universal access to broadband, the policy did not address any Internet risks affecting children yet access to broadband is in the core of the Internet risks *(technological and social)*.

The study observes a progression in awareness of the Internet risks affecting children by government and trying to circumvent these risks by establishing the Internet and Cellphone Bill. This bill was rejected by many including women and LGBTI organizations as it was making it illegal to distribute or permit the distribution of pornography by Internet and mobile service providers as well as equating women and children's rights; furthermore the Bill was taking a protectionist approach to women's rights (Shackleton, 2010).

While on the surface it could be argued that women and women's organisations should be pleased with the draft Bill as it barns pornographic content that can be viewed as promoting sexism and the objectification of women's bodies, it is clear that there is no straightforward answer towards the society's issues *(social)*. This draft bill reiterates the fact that there should be a balance between the desirability of regulating content and the disadvantages that affect other rights like freedom of speech *(legal)*. This was a controversial bill which caused a lot of Internet stakeholders to be against it and it is still to be seen if it will be put to law.

Protection from Harassment Act that was established in 2011 proves to the continuous protection of women and children in this era. In the Act the

person harassed can apply for a protection order from court, it is also highlighted by Snail (2013) that children can apply for a protection order which is an enormous endeavour to ensure protection of children.

Protection from Harassment Act addresses the issues of cyberbullying however the Act will be effective if the victim of harassment is aware of who is their harasser. This can be a difficult task as those who bullies others on the Internet often attempt to remain anonymous *(technological)*. This issue is seen as a challenge as it means police investigators must be able to trace the harasser; it is the opinion of Subject expert A that few police are equipped to do these kind of investigations. Therefore the study asks the question of how practical is the Protection from Harassment Act of 2011 when it comes to identifying the perpetrator of harassment. The Act assumes that you will know the person that harasses you and that may not be attestable when it comes to the Internet. It is the concern of the study that while the country has existing legislation and regulations it is important that the implementation is practical.

The study acknowledges that the economical factor plays a big role in policy making.

5.2.4 Legislation about jurisdictional boundaries

As previously articulated in the study one of the characteristics of the Internet is being borderless. Harmful and illegal Internet content can be accessed and hosted anywhere in the world. Provision has to be made to ensure that national courts has jurisdiction in respect of offences and offenders *(legal)*. Watney (nd) makes an example of the complications of jurisdiction in that “if a South African citizen makes available a film containing child pornography via a website hosted outside South Africa where such material is not

unlawful, he has not committed the offence of possession of the film in South Africa". Section 90 of the ECT Act of 2002 addresses such jurisdictional issues. This section of the Act provides for the national courts to have jurisdiction where the offence was committed by a South African citizen or a person with permanent residence in the South Africa or by a person carrying on business in the Republic of South Africa (RSA, 2002). This is irrespective of where the website is hosted.

Furthermore the Act provides that the national courts have jurisdiction where an offence is committed in South Africa, or the preparation towards an offence is committed in South Africa, or where any results of the offence had an effect in South Africa (RSA, 2002). The section also provides for the national courts to have jurisdiction over transportation including any offence committed on board any ship or aircraft registered in South Africa or on a voyage or flight to or from South Africa at the time that the offence was committed.

South Africa is also involved with the international organizations in preventing Internet risks affecting children; some of its many involvements is realized by being a signatory in the international treaty of the Budapest convention (Subject expert A). Budapest convention is an international agreement that addresses cybercrime and aims to harmonize the national laws and establishing cooperation against cybercrime.

5.2.5 Service provider's responsibility to prevent harmful and illegal Internet content

The question that the study needs to tackle is that are Internet service providers and content providers including mobile service provider's bestowed with enough responsibility to prevent harmful and illegal Internet content. It is

observed that according to the ECT Act of 2002, service providers are mere conduit meaning that they are intermediary in providing “access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system” (RSA, 2002). An interesting finding is that Service provider A seemed to not know if they are obligated by law to prevent harmful and illegal content or not. The respondent articulated that it is quite expensive for service providers to implement firewalls for filtering harmful and illegal Internet content however on the positive side their company is looking at productizing parental controls on the network (*economic*). Though the study does not interrogate the economic factor as it requires an in-depth understanding of price regulation which is beyond the level of detail required to understand the foundational policy and regulatory issues, the study acknowledges that the economic factor plays a vital role for policy making. In order for the Service providers to provide this kind of protection on the Internet, policy makers could consider incentives for the implementation thereof. The respondent also mentioned that the responsibility of preventing harmful and illegal content lies with the parents.

Service providers need to play a very big role in effort to prevent harmful and illegal content. It is the study’s view that more should be done to prevent children from accessing harmful Internet content. However most of the respondents had an opinion that even if the law provides for more responsibilities for the service providers, there is not much that the legislation and regulations can do if the implementation of these regulations is not forthcoming. Therefore the implementation and the monitoring of these responsibilities is vital to make sure that protection is ultimately provided to children.

5.3 Analysis of the findings on Internet regulation principles

The literature review had introduced concepts of the Internet that are central to the debates about the desirability of regulating Internet content and the disadvantages that comes with it. These concepts also brings perspective of the models of Internet regulation that South Africa is using.

5.3.1 Harmful Internet content vs illegal Internet content

The literature differentiates harmful Internet content and illegal Internet content, where child pornography is illegal while online pornography is harmful to children but legal when viewed by adults (Akdeniz, 2001). This statement is true for South Africa; the Sexual Offences Act 32 of 2007 criminalizes child pornography, while ECT Act of 2002 addresses Internet harmful content by providing for ISPs to take down websites that are hosted with them when a public member alerts them of the harmful content they contain. This statement brings a strong debate when it comes to regulating Internet content. The desirability of the government to regulate Internet content with the intention of protecting children has a contradictory outcome of interfering with the legal adult content. This debate is demonstrated by a situation in 2009 when the Films and Publications Act was amended in an attempt to regulate child pornography and hate speech. The amendments required every print and online publication not recognized by the press ombudsman to submit potentially “pornographic” or “violence-inciting” materials to the FPB for approval and imposed criminal penalties for noncompliance (Freedom house South Africa, 2013). These amendments were however ruled as being “unconstitutional, based on the conclusion that the pre-screening of publications (including Internet content) would affect the value of news and be an unjustifiable limitation on freedom of expression” (ibid). This ruling was also upheld by the Constitutional court in September

2012. Another example was the attempt of the government to introduce the Internet and cellphone bill which made it illegal for Internet and mobile service providers in the South Africa to distribute or permit the distribution of pornography, this bill was contested and was never passed into law. These are practical examples of how intricate regulation of Internet content is and that there is a need for the government to strike a balance and not violate other rights while attempting to regulate Internet content.

Subject expert B supports the notion of the government striking a balance; he indicated that the nature of the Internet its openness and therefore there should be avoidance at all costs to try to close it down with heavy regulations. Furthermore he stated that Internet regulation should be thin, making it flexible to allow adaptability as technology dictates.

