THE LIABILITY OF INTERNET SERVICE PROVIDERS
FOR UNLAWFUL CONTENT POSTED BY
THIRD PARTIES

N.D. O’BRIEN

2010
THE LIABILITY OF INTERNET SERVICE PROVIDERS FOR UNLAWFUL CONTENT POSTED BY THIRD PARTIES

By

N.D. O’BRIEN

Submitted in fulfilment of the requirements for the degree of MAGISTER LEGUM

in the Faculty of Law at the Nelson Mandela Metropolitan University

January 2010

Supervisor: Prof F. Marx
I would like to extend my thanks to the following people:

- To my parents and Emma Taggart for their help, encouragement, sacrifice and support;
- To my supervisor, Prof Marx, for his assistance and guidance;
- To Dawn Prinsloo, at the NMMU Library, for providing me with her time and guidance;
- To Ms. Fourie, the Law Faculty Officer, for her always prompt and friendly assistance;
- To Mr. Ant Brooks and the Internet Service Provider Association, for providing me with a variety of interesting information and insights.

Without their invaluable assistance I would not have been able to have completed this work.
Internet Service Providers (ISP’s) are crucial to the operation and development of the Internet. However, through the performance of their basic functions, they faced the great risk of civil and criminal liability for unlawful content posted by third parties. As this risk threatened the potential of the Internet, various jurisdictions opted to promulgate legislation that granted ISP’s safe harbours from liability. The South African (RSA) response is Chapter XI of the Electronic Communications and Transactions Act (ECTA). The protection it provides is however not absolute. It is limited to ISP’s that are members of an Industry Representative Body (IRB) and those ISP’s must perform particular functions in relation to third party content in a certain manner to obtain limited liability. Due to the ECTA’s limited application and a lack of authority, the question is raised as to what is the liability of ISP’s for unlawful content posted by third parties? This dissertation pays particular attention to ISP liability for third party defamatory statements, hate speech, and obscene and indecent material.

The role and characteristics of ISP’s in the functioning of the Internet is described. It is determined that a wide legal definition would be required to encompass the many roles they perform. The definition provided by the ECTA is wide and many different types of ISP can fall underneath it. This may have unintended consequences as entities may receive protection that the legislature did not intend.

The appropriate laws in the United States of America (USA) and the United Kingdom are surveyed and suggestions as to the extent of ISP liability in circumstances where the ECTA does not apply are made. It is established that their position is uncertain due to difficulties in applying the law to the Internet. This could result in the law being applied incorrectly and ISP’s erroneously found liable.

The ECTA’s threshold requirements limit the availability of the safe harbor provisions to ISP’s that are members of a recognised IRB. The IRB must comply with an extensive set of requirements to obtain recognition. The purpose of these requirements is to ensure that only responsible ISP’s obtain the protection provided by the act. After an examination of these
requirements, their necessity is questioned as their purpose appears to be contrary to the logic of the safe harbours provided by the ECTA.

The safe harbours are analysed and comparisons made to similar legislation that exists in the USA and the European Union (EU). It was established that the ECTA is a hybrid of the USA and EU legislation, and to a certain extent improves on them. It was suggested that the extent of ISP liability in relation to certain unlawful content is clearer under the ECTA. However, exceptions may exist in relation to hate speech and obscene and indecent content as a result of legislation that does not properly take the technology of the Internet into account. It was recommended that certain action be taken to correct this position to prevent any negative effects on the Internet industry and conflict with the objectives of the ECTA.

The provision of limited liability contained in the ECTA is balanced with a notice and take-down procedure, which provides relief to victims of unlawful content. This procedure is analysed and it appears to be effective in providing relief. However, through an examination of concerns raised in relation to this type of procedure as it exists in the USA and the EU, it is suggested that certain flaws exist. The take-down procedure negatively effects the freedom of expression and the third party’s rights to due process. Further, the threshold requirements result in not all the users of the Internet being provided with the same remedies. It is recommended that certain action be taken to correct these flaws.

The solution provided by the ECTA should be favoured over the uncertainty that existed before it promulgation. It may be necessary to correct particular flaws that exist. Certain recommendations are suggested in this regard and the concluding chapter.
KEYWORDS

- Internet Service Provider liability
- Electronic Communications and Transactions Act
- Online intermediary liability
- Defamation
- Hate Speech
- Obscenity
- Child Pornography
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFACE</td>
<td>i</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>ii</td>
</tr>
<tr>
<td>KEYWORDS</td>
<td>iv</td>
</tr>
<tr>
<td>TABLE OF CASES</td>
<td>xiii</td>
</tr>
<tr>
<td>TABLE OF LEGISLATION</td>
<td>xvi</td>
</tr>
<tr>
<td>CHAPTER ONE: INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1. General</td>
<td>1</td>
</tr>
<tr>
<td>2. Internet Service Provider liability</td>
<td>3</td>
</tr>
<tr>
<td>3. Legislation limiting ISP liability</td>
<td>4</td>
</tr>
<tr>
<td>4. The South African situation</td>
<td>4</td>
</tr>
<tr>
<td>5. Research objectives</td>
<td>6</td>
</tr>
<tr>
<td>6. Methodology</td>
<td>6</td>
</tr>
<tr>
<td>7. Chapter Outline</td>
<td>7</td>
</tr>
<tr>
<td>CHAPTER TWO: WHAT IS AN ISP?</td>
<td>8</td>
</tr>
<tr>
<td>1. Introduction</td>
<td>8</td>
</tr>
<tr>
<td>2. What is the Internet?</td>
<td>8</td>
</tr>
<tr>
<td>3. How does the Internet function?</td>
<td>9</td>
</tr>
<tr>
<td>3.1 Internet Protocol addresses</td>
<td>11</td>
</tr>
<tr>
<td>3.2 Protocols</td>
<td>12</td>
</tr>
<tr>
<td>4. Common applications on the Internet</td>
<td>13</td>
</tr>
<tr>
<td>4.1 The World Wide Web</td>
<td>13</td>
</tr>
<tr>
<td>4.1.1 Domain name system</td>
<td>15</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>2 3 3</td>
<td>Suggestions for determining ISP liability for third party defamatory content in South Africa</td>
</tr>
<tr>
<td>3</td>
<td>Hate speech</td>
</tr>
<tr>
<td>3 1</td>
<td>Hate Speech: United States of America</td>
</tr>
<tr>
<td>3 1 1</td>
<td>Hate speech and the Internet</td>
</tr>
<tr>
<td>3 1 2</td>
<td>ISP liability for third party hate speech in the United States of America</td>
</tr>
<tr>
<td>3 2</td>
<td>Hate Speech: United Kingdom</td>
</tr>
<tr>
<td>3 2 1</td>
<td>ISP liability for third party hate speech in the United Kingdom</td>
</tr>
<tr>
<td>3 3</td>
<td>Hate speech: South Africa</td>
</tr>
<tr>
<td>3 3 1</td>
<td>Films and Publications Act</td>
</tr>
<tr>
<td>3 3 2</td>
<td>Promotion of Equality and Prevention of Unfair Discrimination Act</td>
</tr>
<tr>
<td>3 3 3</td>
<td>Suggestions as to the extent of ISP liability for third party hate speech in South Africa</td>
</tr>
<tr>
<td>4</td>
<td>Obscenity and indecency</td>
</tr>
<tr>
<td>4 1</td>
<td>Obscenity and indecency: United States of America</td>
</tr>
<tr>
<td>4 1 1</td>
<td>The test for obscenity in the United States of America</td>
</tr>
<tr>
<td>4 1 2</td>
<td>Indecency in the United States of America</td>
</tr>
<tr>
<td>4 1 3</td>
<td>Regulation of obscenity and indecency on the Internet</td>
</tr>
<tr>
<td>4 1 4</td>
<td>ISP liability for third party obscene and indecent content in the United States of America</td>
</tr>
<tr>
<td>4 2</td>
<td>Obscenity and Indecency: United Kingdom</td>
</tr>
<tr>
<td>4 2 1</td>
<td>Obscene Publications Act</td>
</tr>
<tr>
<td>4 2 2</td>
<td>Protection of Children Act</td>
</tr>
<tr>
<td>4 2 3</td>
<td>Criminal Justice and Immigration Act</td>
</tr>
<tr>
<td>4 2 4</td>
<td>ISP liability for third party obscene and indecent content in the United</td>
</tr>
</tbody>
</table>
CHAPTER FOUR: REQUIREMENTS TO OBTAIN LIMITED LIABILITY IN TERMS OF THE ECTA

1 Introduction

2 Conditions for eligibility

3 Guidelines for the recognition of Industry Representative Bodies

3.1 Principles upon which the Guidelines are based

3.2 Objective and scope

3.3 Best practice code of conduct

3.4 Adequate criteria for membership

3.5 Monitoring and enforcement of the IRB’s code of conduct

4 Internet Service Providers Association

5 Comparison of the South African approach to the European Union

6 Criticism of the threshold requirements
CHAPTER FIVE: DEFENCES AVAILABLE TO ISP’S IN TERMS OF THE
ECTA

1  Introduction........................................................................................................ 103
2  A brief comparison of safe harbour legislation........................................... 103
3  The safe harbours contained in the ECTA............................................... 108
3 1  Mere Conduit............................................................................................ 108
3 1 1  Comparison with the EU Directive....................................................... 109
3 2  Caching................................................................................................. 110
3 2 1  Comparison with the EU Directive....................................................... 111
3 3  Hosting....................................................................................................... 112
3 3 1  Comparison with the EU Directive....................................................... 113
3 4  Information location tools........................................................................ 115
3 4 1  Comparison with the Digital Millennium Copyright Act..................... 115
4  Criticism of the defences.............................................................................. 116
5  No general obligation to monitor................................................................. 116
5 1  Comparison with the EU Directive and the Digital Millennium Copyright
   Act.................................................................................................................. 117
6  ECTA’s savings section................................................................................. 118
7  Extent of ISP liability with the application of the ECTA............................. 118
7 1  General....................................................................................................... 118
7 2  Defamation................................................................................................ 119
7 3  Hate Speech.............................................................................................. 119
7 4  Obscenity and indecency.......................................................................... 120
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Are ISP’s overprotected?</td>
<td>120</td>
</tr>
<tr>
<td>9</td>
<td>Recommendations</td>
<td>122</td>
</tr>
<tr>
<td>10</td>
<td>Conclusion</td>
<td>122</td>
</tr>
<tr>
<td></td>
<td><strong>CHAPTER SIX: NOTICE AND TAKE-DOWN PROCEDURE</strong></td>
<td>123</td>
</tr>
<tr>
<td>1</td>
<td>Introduction</td>
<td>123</td>
</tr>
<tr>
<td>2</td>
<td>Notice and take-down procedures</td>
<td>123</td>
</tr>
<tr>
<td>2 1</td>
<td>United States of America</td>
<td>123</td>
</tr>
<tr>
<td>2 2</td>
<td>European Union</td>
<td>126</td>
</tr>
<tr>
<td>2 3</td>
<td>South Africa</td>
<td>127</td>
</tr>
<tr>
<td>2 3 1</td>
<td>ECTA</td>
<td>127</td>
</tr>
<tr>
<td>2 3 2</td>
<td>Guidelines for the recognition of an industry representative body</td>
<td>128</td>
</tr>
<tr>
<td>3</td>
<td>Comparisons between the notice and take-down procedures</td>
<td>128</td>
</tr>
<tr>
<td>4</td>
<td>The Internet Service Providers Association</td>
<td>130</td>
</tr>
<tr>
<td>4 1</td>
<td>ISPA’s notice and take-down procedure</td>
<td>130</td>
</tr>
<tr>
<td>4 2</td>
<td>ISPA’s Code of Conduct Complaints procedure</td>
<td>131</td>
</tr>
<tr>
<td>4 3</td>
<td>ISPA’s notice and take-down procedure in practice</td>
<td>133</td>
</tr>
<tr>
<td>5</td>
<td>Concerns related to the notice and take-down procedures</td>
<td>134</td>
</tr>
<tr>
<td>5 1</td>
<td>Appropriateness of expanding the procedure to all forms of unlawful content</td>
<td>134</td>
</tr>
<tr>
<td>5 2</td>
<td>The negative effect of notice and take-down procedures on the freedom of expression</td>
<td>135</td>
</tr>
<tr>
<td>5 2 1</td>
<td>Negative effect of on the freedom of expression: Digital Millennium Copyright Act</td>
<td>138</td>
</tr>
<tr>
<td>5 2 2</td>
<td>Negative effect on the freedom of speech: EU Directive</td>
<td>139</td>
</tr>
<tr>
<td>5 3</td>
<td>Limitation on the third party’s right to defend himself</td>
<td>141</td>
</tr>
<tr>
<td>5 4</td>
<td>Negative effect on the growth of the Internet</td>
<td>141</td>
</tr>
</tbody>
</table>
Lack of an adequate balance between ISP liability and protection of Internet users................................................................. 142
Relevance of these concerns to South Africa................................. 144
Recommendations...................................................................... 146
Conclusion.................................................................................. 149