5.3.2 Modes of Internet regulation

Another concept of the Internet reflected in the literature is the four modes of Internet governance; which are self-regulation, government regulation, co-regulation and user-empowerment. South Africa is observed to be using co-regulation and self-regulation methods. The government is at the forefront of putting policies, legislation and regulations that are inclusive in regulating the ICT industry. The study views South Africa as using co-regulation. The co-regulation is depicted in the ECT Act by providing for limitation of liability to ISPs on illegal and harmful content if the ISP is a member of representative body where its members are subject to a code of conduct and where the representative body is capable of monitoring and enforcing its code of conduct (RSA, 2002). Another demonstration of co-regulation is observed in the EC Act of 2005 where the Act requires ICASA to develop a code of conduct for broadcasters and stipulates that all broadcast licensees must adhere to this code of conduct unless they are a member of a body which

has proved to the satisfaction of ICASA that its members subscribe and adhere to a code of conduct enforced by that body (RSA, 2005b). These industry bodies are among others the Broadcasting Complaints Commission of South Africa (BCCSA), Advertising Standards Agency (ASA), Internet Service Provider's Association (ISPA) and Wireless Application Service Providers' Association (WASPA). Co-regulation involves active participation of both the government and all Internet stakeholders, therefore South Africa is better positioned to balance the desirability of regulating the Internet with the disadvantages thereof.

User empowerment is recognised by the study as one of the important modes of Internet regulation that is lacking in South Africa *(social)*. The findings on ISAD plan, White Paper on e-Education, ECT Act of 2002, and ICT policy Green paper reveals the promotion of universal access to ICT by communities including children to build an information society and knowledge economy. In the aforementioned policy and legislation, user empowerment is not addressed. This is also observed by most of the respondents who highlighted the lack of awareness of Internet risks and education by children, parents, and guardians. They articulated that parents, teachers and communities do not have the deeper understanding of the Internet risks particularly in the rural areas or in parents and teachers that are older and have slight understanding of the technologies that have evolved presently.

However there are efforts made by Internet stakeholders such as Mxit, google, department of communications, Nelson Mandela Children's Fund, Parent's Corner, Media Monitoring Africa, Childline SA, Department of Women, Children and People with Disabilities, UNICEF South Africa and FPB to advance Internet safety awareness by having a Safety Internet Day (SID) where 200 schools in Gauteng were invited (Subject expert C; Policy maker A; and Regulator B). This highlights the fact that there are some

efforts made in attempting to educate the users about the Internet risks affecting children. The question is that are these efforts enough and are they also carried out in the nationally including rural areas and previously disadvantages areas in the urban environment? The study has not found enough evidence to suggest that this is the case. Therefore it is concerning considering that Internet penetration using cellphones has significantly increased in the rural and previously disadvantages urban areas communities.

5.2.5 Nanny State versus Self-Regulation

The study has articulated that South Africa is inclined towards co-regulation, another question that relates to this finding is whether South Africa is a nanny state or has an element of self-regulation. The literature compares the United States, Sweden and China to understand the different extents of Internet regulations. As the study was exploring the methods of Internet regulation employed in South Africa these three countries gave perspective on the diverse methods of Internet regulation. United States is regarded as overprotective or interfering unduly with personal choice or a 'nanny state'; while Sweden is regarded as self-regulatory or 'laissez faire' that promotes self-regulation. China on the other hand is regarded as more restrictive or authoritarian.

Understanding the method of Internet regulation employed in South Africa is of importance to the study in order to appreciate the strengths and weaknesses. When exploring this concept it is observed in the aforementioned incidents of the Internet and Cellphone Bill together with the amendments of the Films and Publication Act that South Africa has attempted to bring laws that were too restrictive that were rejected by the community.

The findings from the interviews reveal interesting perspectives of Internet regulation in South Africa. Subject Expert D saw South Africa as not having enough regulations, while Subject Expert A thought South Africa is having sufficient regulations because they have “copied” the regulations from international regulations, and lastly the third perspective by Subject Expert B is that South Africa should have thin Internet regulations because Internet was meant to be an open platform. Observing these opposing perspectives confirms the difficulty that the policy makers have in addressing the Internet risks affecting children.

The study interprets South Africa as having elements of a nanny state in the broader social development setting, which is evident in the policies and regulations that were investigated. However from the findings this does not apply to Internet regulation, as there is lack of provisions in most of the legislation and regulations for Internet regulation. South Africa is also not a self–regulated environment. Striking a balance of over restriction and open Internet will continue to be a challenge that the policy makers needs to balance. Presently reviews on outdated legislation and regulation should be the focus of the government.

5.4 Analysis of the findings on children’s experiences

This section analyses the findings on how South African children has experienced in reality the risks that are found on the Internet. The analysis of the findings is highlighted in the same manner as it was presented in Chapter 4 for ease of understanding.

5.4.1 Interpretation on findings on experiences of harmful Internet content

The study observes that the children in South Africa do stumble on online pornography accidentally in some occasions. The finding reveals three researches that confirm this as a fact. These surveys were conducted in different times by different sources. In Chetty and Basson (2006) 's survey seventy percent of 948 children surveyed reported to have come across pornographic images on digital mediums accidentally while sixty four percent of the students were exposed to pornographic digital images shared on digital mediums.

In their research that surveyed 1000 young people between the ages of 12 to 25 the Young people research unit (2011) discovered that thirty percent of the participants were faced with the unwanted discussion about sex online, while 12.6 percent had been asked to do something sexual online and twenty percent has come across website with pornographic material

In the other survey where FPB (2008) had presented 604 questionnaires and 37 interviews not only was the twenty two percent of the students exposed to Internet content of sexual nature and nudity but fourteen percent of the participant who were exposed to this content also had sexual advances made to them. This implies that there is a risk that children may respond positively or negatively towards these sexual advances depending on the child state of mind.

These researches outline the fact that even in the existence of legislation such as Films and Publication Act children are still exposed to online pornographic material. The literature articulates the use of technical tools to prevent harmful and illegal content, it explores several tools to filter the

content which are the classification of URLs, the Internet community ports where parents and schools chooses the zone in which Internet content will be sorted according to what the user chooses, and many other tools like net nanny where parents can restrict Internet content. The question is even with the filtering tools do parents understand how to use them? The study has revealed the lack of education on the Internet risks affecting children, therefore it is not clear if most of the parents are aware of these filtering mechanisms or would be able to know how to use them.

5.4.2 Interpretation on findings on experiences of online grooming

Findings on online grooming reveals that children are still groomed on the Internet by adults to meet with them. The researches that were conducted shows that children talk to strangers every day. In another study by de Lange and von Solomon (2011) it is revealed that 40 percent of the students surveyed met with someone in person after chatting with them online. Thirty percent reported meeting with a stranger in person who differed significantly from what was anticipated. There were also two similar cases by Smillie and Tromp (2010) and by Geduld (2011) where a 15 year old was drugged and raped after meeting with a 27 year old man on Mxit, while the latter case was that of three men who raped a 20 year old after she communicated with one of the men on Mxit.

These studies confirms that online grooming is happening in South Africa despite the existence of laws such as Sexual offences Act. Respondents I highlighted that there are measures put in place at Mxit which educates users on their safety online. Furthermore Mxit has chat rooms that are grouped according to age and can filter content according to the age groups. People has the ability to call a callcenter to report bad behaviour as stipulated in their terms and conditions. The question is how many social

networks has the same mechanisms presented to children? It is the study's opinion that not all social networks give the kind of services that Mxit is giving.

5.4.3 Interpretation of findings on experiences of cyberbullying

Findings indicated that South African children are bullied online. There are several cases that substantiate the claim as articulated in chapter 4. Despite the Protection from harassment Act there are still acts of cyberbullying that is experienced by children and in other instances by adults. Looking at the Protection from harassment Act it is ex-post meaning that you first need to be bullied before you ask for a protection order therefore the Act does not prevent the harassment from happening but rather prevents it from occurring further. Cyberbullying is a complicated Internet risk to deal with as the child might not know who is bullying them because of the Internet nature of anonymity. This requires some investigations from the school and parents to determine who the perpetrator is. That is if the child has reported cyberbullying to their parents or the teacher. Literature has highlighted that cyberbullying has the "capacity to intrude at any time of day or night into places that might otherwise offer respite and sanctuary like homes and bedrooms" (UNICEF, 2011).

The literature had addressed filtering as one of the factors to prevent Internet risks experienced by children. Unfortunately cyberbullying cannot be prevented by filtering tools as it is an act that is done by another party in more platforms than just websites that will be filtered on the Internet. Cyberbullying can occur on e-mails, sms, social networks, chat rooms etc. where an individual had used false identification so that they may not be traceable. An example is if a child does not have access to social networks such as Facebook, Twitter or Mxit and something bad is said about them on

these platforms, those children who have access will spread the word which will ultimately get to the intended bullied child. The recourse for cyberbullying is provided by the Protection of Harassment Act, which has its own abovementioned challenges of identifying the harasser.

5.5 Analysis on the findings of themes on harmful and illegal Internet content affecting children

This section analyses the themes that were derived from the interview process. In this regard, analysis of the following themes was undertaken; Internet safety education and awareness and intergovernmental collaboration as well as with other Internet stakeholder. The study has articulated that the theme of adequacy of policies, legislation and regulations has been analysed and interpreted as part of analysis of policies, legislation and regulations in section 5.2.

5.5.1 Internet safety education and awareness

Findings shows that government together with the private sector has attempted to facilitate Internet safety education amongst children. However it has been articulated by most of the respondents that Internet safety education and awareness is not done enough in South Africa (Policy maker A; Subject expert A; Subject expert B; Subject expert C; Subject expert D).

Although the study has highlighted the importance of parents, communities, and school teachers in the attempt to prevent harmful and illegal Internet content, findings show that there is lack of attention on educating these Internet stakeholders. As the government rolls out computers and Internet in schools nationally, not only do teachers need to be equipped with the skills of

using these computers but they also need to be empowered with the knowledge of how to minimize harmful and illegal Internet content.

5.5.2 Collaboration of government agencies with themselves and together with other Internet stakeholders

Findings show that there are initiatives to educate children and parents on Internet risks affecting children and how these risks can be managed. These initiatives are conducted in a silo by the government agencies. Furthermore the initiative that the study has been privy to was in Gauteng Province. The government agencies do involve the private sector but each department have their own separate initiatives to address the education and awareness of Internet safety. Collaboration of these initiatives is necessary to ensure a national coverage of the audience that will benefit in Internet safety education. Not only should urban area schools benefit from these initiatives as articulated by Subject expert B, Subject expert C and Policy maker B, but rural areas need to be added in these initiatives.

5.5.3 The dynamics of technological challenges

The study has discovered that harmful content does not only have to be accessed only from the Internet. Technologies such as bluetooth is another medium of transmitting content. When explaining this concept Subject expert A gave an example of when a boy is in the toilet and another boy takes a picture of his private parts while urinating, the image can be transmitted from one mobile phone to the other using the above mentioned technologies and can go viral, moving from one mobile phone to the other using bluetooth.

Further to the challenge mentioned above Watney (nd) articulates that online pornography is not confined to the content on websites but may also be distributed in the form of spam. In such a case the receiver never requested

it and the sender of the spam might not be identifiable, as he or she may have used a spoofed address. It is to be noted that although the Internet was initially developed for a user-server relationship, a peer-to-peer file sharing computer systems network is based on a client-client relationship with the consequence that pornography may be exchanged between the users. However, the policing of the content of files being distributed between users in terms of peer-to-peer networking may not be simplistic especially if encryption is used; and online pornography may also be distributed by means of encrypted e-mail attachments.

5.6 Conclusion on the Analysis

The eras of legislation and regulations presented by the study has revealed that there are few legislation that addresses harmful and illegal Internet content however most of the legislation and regulations are legacy that still exist in the present moment. The study has also revealed that South Africa is inclined to a co-regulatory mode of Internet regulation which helps in balancing the desirability of Internet regulation with the disadvantages thereof. Children are still vulnerable on the Internet as they still stumble onto online pornography; are still cyberbullied and are still groomed online by adults with sexual intentions and lastly children do give out their details to strangers and in some cases even meet with strangers they have met on the Internet.

With legislation and regulation available to address the Internet risks affecting children, the question is why South African children still experience Internet risks. The answer is based on the fact that not only legislation and regulation are able to minimise the Internet risks affecting children but the combination of other factors of social and technology plays a role. There are however positive encounters where the legislation was used to prevent an

ongoing grooming by an adult. Findings shows that the Protection of harassment bill was applied for a parent to get an interdict after a Durban woman had become obsessive and manipulative to his 17-year-old matric daughter whom she had met on MXit chatroom (Versluis, 2008).

Chapter 6: Conclusions and Recommendations

6.1 Introduction

This chapter summarizes the discussions of the previous chapter focusing on key factors affecting effective Internet regulation and themes thereof. The research is the qualitative study with a phenomenological approach. The purpose of the study was to establish the effectiveness of policies, legislation and regulations in preventing harmful and illegal Internet content affecting children. This chapter summarizes the discussions of the previous chapters focusing on the key themes that emerged from the research. In order to understand this, the study investigated how the different policies, legislation and regulation address the risks on the Internet; as well as the experiences of children that were negatively affected by their interactions on the Internet; furthermore the roles of the Internet stakeholders and how they can be better utilized and lastly how technologies particularly mobile affect Internet regulation.

Understanding the aspects that were investigated helps draw conclusions on how the harmful and illegal Internet content can be addressed thereby answering the primary research question of the study. This study encourages government to better understand the aspects related to Internet regulation, and provides recommendations for consideration by the government and its agencies. The limitations of this study and possible future research questions are discussed.

The study recognizes the benefits that the Internet and associated technologies can bring to the society and children with a huge potential to transform lives. As articulated by UNICEF (2011) Internet is a central part of young people's social life and the way they have become integral to modern society and are now an intrinsic part of young people's social lives.

6.2 The role of the policies, legislation and regulations in preventing Internet risks affecting children

The study sort to understand the role of policies, legislation and regulations in preventing harmful and illegal Internet content. It was observed by the study that none of the policies and regulations were found to address Internet risks affecting children, instead it was few legislation that was addressing these risks. Recommendation is to review outdated legislation and increase regulations that addresses these Internet risks. This includes regulations that can prescribe the design of pornographic websites. For example the regulation can prescribe that the first page of the website does not show any pornographic images and they have a warning that indicates that the content is for adults' consumption only. The notice needs to have a dialog box that prompts if a user wants to continue with the adult content. The study has not proven that warnings on cigarettes packets reflecting that smoking kills and on certain alcohol beverages that warns consumers of the fact that alcohol restricts their capacity to drive are effective. However it is the opinion of the study that this will prevent exposure of many children who accidentally landed in the pornographic website. Furthermore to curb the economic difficulty of Service providers as articulated by Service Provider A policy makers can incentivise them to implement the security infrastructure necessary to prevent harmful and illegal Internet content. This can include but not limited to tax cuts.

Answering the sub-question in Chapter 3 that stipulates "to what extent does policies, legislation and regulations address cybercrime affecting children?" although not all policies, legislation and regulations addressed the risks of Internet access, it is the conclusion of the study that there are legislation that addresses harmful and illegal Internet content. However most of the legislation are outdated and that does not address the present challenges

that are exacerbated by the dynamic technology changes. The study therefore recommends a review of legislation to address the technological changes.