CHAPTER SEVEN: CONCLUSION AND RECOMMENDATIONS ............ 150
Summary of findings.................................................................... 150
Conclusions drawn...................................................................... 152
ECTA.......................................................................................... 153
Promotion of Equality and Prevention of Unfair Discrimination Act.... 155
Films and Publications Act............................................................ 155
Recommendations...................................................................... 155
ECTA.......................................................................................... 155
Promotion of Equality and Prevention of Unfair Discrimination Act.... 156
Films and Publications Act............................................................ 157
Concluding remarks................................................................... 157

BIBLIOGRAPHY.......................................................................... 158
# TABLE OF CASES

**BELGIUM**

*SABAM v SA Scarlet* District Court of Brussels No 04/8975/A Decision of 29 June 2007

**REPUBLIC OF SOUTH AFRICA**

*De Reuck v Director of Public Prosecutions* 2004 (1) SA 406 (CC)

*Kruger v Coetzee* 1966 2 SA 428 (A) 430

*Lascon Properties (Pty) Ltd v Wadeville Investment Co (Pty) Ltd and another* 1997 (4) SA 578 (W)

*Mthembi-Mahanye v Mail &Guardian Ltd and another* 2004 (6) SA 329 (SCA)

*National Media Ltd and Others v Bogoshi* 1998 (4) SA 1196 (SCA)

*Pakendorf v De Flamingh* 1982 3 SA 146 (A)

*Suid-Afrikaanse Uitsaaiikorporasie v O’Malley* 1977 3 SA 394 (A)

*Tsichlas and another v Touch Line Media (Pty) Ltd* 2004 (2) SA 112 (W)

**UNITED STATES OF AMERICA**

*Abrams v United States* 250 US 616 (1919)

*American Civil Liberties Union v Reno* 31 F Supp 2d 473 (ED Pa 1999)


*Barret v Clark* 29 Media L Rep 2473 (Cal App Dept Super Ct 2001)


*Barrett v Rosenthal* SC Cal Alameda County Ct App 1/2 A096451

*Batzel v Smith* 333 F 3d 1018 (9th Cir 2003)

*Blumenthal v Drudge and America Online Inc* 992 F Supp 44 (DDC April 22 1998)

*Center for Democracy & Technology v Pappert* 337 F Supp 2d 606 (ED Pa 2004)

*Chaplinsky v New Hampshire* 325 US 568 (1942)

*Cianci v New Times Publishing Co* 639 F2d 54 61 (2d Cir 1980)

*Columbia/Williamette Inc v American Coalition of Life Advocates* 290 F 3d 1058 (9th Cir 2002)

*Cubby Inc v CompuServe Inc* 776 F Supp 135 (SD NY 1991)

*Davidson v Time Warner Inc* 1997 US Dist LEXIS 21559 (SD Tex 1997)
Ginsberg v New York 390 US 629 (1968)
Herczeg v Hustler Magazine 814 F 2d 1020 (5th Circ 1987)
Kathleen R v City of Livermore 87 Cal App 4th 684 (2001)
Lerman v Chuckleberry Publishing Inc 521 F Supp228 (SD NY 1981)
Lerman v Flynt Distributing Co 745 F 2d 123 139 (2d Cir 1984)
Lerman v Flynt Distributing Co 471 US 1054 105 SCt 2114 85 L Ed 2d 479 (1985)
Lunney v Prodigy Services Company 683 NYS 2d 560 (SD NY 1998)
Lunney v Prodigy Services Company 723 NE 2d 539 (NY 1999)
Mainstream Loudon v Board of the Loudoun County Library 2 F Supp 2d 783 794-95 (ED Va 1998)
Marczeski v Law 122 F Supp 2d 315 327 (D Conn 2000)
Miller v California 413 US 15 (1973)
Olivia v NBC 178 Cal Rptr 888 (Ct App 1981)
Online Policy Group v Diebold Inc 337 F Supp 2d 1195 1203 (ND Cal 2004)
Playboy Enterprises Inc v Frena 839 F Supp 1552 (MD Fla 1993)
Reno v American Civil Liberties Union 521 US 844 (1997)
Rice v Paladin Enterprises 128 F 3d 233 (4th Circ 1997)
Schneider v Amazon.com 31 P 3d 37 42-43 (Wash Ct App 2001)
Sega Enterprises Inc v MAPHIA 857 F Supp 679 (ND Cal 1994)
Smith v California 361 US 147 (1959)
Stoner v eBay Inc 2000 WL 1705637
Stratton Oakmont v Prodigy Services Co 1995 NY Misc LEXIS 229
United States v Thomas 74 F 3d 701 (6th Cir)
United States v Thomas 117 S Ct 74 (1996)
United States v American Library Association Inc 201 F Supp 2d 401 (ED Pa 2002)
Yahoo! Inc v LICRA 145 F Supp 2d 1181 (ND Cal 2001)
Zeran v America Online Inc 129 F 3d 327 (4th Cir 1997)
UNITED KINGDOM