The study also observes that the legislation and regulations that are in place depend on others to address Internet risk, meaning that when in court a perpetrator cannot be prosecuted without referring to other laws to convict a person. Common laws and criminal laws will have to be used to help with the prosecution. The study recommends that all policies, legislation and regulation advocating an increase in broadband and Internet access needs to address Internet risks affecting children.

Policy, legislation and regulation is not always the answer if it cannot be translated to implementation. The study's findings shows that while legislation and regulations are focused on national level the actual transgressions happen in the schools, at home, churches, night clubs etc. and that there is no translation from the macro level which is national to the micro level which is in the homes. Policy maker B articulates that in the schooling system regulation of the Internet is still emergent. This implies that the implementation of the legislation and regulation should be clear and concise to summarize what individual law enforcements individuals including parents, teachers and guardians need to do.

The other recommendation is that the law should allow for tools needed to get perpetrators to be available. For example parents whose children are experiencing cyberbullying need to have tools to identify the perpetrator on the Internet so that they can be able to approach the court and ask for protection order as provided in the Protection of Harassment Act of 2011.

Since most of the legislation that the study explored are ex-post, the study recommends that the government should have more ex-ante laws to ensure prevention of the Internet risks as opposed to ex-post laws that takes effect after the offence has been committed.

Policies, legislation and regulations addressing Internet risks need to be in line with the relevant international standards to ensure that South Africa does not become a target country deemed to have the least children protection. Government should promote the collaboration and communication with other governments.

6.3 User empowerment

User empowerment is one of the important conceptions necessary for a successful Internet regulation. The policies, legislation and regulations can be as precise as possible however the prevention of Internet risks affecting children cannot be successful without the empowerment of the users, thus making the effort null and void. It is therefore imperative for the study to give this attention. The study has divided user empowerment into two sections, which is empowerment of children and empowerment of the Internet community including parents, guardians, teachers and government agencies.

6.3.1 Empowering children

Young people's exploratory nature enables them to access the many benefits of the Internet in terms of education, culture and creativity and that is what the government and communities aspire to. Contradicting this phenomenon is the fact that it is the nature of experimentation, exploration and interest in defining themselves socially and sexually that put them into the identified Internet risks especially online grooming (UNICEF, 2011). It is imperative that

when finding solutions children are involved in developing and implementing protective measures that make sense to them; in that way the strategies of protecting them will have their buy-in and will be easier for them to comply.

Recommendations of the study is for government, parents, teachers and guardians to ensure that children have the best possible information about the nature of the Internet risks as well as empowering them to take necessary actions to prevent exposure to harm. Children need to know where to go for help, recognizing that they, themselves, are a key source of much of that help. This can be achieved by adding Internet risks education as a curriculum at schools; providing children with necessary support like knowing that there are adults that they can go to for advice and help when faced with Internet risks; having hotlines where they can call when they need advice and help when faced with any Internet risk. Subject expert D had articulated that childline has capacity of two counsellors per province, these counsellors can be increased to improve the capacity childline can provide so that more children can be accommodated.

The study recommends that children be involved as campaigners and utilize their unique insights and experiences to inform the development of more effective protection. When tackling cyberbullying, schools should have campaigns that drives a message that cyberbullying is “uncool”. In this way every child will know that it is “uncool” to bully other children. They should have a platform to report anybody they suspect to be bullying other children. Additionally, there should be online support that is able to pre-empt abusive situations. This can be achieved for example by a website with an icon on the home page that allows children who are worried about the behaviour of someone communicating with them to click and share their concerns which is then linked to childline.

Some children will continue to behave in risky ways regardless of the information provided to them, through their essence of exploration, lack of awareness of the implications of their actions both socially and in terms of the nature and consequences of technology, misplaced confidence that they are in control, and assumptions that it is others, not themselves, who are at risk (UNICEF, 2011). The study recommends that when these children experiences Internet risks there must be support mechanisms at schools and government areas to counsel them.

6.3.2 Empowering the community

For the purpose of this study parents, guardians, teachers, owners to Internet cafes, government individuals and any individual that work with children will be called the Internet community. The Internet community is an integral part of the process of empowering children. It is articulated in the study that preventing harmful and illegal Internet content is multi-faceted and empowering the community is one such important aspect. The study recommends programmes that inform the Internet community about the benefits and risks associated with Internet access, what strategies can be employed by children to keep safe, where to find help, and the importance of dialogue and engagement with their children. Researches about children's safety should to be accessible and made palatable not only to academics but also to wide range of people by making it simple to understand and digest as proposed by Subject Expert B.

The abovementioned programmes will enable Internet communities to be vigilant and identify harmful and illegal Internet content thus addressing the concerns with the relevant ISPs. EC Act of 2002 provides for ISP to take down websites when notified by the users. This will only happen if the Internet community is aware of this provision and be able to take steps

accordingly. When reviewing the ECT Act as recommended by the study, the ease at which people can inform ISPs of the take down notification is important.

It is also important for the Internet community to be able to recognize warning signs and symptoms of children affected by harmful and illegal Internet content so that such children can receive the necessary help; through the educational programmes this can be achieved. Simple measures such as ensuring that a web browser is set to 'safe search' can provide added protections for children, yet few parents may not know how to put that in place.

6.4 Inclusive model of all Internet stakeholders

The fragmented approach of dealing with the prevention of Internet risks affecting children does not maximise efficiencies. There is a need for more systematic and coordinated processes across government and involving all relevant agencies, if effective protection of children is to be achieved. This is articulated in Chapter 5 of the study. Presently several government departments have their own initiatives of Internet safety education. Content providers are also partnering with government agencies separately. All efforts needs to be combined to get the necessary traction and to ensure that the Internet safety campaigns cover all parts of the country including rural areas.

It is not possible to access the Internet without the services of an ISP, and thus the study recognizes the vital role ISPs has to fulfil in addressing the Internet risks. Despite the fact that ISPs are considered to be conduit, they are the obvious targets to enforcement of Internet safety principles. It is this reason that the study recommends that ISPs and content providers be given

statutory responsibilities in terms of filtering harmful and illegal content and report any discovery of such illegal Internet content to the police. Furthermore a more inclusive model of ISPs and content providers is for them to provide free filtering software as well as free filtering lessons on how to use the software. Self-regulation by ISPs which is already in place is encouraged.

6.5 Balancing over restriction and open Internet

The study has observed resistance to attempts to introduce or amend laws that are seen to be violating other rights like freedom of expression. Therefore it is important for the government to ensure that there is a balance between over restriction and the freedom of expression. The study recommends that South Africa The study recommends the establishment of forums where this balance is discussed especially when there is a new law or amendments to proposed laws. This recommendation will promote self-regulatory environment where Internet stakeholders including government will make informed Internet policies and regulations.

6.6 Future Research Question

Although this study revealed the gaps that needs to be filled to ensure effective and proactive prevention of Internet risks, this study was limited in terms of interviewing children and parents. Furthermore this study is in the centre of a dynamically changing technology. A potential future research question could investigate how to translate legislation and regulation into implementation.

6.7 Conclusion of the harmful and illegal Internet content affecting children

Internet access and use has not only changed the communication dynamics, behaviour and habits of children, but has also had a huge impact on many dimensions of business, culture, politics, sport and society. These media types are also increasingly impacting on the way in which interpersonal relationships between people are formed.

In the beginning of the study, the study was inclined to finding answers from the policies, legislation and regulations that regulate harmful and illegal Internet content that affect children. Subsequently the study discovered that the phenomenon of Internet regulation including the prevention of Internet risks affecting children is very complex and is multi-faceted. There is no single notion that brings the solution but different factors needs to be considered. Furthermore concentrating on one factor and neglecting the other factors constitute a disaster. It is concluded that it is not only the laws and regulation can prevent the Internet risks but that Internet safety education, intergovernmental collaboration to Internet education, and service providers' involvement are equally important in effectively preventing the Internet risks.

It has also appeared that any chance of success of legislation and regulation is dependent upon all the modes of Internet regulation which is co-regulation and user empowerment; furthermore there must be a unified international effort. South Africa has positioned itself as a global player and it needs to continue collaborating with International and national organizations.

Empowering both children and the Internet community is equally important at preventing the Internet risks. The application of existing legislation (ECT Act of 2002) will be unsuccessful without the sustained contribution of ISPs and

individual Internet users in taking down the websites with harmful content and reporting to the police those with illegal content. This will require the proactive commitment of the Internet community to apply a moral judgment and to act in accordance thereof. Service providers have a moral obligation to be more involved and not to sit by the side lines while earning profits of Internet access and consumption of Internet applications.

References

Akdeniz, Y. (2001). Internet content regulation - UK Government and the Control of Internet Content, *Computer Law & Security Report vol 17 no.5., Elsevier Science Ltd.*

Australian Government. Department of Broadband Communication and the Digital Economy. (nd). Protect your children. Retrieved April 20, 2013, from http://www.staysmartonline.gov.au/home_users/protect_your_children

Babbie, E & Mouton, J. (2001). *The practice of Social research*. Oxford Southern Africa.

Badenhorst, C. (2011).Legal responses to cyberbullying and sexting in South Africa. Centre for justice and crime prevention Issue No. 10. Retrieved from http://www.cjcp.org.za/articlesPDF/32/Issue%20Paper%2010-1.pdf

Barlow, J. (1996). A declaration of the independence of cyberspace. Barlow@eff.org. Retrieved from https://projects.eff.org/~barlow/Declaration-Final.html

Bercowitz, B., Madsen, R., & Wulff, F. (nd). Implementing Sovereignty on the Internet. Retrieved 2012 April from http://www-cs-faculty.stanford.edu/~eroberts/cs201/projects/implementing-sovereignity/page1.html

Buys, R & Cronje, F. (2004). *Cyberlaw @ SA II the law of the Internet in South Africa*, Van Schaik publishers, 1064 Arcadia Street, Hatfield, Pretoria.

Carossa, P. (2003). Subsidiarity as a structural principle of international human rights law. Jstor .The American Journal of International Law, Vol. 97, No. 1 (Jan., 2003), pp. 38-79

Chetty,I & Basson, A. (2006). Internet usage and the exposure of pornography to learners in South African schools (Nov. 2006), Film and Publication Board report on. Retrieved October 4, 2012 from http://www.cie.org.za/images/uploads/Report_on_Internet_Usage_2006.pdf

Commission of E-business, IT & Telecoms. (2002). The Impact of Internet content regulation. Retrieved from http://www.iccwbo.org/id510/index.html.

Creswell, JW. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 3rd Edition. Los Angeles: Sage Publications, Inc., 2009.

Delacourt, J. (1997). The international impact of internet regulation. Harvard International L.J 38 (1997) 207 et seq 208.

de Lange, M and von Solms, R. (4 February 2011). Children at Risk of Online Activity. Mail&Guardian. Retrieved from http://mg.co.za/article/2011-02-04-children-at-risk-of-online-bullying

Department of Basic Education. (2004). White paper on e-Education: Transforming learning and teaching through information and communication technologies (ICTs). Retrieved January 27 2014 from http://www.education.gov.za/DocumentsLibrary/Legislation/WhitePapers/tabid/191/Default.aspx

Department of Communications. (2010). 2012 -2013 Strategic Plan. Retrieved October 20, 2012 from http://www.info.gov.za/view/DownloadFileAction?id=144185

Department of Education. (2009). Number of all ordinary schools with or without computer center. Retrieved from http://www.thutong.doe.gov.za/administration/Administration/GeneralInformation/Statistics/tabid/3338/Default.aspx

Dong,F. (2012). Controlling the internet in China: The real story. Convergence: *The International Journal of Research into New Media*. Retrieved from: http://con.sagepub.com/content/18/4/403

d' Udekem-Gevers, M. & Poullet, Y. (2001). Internet content regulation-Concerns from a European User Empowerment Perspective about Internet content regulation: An analysis of some Recent Statements – PART I, *Computer Law & Security Report vol 17 no.6.* Elsevier Science Ltd.

d' Udekem-Gevers, M. & Poullet, Y. (2002). Internet content regulation-Concerns from a European User Empowerment Perspective about content regulation: An analysis of some Recent Statements – PART II, University of Namur, Belgium. *Computer Law & Security Report vol 18 no.1.*

Dutton,WH; Dopatka, A; Hills, M; Law, G; Nash, V. (2011). Freedom of connection Freedom of expression: the changing legal and regulatory ecology shaping the Internet. UNESCO publishing, 7 place de Fontenoy, 75352 Paris 07 SP, Communication and Information Sector, Division for Freedom of Expression, Democracy and Peace. Retrieved from www.unesco.org/webworld

Eberstadt, M & Layden, M. (2010). The social costs of pornography. Statement of findings and recommendations. Witherspoon Institute. Witherspoon Institute 16 Stockton Street, Princeton, New Jersey 08540.

Edwards, G. (8 August 2008). MXit 'slut list' ends in court. New24. Retrieved from http://www.news24.com/SouthAfrica/News/MXit-slut-list-ends-in-court-20080807

Esposito, L. (1998). Regulating the internet: the new battle against child pornography. Case Western Reserve University School of Law. *Case Western Reserve Journal of International Law*.

Fick, J. (2009). Prevention is better than prosecution: Deepening the Defence against Cyber Crime. Lex Informatica 2009: South Africa Cyberlaw and ICT Conference.

Film and Publications Board. (2008). FPB investigation into the Exposure of Children to Sexually Explicit Content through the Internet and Cell phones. Retrieved from http://www.fpb.org.za/research

Freedom House. (2013). Key Developments: May 2012 – April 2013. Retrieved from http://www.freedomhouse.org/report/freedom-net/2013/south-africa

Geduld, S. (July 25 2011). MXit date ends in rape. Retrieved from http://www.iol.co.za/news/crime-courts/mxit-date-ends-in-rape-1.1105240

Gillwald, A. (2005).Good intentions, poor outcomes: Telecommunications reform in South Africa. LINK Centre, Graduate School of Public and Development Management, Witwatersrand University, Box 601, Wits 2050, South Africa. *Science Direct Telecommunications Policy 29 (2005) 469–491.*

Goldstuck, A. (2012) Internet access in South Africa 2012. World Wide Worx backed by MSN online portal.

Greenleaf, G. (2002). Internet Architecture and Governance*. [PowerPoint slides].* Retrieved on 1 August 2012 from http://www.ppt2txt.com/r/33a84528/.