Atkins v DPP (2000) 2 All ER 425 QBD Divisional Court
Carrie v Tolkien (2009) EWHC 29 (QB)
DPP v A and BC Chewing Gum Ltd (1968) 1 QB 159
Firsht v Raphael (2008) EWHC 1781 (QB)
Godfrey v Demon Internet Ltd QBD (1999) 4 All ER 342
R v Fellows, R v Arnold (1997) 2 All ER 548 CA
R v Perrin (2002) EWCA Crim 747
R v Smith and Jayson (2002) EWCA Crim 683
R v Waddon (2000) All ER (D) 502
Sim v Stretch (1936) 2 All ER 1237
Vitzetelly v Mudie’s Select Library Ltd (1900) 2 QB
TABLE OF LEGISLATION

STATUTES

REPUBLIC OF SOUTH AFRICA
Electronic Communications Act 26 of 2005
Electronic Communications and Transactions Act 25 of 2002
Films and Publications Act 65 of 1996
Films and Publications Amendment Act 3 of 2009
Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002

UNITED STATES OF AMERICA
Children’s Internet Protection Act of 2000
Child Online Protection Act of 1998
Child Pornography Prevention Act of 1996
Communications Decency Act of 1996
Copyright Act of 1976
Digital Millennium Copyright Act of 1998
Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003
Telecommunications Act of 1996
Victims of Child Abuse Act of 1990

UNITED KINGDOM
Broadcasting Act of 1990
Criminal Justice and Immigration Act of 2008
Criminal Justice and Public Order Act of 1994
Defamation Act of 1996
Obscene Publications Act of 1959
Protection of Children Act of 1978
Protection of Children Act of 1994
Public Order Act of 1986
Racial and Religious Hatred Act of 2006

EUROPEAN UNION DIRECTIVES

SUBORDINATE LEGISLATION

REPUBLIC OF SOUTH AFRICA

UNITED KINGDOM

BILLS

REPUBLIC OF SOUTH AFRICA
Electronic Communication and Transaction Bill B8-2002
CHAPTER ONE: INTRODUCTION

1 General

The Internet has had a profound effect on the progress and development of humanity.¹ People have greater access to information and each other than ever before.² The Internet provides many benefits such as the free flow of a variety of information, the expansion of the scope of an individual’s freedom of speech, the revolutionizing of communication and the ease that an individual can access these benefits.³ It has been stated that it is a:

“democratic imperative that the common good is best served by the free flow of information…”⁴

The Internet fulfills this imperative and, with all of its benefits, must be recognized as a tool for the common good. Unfortunately, it does lend itself to abuse as the ease of immediate publication and the degree of anonymity afforded to users has created the potential for the infringement of the rights of others.⁵ Examples are:

- The dissemination of defamatory material:
  
  The Internet provides an easily accessible forum to disseminate defamatory content to a wide audience.⁶ Evidence of the extent of this problem can be

---

⁴ National Media Ltd and Others v Bogoshi 1998 (4) SA 1196 (SCA) 1210G.
found in the large number of online defamation cases in the United States of America (USA).  

- **Hate speech:**
  The Internet is used for the dissemination of hate speech, recruiting for hate organisations, promotion of race wars and the advertising and sale of racist entertainment. The extent of the availability of online hate speech has prompted the drafting of international conventions to combat the problem.  

- **Obscenity and Indecency**
  There is a vast amount of pornographic material available on the Internet, with an almost 2000% increase in the number of pornographic websites in a five year period. The ease of access to this content, especially to minors, is cause of great concern. Of even more concern to governments is the amount and ease of access to child pornography online. According to the Internet Watch Foundation there are over five million images of child pornography online. According to the Internet and UNICEF estimates that 90% of all paedophilic activities now involve the Internet.  

These examples illustrate that although the Internet may serve the common good, the great freedom it affords users is abused and it can be a dangerous tool.

---

7 Examples are: Cubby Inc v CompuServe Inc 776 F Supp 135 (SD NY 1991); Blumenthal v Drudge and America Online Inc 992 F Supp 44 (DDC April 22 1998); Lunney v Prodigy Services Company 723 N E 2d 539 (NY 1999).
8 Nel “Freedom of expression” in Cyberlaw 221-222.
9 Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (Strasbourg 28 January 2003 ETS no 189).
13 Van Zyl 2008 THRHR 231.
2 Internet Service Provider liability
A particular problem with the Internet is that it is not always possible to identify the author of the unlawful content.\(^{14}\) However, liability for unlawful content posted on the Internet is not necessarily limited to the author.\(^{15}\) An important party to the transmission of online content is the Internet Service Providers (ISP’s). ISP’s are entities that provide users access to the Internet as well as perform other roles such as: provision of email services, domain name registration, hosting of websites as well as transmission, routing and the receipt of messages.\(^{16}\) ISP’s are attractive targets for litigation as they are easily identifiable and are considered to have ‘deeper pockets’ than the author of the unlawful content.\(^{17}\) Should the desired outcome of a litigant or a regulator be the blocking of an entire category or type of unlawful content, this can be more easily achieved through targeting the ISP rather than an individual author at a time.\(^{18}\) The question therefore arises: What is the extent of the liability of ISP’s for unlawful content posted by third parties? (also referred to herein as ISP liability for third party unlawful content).

There are a wide range of laws that impose civil and criminal liability for unlawful content. Jurisdictions faced the problem of how to apply legal principles developed without cognizance of the Internet to online legal issues, or whether it was even possible to do so.\(^{19}\) There was uncertainty as to the extent of ISP liability and it became apparent that the law was not necessarily easily applicable to the Internet.\(^{20}\) Due to the wide array of law imposing liability and the uncertainty as to the extent of


\(^{15}\) Burns *Communications Law* (2001) 393.


\(^{18}\) For instance, ISP’s have been required to block access from within Germany of neo-Nazi websites. Roos “Freedom of expression” in Van der Merwe (ed) *Information and Communications Technology Law* (2008) 339 442; Reed & Angel *Computer Law* 363.