Griffith, E. (March 13, 2013). What Is Cloud Computing? Retrieved June 13 2013 from http://www.pcmag.com/article2/0,2817,2372163,00.asp

Groenewald, T. (2004). A Phenomenological Research Design Illustrated. International Journal of Qualitative Methods. Retrieved April 04 2011 from http://www.ualberta.ca/~iiqm/backissues/3_1/pdf/groenewald.pdf

GSMA. (2011).European Mobile Industry Observatory 2011. Retrieved June 11 2012 from http://www.gsma.com/publicpolicy/wp-content/uploads/2012/04/emofullwebfinal.pdf

Hildenbrand, J. (March 2012). 3 is the new unlimited says AT&T, as they officially change unlimited data plans. Retrieved from http://www.androidcentral.com/3-new-unlimited-says-att-they-officially-change-unlimited-data-plans

Hoff, D & Mitchell,S. (2009). Cyberbullying: causes, effects, and remedies. Emerald Journal of Educational Administration Vol. 47 Issue: 5 pp. 652 – 665.

Huang,I; Guo,R; Xie,H; & Wu, Z. (2012).The convergence of Information and Communication Technologies gains momentum. Huawei Technologies. The Global Information Technology Report 2012. Retrieved April 20 3013 from http://www3.weforum.org/docs/GITR/2012/GITR_Chapter1.2_2012.pdf

ICASA. (2008). ICASA Code of Conduct for Broadcasters (SA). Notice 1580 of 2008 retrieved from http://thornton.co.za/resources/31753_1580.pdf.

Immigration and Customs Enforcement. (April 2013). 2 plead guilty in one of largest child pornography cases in US history. Retrieved from https://www.ice.gov/news/releases/1304/130417shreveport.htm

ITU. (2011). ICT Facts and Figures. Retrieved from http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf

International Center for missing and exploited children. (2008). Child Pornography: Model Legislation & Global Review. Retrieved from http://icmec.org/en_X1/icmec_publications/English__6th_Edition_FINAL_.pdf

ITWeb. (14 May 2012). Internet 'finally' reaches mass market. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=54412:Internet-finally-reaches-mass-market&catid=260.

Johnson, D. & Post, D. (1996). Law and Borders —The Rise of Law in Cyberspace. 45 Stan. L. Rev. 1367 (1996). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=535

Kende, M. (2008). Regulating Internet pornography aimed at children: A Comparative Constitutional Perspective on Passing the Camel through the Needle's Eye. Retrieved from http://www.law2.byu.edu/lawreview/archives/2007/6/7KENDE.FIN.pdf

Kolstad, C.,Uclen, T. & Johnson, G. (1990). Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements? *The American Economic Review, Vol. 80, No. 4, pp. 888-901.*

Kreutzer,T. (2009). Assessing cell phone usage in a South African township school. *International Journal of Education and Development using Information and Communication Technology (IJEDICT), Vol. 5, Issue 5, pp.43-57.*

Landes, D. (2009). Norwegian group joins case against Sweden's wiretapping law.e Retrieved from http://www.thelocal.se/17578/20090213/#.UXuo6L933dk

Lessig, L. (1998). "The New Chicago School." The Journal of Legal Studies, Vol. 27, No. S2 (June 1998), pp. 661-691

Liang, B., & Lu, H. (2010). Internet Development, Censorship, and Cyber Crimes in China. Sage. *Journal of Contemporary Criminal Justice 2010 26: 103 DOI: 10.1177/1043986209350437.* Retrieved from http://ccj.sagepub.com/content/26/1/103

Longe, O., Chiemeke, S., Onifade, F., Balogun, F., Longe, F., & Otti,V. (2007). Exposure of Children and Teenagers to Internet Pornography in South Western Nigeria: Concerns. Trends & Implications. *Journal of Information Technology Impact, Vol. 7, No. 3, pp. 195-212.*

Madon, S. (2000). The Internet and socio-economic development: exploring the interaction, Information Technology & People, Vol. 13 Issue: 2 pp. 85 - 101

Maree,K., Creswell, J., Ebersohn,L., Eloff, I., Ferreira, R., Ivankova, N., Jansen, J., Nieuwenhuis, J., Pietersen, J., Plano Clark, V., and van der Westhuizen, C (Eds.) . (2007). *First steps in research*. Van Schaick Publishers.

Merriam,SB. (2009). *Qualitative research: A guide to design and implementation*. John Wiley & Sons. 989 Market Street, San Frascisco

Meyer, D. (October 12, 2011). RIM explains BlackBerry downtime as outage spreads. Retrieved from http://www.zdnet.com/rim-explains-blackberry-downtime-as-outage-spreads-3040094166/

Miller,C. Thompson, N. and Franz, D. (2009). Proactive Strategies to Safeguard Young Adolescents in the Cyberage. Middle School Journal, Vol. 41, No. 1, pp. 28-34. Published by: Association for Middle Level Education (AMLE). Retrieved from: http://www.jstor.org/stable/23044505

Minne,D. (2009). "Grooming as a precursor to sexual offences against children". KZN child law conference 2009. Retrieved 11 April 2011 from http://www.justice.gov.za/cfw/2009child-law-kzn/day2_paper_SexualGrooming.pdf

Moyle, K. (2012).Filtering children's access to the internet at school. Charles Darwin University Australia. Retrieved from http://www.icicte.org/Proceedings2012/Papers/10-3-Moyle.pdf

Mthimkhulu, Z. (2010). Regulating Freedom? An Examination of the Discourse on Internet Regulation and Freedom of Expression in South Africa (2010).

Münch,M. (2013). Do as the Swedes do? Internet policy and regulation in Sweden – a snapshot. Retrieved from http://policyreview.info/articles/analysis/do-swedes-do-internet-policy-and-regulation-sweden-%E2%80%93-snapshot

Neuman, L. (2011). *Social research methods: Qualitative and quantitative approaches*. Sixth Edition. Pearson International Edition

Ofcom. (2014). Ofcom Report on Internet safety measures Strategies of parental protection for children online. Retrieved from http://stakeholders.ofcom.org.uk/binaries/internet/internet-safety-measures.pdf

Organization of African Unity. (1999). African charter on the rights and welfare of the child. OAU Doc. CAB/LEG/24.9/49 (1990), entered into force Nov. 29, 1999.

Owolade, A. & Snail, S. (2009). Sexual Exploitation in the Online World - a South African Perspective. Lex Informatica 2009: *South Africa Cyberlaw and ICT Conference.*

Pieters, A. & Krupin, C. (2010). Youth Online Behaviour. McAfee. Retrieved November 29 2012 from http://safekids.com/mcafee_harris.pdf

Poulsen, K & Zetter, K. (06.June. 2010). U.S. Intelligence Analyst Arrested in Wikileaks Video Probe. Wired. Retrieved 13 July 2012 from http://www.wired.com/threatlevel/2010/06/leak/

Presidential National Commission on Information Society and Development (PNC on ISAD). (2007). Information Society and Development. Retrieved from http://www.pmg.org.za/report/20090709-department-communications-presidential-national-commission-informatio

Preston, C. (2009). All knowledge is not equal: Facilitating children's access to knowledge by making the Internet safer. *International Journal of Communications law and policy.*

Price, M. & Verhulst, S. (2004). *Self-Regulation and the Internet*. Kluwer Law International. The Netherlands United Kingdom Postal address: PO Box 316 2400 AH Alphen

Provos,N., Rajab,M., & Mavrommatis, P. (2009). Cybercrime 2.0: When the Cloud Turns Dark. Communications of the ACM, vol. 53, no. 4. doi:10.1145/1498765.1498782

Razak, A. (n.d). Understanding Legal Research. Department of Management and Marketing, Faculty of Economics and Management, University Putra Malaysia.