ISP liability, there was a belief that this potentially threatened the growth of the Internet.\textsuperscript{21} Various jurisdictions promulgated legislation to resolve this problem.\textsuperscript{22}

3 Legislation limiting ISP liability
The legislation that was promulgated in different jurisdictions provides ISP’s with safe harbours from liability. There are at least two forms of this legislation.\textsuperscript{23} The one form provides ISP’s with broad immunity from liability for unlawful content hosted by third parties. An example of this form can be found in the USA, in section 230 of the Communications Decency Act of 1996 (CDA).\textsuperscript{24} Another approach provides ISP’s, which perform certain functions in a particular manner, with limited immunity from liability for unlawful content posted by third parties. Three examples of this form of legislation exist: In the USA, the Digital Millenium Copyright Act (DMCA);\textsuperscript{25} in the European Union (EU), the Electronic Commerce Directive 2000/31/EC (EU Directive);\textsuperscript{26} and in the Republic of South Africa (RSA), the Electronic Communications and Transactions Act 25 of 2002 (ECTA).

4 The South African situation
There is little authority in RSA relating to the management, administration and control of the Internet.\textsuperscript{27} Despite this, the legislature recognized that the risk of civil and criminal liability to ISP’s in RSA law potentially threatened the existence of ISP’s and the effective functioning of the Internet.\textsuperscript{28} In response, ISP’s were provided with protection in Chapter XI of the ECTA.\textsuperscript{29} For an ISP to be eligible for protection it must comply with certain requirements relating to membership of an Industry


\textsuperscript{23} Edwards “The fall” in \textit{Law and the Internet} 49.

\textsuperscript{24} This is Title V of the Telecommunications Act of 1996, Pub L No 104-104 110 Stat 56.

\textsuperscript{25} 17 USC § 512 ff 105 Pub L No 304 112 Stat 2660.


\textsuperscript{27} \textit{Tsichlas and another v Touch Line Media (Pty) Ltd} 2004 (2) SA 112 (W).

\textsuperscript{28} GG 29474 6

\textsuperscript{29} \textit{Ibid}. 
Representative Body (IRB) recognized by the Minister of Communications. This demonstrates the legislature’s emphasis on regulation of the Internet by the industry. Further, the protection of the ECTA is only available to ISP’s that perform particular functions in a certain manner. In certain instances, for an ISP to be able to obtain limited liability it would have to comply with a take-down notice in terms of the Acts notice and take-down procedure. The protection provided by the ECTA is however not absolute. Should an ISP fall outside the Acts protection, its liability will be determined through the normal application of law. This dissertation will attempt to establish the extent of ISP liability for third party unlawful content in relation to three forms of unlawful content: defamatory content, hate speech, and obscene and indecent content. The following questions will be addressed:

- In Chapter Two
  - What is an ISP?

- In Chapter Three
  - What is the extent of ISP liability, in the absence of the application of the ECTA, for defamatory content, hate speech, and obscene and indecent content posted by third parties online?

- In Chapter Four
  - What are the threshold requirements which ISP’s must comply with to be eligible for the protection afforded by the ECTA?
  - What is the importance of an IRB in terms of the ECTA?
  - What are the requirements for the recognition for an IRB by the Minister?

- In Chapter Five
  - What are the safe-harbours available to ISP’s?
  - Is it appropriate for ISP’s to be protected for all forms of unlawful content?
  - Are ISP’s over-protected?

31 GG 29474 7.
33 S77.
• In Chapter Six
  o What are the guidelines for the take-down procedure?
  o Can the take-down notice be abused and hinder the freedom of expression or any other rights?
  o Is the ECTA effective in providing relief for victims of Internet abuse?
  o Does the ECTA provide a balance between ISP accountability and protection of the interests of the users of the Internet in RSA?

5 Research Objectives
The objective of this dissertation is to determine the extent of ISP liability for third party unlawful content in RSA law. Attention will be paid to ISP liability in terms of the law applicable to defamation, hate speech, and obscenity and indecency. The relevant provisions of the ECTA will be analysed. An investigation will be made as to its strengths, weaknesses and its effectiveness in providing ISP’s with protection against liability. An attempt will be made to provide answers to the questions raised above.

6 Methodology
An investigation as to the characteristics of ISP’s and the roles they perform will be undertaken in Chapter Two. The author will conduct in Chapter Three a survey of the appropriate laws from the USA and United Kingdom (UK) to provide suggestions as to the extent of ISP liability in circumstances where the ECTA does not apply. The focus will be on ISP liability for third party defamatory content, hate speech, and obscene and indecent content. In Chapter Four the author will critically examine the threshold requirements that ISP’s must comply with to obtain limited liability and the requirements for the recognition of an IRB. In Chapter Five the author will examine the safe harbours provided by the ECTA and their effect on the extent of ISP liability for the unlawful third party content raised supra. The author will perform a comparison between the ECTA and the appropriate laws from the USA and the EU. In Chapter Six, the author will examine the guidelines for the notice and take-down procedure provided in the ECTA. Comparisons will be made to the appropriate laws from the USA and the EU. Concerns that exist in those jurisdictions in relation to this procedure will be examined with determinations made as to their relevance to RSA.
Chapter Outline

Chapter One: Introduction
Chapter Two: What is an ISP?
Chapter Three: ISP liability in the absence of the ECTA
Chapter Four: Requirements to obtain limited liability in terms of the ECTA
Chapter Five: Defences available to ISP’s in terms of the ECTA
Chapter Six: Notice and take-down procedure
Chapter Seven: Conclusion and recommendations
CHAPTER TWO: WHAT IS AN ISP?

1 Introduction
It is necessary to understand what an ISP is and the role’s that it can perform to appreciate the extent of the legal consequences that can be attached to its actions. However, it will first be necessary to understand what the Internet is, how it functions, the role players involved and the functions they perform to understand what an ISP is.

2 What is the Internet?
The Internet is defined in the Electronic Communications and Transaction Act (ECTA) as:

“… (an) interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof”\(^{34}\)

The Internet is therefore a collective noun\(^ {35}\) as it is a network of networks\(^ {36}\) or collection of networks\(^ {37}\). The networks consist of computers linked to each other either by cables, satellites or other wireless technology. Some computers hold information, while others merely route it to the next point in the network.\(^ {38}\) While networks and individual computers may be controlled by a single entity, the Internet as a whole is not.\(^ {39}\) The Internet therefore consists of:

- hosts, which are computers that store digital information or data,\(^ {40}\)

---
\(^{34}\) S1 of Act 25 of 2002.
\(^{35}\) Reed *Internet Law* 7.
\(^{39}\) Reed *Internet Law* 18; Longworth “The possibilities for a legal framework” in *Law of Cyberspace* 14-15, 18; Evans et al *Technology in Action* 516.
\(^{40}\) Jordaan “Information Technology” in *E-Commerce* 30; Smith *Internet Law* 9; Dean *Enhanced Network* 8-9, 77. The technological term ‘data’ is used in this chapter due to the technological nature of the discussion herein. Data is defined in s1 of Act 25 of 2002 as the electronic representation of information in any form. Information can of course be referred to as content, such as third party content for example: pictures, movies or text.
- routers or switches, which are computers that receive and forward data,\textsuperscript{41} and
- physical layer or pipes, which are telecommunication links or transmission medium between hosts and other devices connected to the Internet.\textsuperscript{42}

The Internet is not the content itself but rather the means via which content is transmitted. Services such as the World Wide Web, e-mail and file downloading, are not provided by the Internet itself, but rather by particular role players.\textsuperscript{43}

3 How does the Internet function?

The Internet is therefore a communication technology\textsuperscript{44} that assists in the transmission of data from one computer to another.\textsuperscript{45} When a user of the Internet requests data from another computer, it is transmitted from the ‘source computer’ (or source host) to the ‘receiving computer’ (or receiving host). The data travels along the best possible route, via routers and switches along some form of cable or wireless technology.\textsuperscript{46} Should a route be overloaded or out of service, the data is transmitted via another route.\textsuperscript{47} The major routes or links between networks is referred to as the Internet backbone.\textsuperscript{48}

The data is not transmitted in a continuous stream directly from the source host to the receiving host.\textsuperscript{49} The data is split by the source host into packets, which are addressed to the receiving

\textsuperscript{41} Longworth “The possibilities for a legal framework” in Law of Cyberspace 14; Smith Internet Law 5; Dean Enhanced Network 43, 275-276, 280-283; Molyneux The Internet Under the Hood: An introduction to network technologies for Information Professionals (2003) 69, 88-89; Evans et al Technology in Action 496-497.

\textsuperscript{42} Jordaan “Information Technology” in E-Commerce 29; Smith Internet Law 5; Molyneux The Internet Under the Hood 109-116; Dean Enhanced Network 8-11, 308-310; Stallings Data and Computer Communications 35, 38.

\textsuperscript{43} Reed Internet Law 8; Smith Internet Law 4-5; Jordaan “Information Technology” in E-Commerce 32; Dean Enhanced Network 25; Evans et al Technology in Action 66.

\textsuperscript{44} Longworth “The possibilities for a legal framework” in Law of Cyberspace 14; Stallings Data and Computer Communications 581; Molyneux The Internet Under the Hood 4.

\textsuperscript{45} Alhadeff & Cohen “Functionality of VANS” in Cyberlaw 232-233; Smith Internet Law 5; Stallings Data and Computer Communications 23, 56.

\textsuperscript{46} Reed Internet Law 8; Jordaan “Information Technology” in E-Commerce 19, 29; Alhadeff & Cohen “Functionality of VANS” in Cyberlaw 232-233.

\textsuperscript{47} Jordaan “Information Technology” in E-Commerce 29; Longworth “The possibilities for a legal framework” in Law of Cyberspace 17; Stallings Data and Computer Communications 587, 626; Alhadeff & Cohen “Functionality of VANS” in Cyberlaw 233.

\textsuperscript{48} Jordaan “Information Technology” in E-Commerce 29; Evans et al Technology in Action 67.

\textsuperscript{49} Longworth “The possibilities for a legal framework” in Law of Cyberspace 14; Stallings Data and Computer Communications 572-573, 587.
host. These are copied from one computer to another during their transmission through the network or networks. The packets may be transmitted to a number of different computers along different routes until reaching the receiving host which reassembles the data upon receipt of the packets. It is not necessary for the packets to follow the same route, arrive at the same time or even in any particular order. The intermediary computers (usually routers or switches) can be seen as mere conduits for data.

With a multitude of packets of data being transmitted over the Internet, bottlenecks in pipes can develop. This results in slower access to the data. There are two solutions to this problem, mirroring and caching. Mirroring of data involves making identical copies of the data on either side of a bottleneck. When data is requested by a user, the host directs that request to the closest mirror site relative to the user’s position. Caching is the automatic temporary copying of data that occurs at a user level as well as by certain Internet application programmes. This process allows for quicker and more efficient access to that data should it be requested again, thus saving time by not having to request that data again from its source. The transmission of data over the Internet is facilitated by the use of Internet Protocol addresses and protocols.

---

50 Reed Internet Law 8-9; Alhadeff & Cohen “Functionality of VANS” in Cyberlaw 232-233; Longworth “The possibilities for a legal framework” in Law of Cyberspace 14; Stallings Data and Computer Communications 572-576, 587; Dean Enhanced Network 198-199; Molyneux The Internet under the hood 27-28, 293; Evans et al Technology in Action 522-523.
51 Reed Internet Law 8; Alhadeff & Cohen “Functionality of VANS” in Cyberlaw 233; Stallings Data and Computer Communications 23, 587.
52 Reed Internet Law 8-9; Alhadeff & Cohen “Functionality of VANS” in Cyberlaw 232-233; Longworth “The possibilities for a legal framework” in Law of Cyberspace 14; Stallings Data and Computer Communications 572-576, 587; Dean Enhanced Network 198-199; Molyneux The Internet Under the Hood 27-28, 293; Evans et al Technology in Action 522-523.
53 Reed Internet Law 8; Longworth “The possibilities for a legal framework” in Law of Cyberspace 14; Stallings Data and Computer Communications 572-576, 587; Dean Enhanced Network 198-199; Evans et al Technology in Action 522-523.
54 Reed Internet Law 20; Stallings Data and Computer Communications 691.
56 Reed Internet Law 20-21; Khumalo “Copyright and the Internet” in Cyberlaw 20; Stallings Data and Computer Communications 763, 765; Dean Enhanced Network 556; Evans et al Technology in Action 528; Roos “Freedom of expression” in ICT Law 425-426.
57 Jordaan “Information Technology” in E-Commerce 27-28; Alhadeff & Cohen “Functionality of VANS” in Cyberlaw 232; Stallings Data and Computer Communications 38-44, 592; Dean Enhanced Network 68-75, 520; Legal Instruments for Combating Racism 45.
3.1 Internet Protocol addresses

All computers or devices that are linked to the Internet have a unique address. This address is referred to as an Internet Protocol (IP) address or number, which consists of numbers between 0 and 255 separated by periods, e.g. 235.46.34.3. The IP address assists computers in finding other computers or devices on the Internet. Any transmission of data over the Internet carries the IP address of the source and receiving host. This is done so that the computers functioning as conduits on the Internet can route the data to the right target. The source host's address is included so that the receiving host may notify it of which packets have or have not arrived. The source host then resends the missing packets.