Resnick, P. & Miller, J. (1996). PICS: Internet Access Controls without Censorship. Communications of the *ACM October 1996/Vol. 39, No. 10.* Retrieved http://www.schoolfind.co.za/gauteng-schools.php.

Republic of South Africa. (1983).Child Care Act 74 of 1983. Retrieved from http://www.dsd.gov.za/dmdocuments/Child_Care_Act.pdf

Republic of South Africa. (1996a). Films and Publication Act 65 of 1996. Retrieved from http://www.info.gov.za/view/DownloadFileAction?id=70901.

Republic of South Africa. (1996b).The Constitution of the Republic of South Africa of 1996. Retrieved from http://www.info.gov.za/documents/constitution/1996/a108-96.pdf

Republic of South Africa. (1996c). Telecommunication Act of 1996. Retrieved from http://www.internet.org.za/telecoms_act.html

Republic of South Africa. (2000). ICASA Act of 2000. Retrieved from: http://www.info.gov.za/view/DownloadFileAction?id=101146

Republic of South Africa. (2002). Electronic Communication and Transaction Act No.25 of 2002. Retrieved from http://www.acts.co.za/ect_act/index.htm.

Republic of South Africa. (2005a). Children's Act 38 of 2005. Retrieved from http://www.westerncape.gov.za/Text/2010/12/childrens.act.final_regulations26_jan_2010.pdf

Republic of South Africa. (2005b). Electronic Communication of 2005. Retrieved from http://www.info.gov.za/view/DownloadFileAction?id=67890

Republic of South Africa. (2007). Sexual Offences and Related Matters Amendment Act, No. 32 of 2007. Retrieved from http://www.justice.gov.za/legislation/acts/2007-032.pdf

Republic of South Africa. (2010). Broadband Policy for South Africa. Retrieved from http://www.info.gov.za/view/DownloadFileAction?id=127922

Republic of South Africa. (2011). Protection from Harassment Act of 2011. Retrieved from http://www.justice.gov.za/legislation/acts/2011-017.pdf

Republic of South Africa. (2013). South Africa Connect: Creating opportunity, ensuring inclusion South Africa's Broadband Policy. Retrieved from www.gov.za/documents/download.php?f=205142

Republic of South Africa. (2014). National integrated ICT Policy Green Paper. Chapter 6. Retrieved from http://www.doc.gov.za/documents-publications/category/22-national-integrated-ict-policy-green-paper.html

Rose, AC. (2011). Censorship and Content Regulation on the Internet . Pennstate University. Retrieved from https://wikispaces.psu.edu/display/IST432SP11Team9/IST+432+-+Team+9+-+Censorship+and+Content+Regulation+on+the+Internet

Shackleton, S. (6 July 2010). Justifiable protection or entrenching patriarchy? Pornography and the internet in South Africa. Association for Progressive Communications. Retrieved from http://www.apc.org/en/node/10726/

Shinder, DL. (2002). *Scene of the cybercrime*. Chapter 1.Computer Forensics Handbook. Syngress Publishing, Inc.800 Hingham Street, Rockland, MA 02370

Snail, SL. (2013). Cyber crime (South African Perspectives) and Child Protection online. *[PowerPoint slides].*

Smillie, S and Tromp, B. (August 6 2010). Teen in Mxit rape ordeal. Retrieved from: http://www.iol.co.za/news/south-africa/teen-in-mxit-rape-ordeal-1.672193#.Uawrv8sayK0

Smith L. (2008). The new challenges of cybercrime. Federal Sentencing Reporter, Vol 20. No. 5. University of California Press on behalf of the Vera Institute of Justice. Retrieved from http://www.jstor.org/stable/10.1525/fsr.2008.20.5.356

Snyder,M. (May 31st, 2012). 18 examples of the nanny state gone wild. Retrieved from http://theeconomiccollapseblog.com/archives/18-examples-of-the-nanny-state-gone-wild

Soy, K. (1997). *The case study as a research method*. Unpublished paper, University of Texas at Austin. Retrieved from http://www.gslis.utexas.edu/~ssoy/usesusers/l391d1b.htm.

Statistics South Africa. (2012). General household survey 2012. Statistical release P0318. Retrieved from: http://www.statssa.gov.za/Publications2/P0318/P0318August2012.pdf

Stoker,G. (1998). Governance as theory: five propositions. United Nations Educational, Scientific and Cultural Organization. Retrieved from http://classwebs.spea.indiana.edu/kenricha/Oxford/Archives/Oxford%202006/Courses/Governance/Articles/Stoker%20-%20Governance.pdf

Tavani, H. (2006). Regulating cyberspace: concepts and controversies. Department of Philosophy, River College, Nashua, New Hampshire, USA. Emerald. Vol. 25 ISS: 1pp. 37-46.

Tongco, DC. (2007). Purposive Sampling as a Tool for Informant Selection. Department of Botany, University of Hawai`i at Manoa, 3190 Maile Way, Honolulu.

Tubbs, B. (8 May 2012). Cellphone ban in schools – the right move?. ITWeb. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=54226

United Nations. (2000). United Nations Convention against Transnational organized crime and the protocols thereto. United Nations Office on drugs and crime.

United Nations. (2002). Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. A/RES/54/263 of 25 May 2000 entered into force on 18 January 2002. Retrieved from http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx

United Nations. (2009). Convention on the rights of the child. CRC/C/GC/12. 20 July 2009 GE.09-43699 (E) 280709.

UNICEF. (2007). Reforming child law In south africa: Budgeting and implementation planning. UNICEF IRC publications Communications Unit, UNICEF Innocenti Research Centre Piazza SS. Annunziata, 12 50122 Florence, Italy.

UNICEF. (2011). Child Safety Online Global challenges and strategies. UNICEF IRC publications Communications Unit, UNICEF Innocenti Research Centre Piazza SS. Annunziata, 12 50122 Florence, Italy.

UNICEF, Beger,G, Hoveyda, P and Sinha, A. (2011), From 'What's your ASLR' to 'Do You Wanna Go Private?', UNICEF. Retrieved from http://www.UNICEF.org/southafrica/SAF_resources_mxitstudy.pdf

UNICEF, Beger,G, Sinha, A. (2012). South African mobile generation. Retrieved from http://www.UNICEF.org/southafrica/SAF_resources_mobilegeneration.pdf

Van Wyk, E. (2010-11-07). Pupils film girl's gang-rape at school. City Press newspaper. Retrieved from: http://www.citypress.co.za/SouthAfrica/News/Pupils-film-girls-gang-rape-at-school-20101107.

Versluis,J. (2 April 2008). Judge stops obsessive MXit saga. News24. Retrieved from http://www.news24.com/SouthAfrica/News/Judge-stops-obsessive-MXit-saga-20080401

Watney, M. (nd). Regulation of Internet pornography in South Africa. Retrieved from http://www.isrcl.org/Papers/2005/Watney.pdf

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., & Grove-Hills, J. (2010 p7). European Online Grooming Project for the European Commission Safer Internet Plus Programme, London. Retrieved 28 November 2012 from http://www.europeanonlinegroomingproject.com/wp-content/file-uploads/EOGP-Project-scoping-report.pdf

Westerlund, M. (2011). The production of pro-suicide content on the internet: A counter-discourse activity. Sage Publications Retrieved April 20 2013 from http://nms.sagepub.com/content/14/5/764

West, C. (2012). Pornography and Censorship. *The Stanford Encyclopedia of Philosophy.* Edward N. Zalta (ed.). Retrived from http://plato.stanford.edu/archives/win2012/entries/pornography-censorship/

World Wide Worx. (2011). The Mobile Internet in South Africa 2011. Retrieved from www.worldwideworx.com.

(Nov 2012). African Undersea cables. Retrieved from: http://manaypossibilities.net/african-undersea-cables/

Xiao, Y.,Ye,J., Chen, R., Tang, M. (2012). Research on Quantitative Model of Risk Assessment for Amusement Rides. China Special Equipment Inspection and Research Institute, Beijing, China. Guangxi Construction Machinery Manufacturing Co., Ltd, Nanning, China. Atlantis Press, Paris, France

Yin, R. K. (1994). *Case study research: Design and methods* (2nd ed.). Newbury Park, CA: Sage Publications.

Young people Research Unit. (2011). Age-inappropriate viewing and online victimization among South African Young people. Bureau of Market Research, Unisa, May 2011.

Appendices

Appendix A: Document Analysis

Document Analysis was performed on the legislation relating to harmful and illegal Internet content and access affecting children.

The questions that will be posed to all the legislation undergoing document analysis are below and will be the same for all of them. They are:

- To what extend does regulation address internet child pornography?
- To what extend does the regulation addresses address online pornography accessed by children?
- To what extend does regulation address online sexual grooming?
- To what extend does regulation address inappropriate website content?
- To what extend does the legislation address cyberbullying?

Appendix B: Research questionnaire

Dear Sir/Madam

I am Goitsemang Mthethwa, currently working towards completion of the degree, Master in Management ICT Policy and Regulation (MMICTPR), at the University of Witwatersrand (WITS). The curriculum consists of coursework and research, which involves compilation of a Research Report.

My research focuses on the **Internet regulation of harmful content that affects children**. The study identified several sources of data, and one is to obtain information from Regulators, Service Providers personnel and Subject Matter experts on observed issues. Your contribution is going to help me complete the work. The questions are presented in an open ended format:

Open ended questions:

Requires an elaborative response on the views you have in relation to the questions. You are therefore kindly requested to assist by answering the questions that follow, to the best of your ability and understanding. This study attempts to establish the effectiveness of the South African law and regulations with regards to internet content that affects children negatively. Children experiences risks by accessing Internet, these risks include cyberbullying, access to pornography and child pornography, internet grooming etc. The reason for the study is to establish how South African children can be protected from the internet access risks which are increasing with the proliferation of devices that have internet access.

All your responses will be held in strict confidence; findings will be summarised and no statements used in the report will be attributed directly to you. The interview will take approximately 30-45 minutes and with your permission the proceedings will be recorded.

Thanking you
G.M Mthethwa

Topic: Internet Regulation of Harmful Content Affecting Children

INTERVIEW SCHEDULE

There are **4 sections** in this Questionnaire
Section A is for the Subject Matter experts
Section B is for Service Providers
Section C is for the Policy Makers and Regulators
Section D is for Industry Bodies

SECTION A: Subject matter experts

How does the country deal with jurisdictional boundaries with regard to Internet regulation, Is the legislation and regulation covering the technological advances experienced today, is the existing legislation effective to curb illegal Internet content, how can the legislation be improved to cover all the new technological advances?

1. How can the country deal with jurisdictional boundaries in regulating Internet?

2. What are the challenges that face the Policy makers and Regulators with regard to the current technological advances? **Probe:** What can be done?

3. How can the Policy makers and Regulators address the risks in the technologically advancing world?

4. To what extent is the awareness of schools with regards to the addressing sexting, online impersonation, cyberbullying and forwarding pornographic material?
   Probe: What about parents?

5. Do you think the legislation, policies and regulations that deals with children's safety on the Internet are effective? and why?

6. What are the factors that needs to be considered to ensure the effectiveness of legislation and regulation in Internet regulation?

7. Do you think Service Providers are given enough responsibility in terms of preventing access to online pornography?

8. What changes and improvements are required?

9. Is there anything you would like to add?

SECTION B: Service providers

What measures strategies, interventions and tools are in place to identify and filter harmful and illegal content, how effective is the turndown notification process, is the existing legislation effective to curb illegal Internet content, is the legislation and regulation cover the technological advances experienced today, how can the legislation be improved to cover all the new technological advances?

1. What measures do firms put in place to identify and filter harmful and illegal content?
   Probe: Which strategies, interventions and tools does your company employ for identification and filtering?

2. The law provides for Internet Service Providers to take down a website after receiving a turndown notification. How many turndown notifications to you receive in a month?

3. In complying with the legislation and regulations governing the services that you give how do you deal with technological changes?

4. Do you think the legislation, policies and regulations that deals with children's safety on the internet effective? and why?

5. What are the factors that needs to be considered to ensure the effectiveness of legislation in Internet regulation?

6. What changes and improvements are required?

7. Is there anything more you would like to add?

SECTION C: Policy makers & Regulators

How does the policy maker or regulator deal with jurisdictional boundaries with regards to Internet policies, to what extent is these regulations in line with the current technological advances and challenges they bring?

1. How can the country deal with jurisdictional boundaries in regulating Internet?

2. To what extent is the awareness of schools with regards to the addressing sexting, online impersonation, cyberbullying and forwarding pornographic material?
   Probe: What about parents?
3. What are the challenges that face the policy makers and regulators with regard to the current technological advances in accessing Internet?

4. Do you think the Policies, Legislation and Regulations that deals with children's safety on the internet are effective? and why?

5. What are the factors that the Policy maker and Regulator considers to ensure the effectiveness of legislation and regulation in Internet regulation?

6. What changes and improvements are required?

7. Is there anything more you would like to add?

SECTION D: Industry bodies

How does the industry bodies align with the legislation and regulation that govern that policies, to what extent is these regulations in line with the current technological advances and challenges they bring?

1. How can the country deal with jurisdictional boundaries in regulating Internet?

2. What are the challenges that face the Industry bodies with regards to aligning with the legislation and regulations?

3. What are the challenges that face the policy makers and regulators with regard to the current technological advances in accessing Internet?

4. Do you think the legislation, policies and regulations that deals with children's safety on the internet effective? and why?

5. To what extent is the awareness of schools with regards to the addressing sexting, online impersonation, cyberbullying and forwarding pornographic material?
   Probe: What about parents?

6. What are the factors that needs to be considered to ensure the effectiveness of legislation in Internet regulation?

7. What changes and improvements are required?

8. Is there anything more you would like to add?

Appendix C: Details of Interview Respondents

Respondent	**Company/ Institution**	**Focus**	**Type of Interview**	**Date of Interview**
Regulator A	ICASA	Regulator	Telephone	(13/01/2014)
Regulator B	Films and Publication Board	Regulator	Telephone	(13/01/2014)
Policy maker A	Department of Communications	Policy Maker	Telephone	(14/01/2014)
Policy maker B	Department of Education	Policy Maker	Telephone	31/01/2014
Service provider A	Telkom Internet	Internet Service Provider	Face to Face	16/01/2014
Subject expert A	Snail Attorneys @ Law Inc	Subject Matter Expert	Face to Face	16/01/2014
Subject expert B	Convergence Partners	Subject Matter Expert	Face to Face	20/01/2014
Subject expert C	Mxit	Content Provider	Telephone	03/02/2014
Subject expert D	Childline	Subject Matter Expert	Telephone	04/02/2014