Users of the Internet cannot always remember the numerical IP addresses. This resulted in the creation of a Domain Name System (DNS), which associates IP addresses of hosts to character based names called domains. A useful analogy is that the IP address and associated domain name is similar to a person’s identity number and that person’s name. The process of association is called domain name resolution. Domain names are registered to IP addresses and


59 Jordaan “Information Technology” in E-Commerce 27-28. 30; Greenberg “Trademarks” in Cyberlaw 36; Smith Internet Law 148; Burns Communications Law 389; Smith Internet Law 148; Stallings Data and Computer Communications 595; Dean Enhanced Network 75-76, 520-522; Molyneux The Internet Under the Hood 94; Evans et al Technology in Action 67; Reed Internet Law 42-43.

60 Jordaan “Information Technology” in E-Commerce 28, 30; Greenberg “Trademarks” in Cyberlaw 36; Stallings Data and Computer Communications 23, 577-578; Dean Enhanced Network 75, 520; Reed Internet Law 42-43; Smith Internet Law 148.

61 Jordaan “Information Technology” in E-Commerce 30; Smith Internet Law 9; Stallings Data and Computer Communications 23, 577-578, 592; Dean Enhanced Network 520; Molyneux The Internet Under the Hood 81, 84, 130-131; Reed Internet Law 42-43.

62 Molyneux The Internet Under the Hood 81, 84, 130-131; Dean Enhanced Network 43,44, 520; Stallings Data and Computer Communications 576-578; Evans et al Technology in Action 527.

63 Jordaan “Information Technology” in E-Commerce 30; Reed Internet Law 31; Greenberg “Trademarks” in Cyberlaw 36; Dean Enhanced Network 534; Molyneux The Internet Under the Hood 86, 157; Evans et al Technology in Action 67; Smith Internet Law 148; Schlossbauer & Wein “The Domain Name System and Internet Governance on the examples of .at Domains and IDNs” in Benedek, Bauer & Kettemann (eds) Internet Governance and the Information Society: Global perspectives and European Dimensions (2008) 141 142.

64 Jordaan “Information Technology” in E-Commerce 30; Reed Internet Law 42; Greenberg “Trademarks” in Cyberlaw 36; Longworth “The possibilities for a legal framework” in Law of Cyberspace 14; Smith Internet Law 9, 148; Dean Enhanced Network 534, 536-537; Molyneux The Internet Under the Hood 157. Schlossbauer & Wein “The Domain Name System” in Internet Governance 142.

65 Greenberg “Trademarks” in Cyberlaw 36-37; Dean Enhanced Network 534.
are kept in DNS hosts. The user enters the domain name into Internet search software, which sends a request to the DNS host to find the IP address associated with that domain name. The DNS host then sends the IP address back to the user’s computer which proceeds to use the IP address to locate the host the user is looking for.66

3 2 Protocols
The transmission and reception of data from one computer to another is governed by rules of communication called protocols.67 A protocol assists in the recognition and dealing of data. It is essential for computers to have the same protocols in order to ensure that data is always represented or dealt with the same way by all computers involved, therefore preserving the integrity of the information.68 To communicate over the Internet, hosts use a layered set of protocols which form the Internet protocol suite:

- The Application layer:
  This layer defines the type of information contained in the packets and what to do with it.69 Examples of this protocol are:
  - Hyper Text Transfer Protocol, which is the basis of the World Wide Web;70
  - Simple Mail Transfer Protocol, Post Office Protocol and Internet Message Access Protocol, which are used for e-mail;71
  - File Transfer Protocol (FTP), which is used for the downloading of files.72

---

66 Jordaan “Information Technology” in E-Commerce 30; Reed Internet Law 42-43; Greenberg “Trademarks” in Cyberlaw 36; Smith Internet Law 9; Dean Enhanced Network 534-537; Molyneux The Internet under the hood 86; Evans et al Technology in Action 67; Smith Internet Law 148.
67 Jordaan “Information Technology” in E-Commerce 28; Alhadeff & Cohen “Functionality of VANS” in Cyberlaw 232; Stallings Data and Computer Communications 20; Dean Enhanced Network 67; Molyneux The Internet Under the Hood 9; Evans et al Technology in Action 517.
68 Reed Internet Law 11-13; Alhadeff & Cohen “Functionality of VANS” in Cyberlaw 232; Jordaan “Information Technology” in E-Commerce 30; Stallings Data and Computer Communications 20-23; Dean Enhanced Network 67-68.
69 Reed Internet Law 13; Stallings Data and Computer Communications 23, 38-39, 43; Dean Enhanced Network 70, 74-75.
70 Reed Internet Law 13; Jordaan “Information Technology” in E-Commerce 28; Stallings Data and Computer Communications 762; Dean Enhanced Network 556, 569; Molyneux The Internet Under the Hood 199.
71 Reed Internet Law 13.
72 Reed Internet Law 13; Jordaan “Information Technology” in E-Commerce 31, 33-34; Stallings Data and Computer Communications 43; Dean Enhanced Network 75, 554-555, 570; Molyneux The Internet under the hood 4, 288.
This allows a user to search the Internet, check for e-mail and download a file all at the same time. As each packet arrives, the Internet access software on the user’s PC examines the Application layer information which directs the packet to the correct software to allow it to be read properly.

- **The Transport Layer:**
The Transport Control Protocol layer controls the exchange of packets of data between hosts by setting out mechanisms to check that the packets have arrived and have not been corrupted. It will also have mechanisms for re-sending the packets if the transmission fails.

- **The Internet Layer:**
The IP sets out rules for where the receiving host should route the packets of data by defining the addressing system as well as numbering the packets.

The Transport Control Protocol/Internet Protocol is the standard set of communication rules used by computers linked to the Internet that ensure the efficient control and routing of data.

### 4 Common applications on the Internet
The Internet is merely a communication tool upon which different applications can be accessed. Some of the more common applications will now be briefly discussed.

#### 4.1 The World Wide Web
The World Wide Web (WWW) is defined by the ECTA as:
“…an information browsing framework that allows a user to locate and access information stored on a remote computer and to follow references from one computer to related information on another computer”\textsuperscript{78}

The aim of the WWW is to provide universal access to a large variety of data contained in web pages, which are found on websites.\textsuperscript{79} Data in the form of text, sound, images and video can be found on the WWW. A web page may contain links to other web pages, allowing for the creation of a “thread of related information”.\textsuperscript{80} These web pages can be stored on different hosts in completely different countries, making it possible that one website may not have all of its pages stored on one host.\textsuperscript{81} There are various forms of linking, such as:

- Surface linking, which is a link from one website to the home page of the linked website.\textsuperscript{82}
- Deep linking, which is linking that bypasses the home page and creates a link to a particular part of another user’s website.\textsuperscript{83}
- Framing, which is a form of linking where the data on another website is framed and encased by the linking site.\textsuperscript{84}

It is apparent that the technology of the Internet and the WWW can therefore create situations where the normal boundaries of ownership and responsibility are blurred.\textsuperscript{85}

To locate a web page or any data on the WWW, one may enter a Uniform Resource Locator (URL) into a web browser. URL’s allow a user to find any resource on the Internet and the

\textsuperscript{78} S1 of Act 25 of 2002.
\textsuperscript{79} Jordaan “Information Technology” in \textit{E-Commerce} 31-32; Longworth “The possibilities for a legal framework” in \textit{Law of Cyberspace} 14; Stallings \textit{Data and Computer Communications} 762; Molyneux \textit{The Internet Under the Hood} 31.
\textsuperscript{80} Jordaan “Information Technology” in \textit{E-Commerce} 32.
\textsuperscript{81} Jordaan “Information Technology” in \textit{E-Commerce} 32; Khumalo “Copyright and the Internet” in \textit{Cyberlaw} 16; Longworth “The possibilities for a legal framework” in \textit{Law of Cyberspace} 14-15; Smith \textit{Internet Law} 57.
\textsuperscript{82} Khumalo “Copyright and the Internet” in \textit{Cyberlaw} 16; Smith \textit{Internet Law} 58; Reed \textit{Internet Law} 77.
\textsuperscript{83} Smith \textit{Internet Law} 58; Khumalo “Copyright and the Internet” in \textit{Cyberlaw} 16; Reed \textit{Internet Law} 77-78; Ebersöhn “Hyperlinking and deep-linking” 2003 (11) \textit{JBL} 73 73.
\textsuperscript{84} Smith \textit{Internet Law} 75; Khumalo “Copyright and the Internet” in \textit{Cyberlaw} 16; Reed \textit{Internet Law} 74-75.
\textsuperscript{85} Smith \textit{Internet Law} 56; Reed \textit{Internet Law} 88.
WWW, provided they know its unique address. The URL can either be the IP address number or the domain name.  

4.1.1 Domain Name System

Domain names are registered in order to ensure uniqueness and prevent a duplication of names. There are a variety of international and national organisations that deal with the administration, regulation and co-ordination of the Internet and of domain names. One of the most important organisations is the Internet Corporation of Assigned Names and Numbers (ICANN). Amongst its duties is the allocation of IP addresses as well as the authorisation of new Top Level Domain Names (TLD’s). There are two types of (TLD’s), namely Generic Top Level Domains (gTLD’s) and Country Code Top Level Domains (ccTLD’s). TLD’s may be restricted, reserved for organizations that meet certain conditions, or unrestricted, which are available to anyone. Country Code Top Level Domain’s (ccTLD’s) are two letter codes for a particular country or geographical territory, which can be further divided into second level domains.

---

86 Reed Internet Law 42-43; Jordaan “Information Technology” in E-Commerce 27-28,30; Dean Enhanced Network 569; Molyneux The Internet Under the Hood 86; Evans et al Technology in Action 76-77.
87 Greenberg “Trademarks” in Cyberlaw 36; Jordaan “Information Technology” in E-Commerce 28, 30; Burns Communications Law 390; Dean Enhanced Network 534-535.
88 Greenberg “Trademarks” in Cyberlaw 34; Smith Internet Law 150-157; Longworth “The possibilities for a legal framework” in Law of Cyberspace 14; Dean Enhanced Network 534-535; Molyneux The Internet Under the Hood 30-31.
90 Reed Internet Law 44; Smith Internet Law 150.
91 An example of a restricted TLD is ‘.mil’, which is for military installations of the USA. An example of an unrestricted TLD is ‘.com’, which is available to users other than commercial organizations. Greenberg “Trademarks” in Cyberlaw 38; Jordaan “Information Technology” in E-Commerce 28-29; Dean Enhanced Network 534-535; Evans et al Technology in Action 77-78; Reed Internet Law 44; du Plessis & Viljoen “Registering domain names” 1998 (6) JBL 148 148.
92 Greenberg “Trademarks” in Cyberlaw 38; Dean Enhanced Network 534-535; Molyneux The Internet Under the Hood 158; Reed Internet Law 44; Smith Internet Law 150. For example: ‘.za.’ for RSA. Greenberg “Trademarks” in Cyberlaw 38; du Plessis & Viljoen 1998 JBL 149.
93 For example: ‘.ac’ for research and academic institutions. Greenberg “Trademarks” in Cyberlaw 38; Evans et al Technology in Action 528. For example: ‘.ac’ for research and academic institutions. du Plessis & Viljoen 1998 JBL 149. An example of a full domain name would be www.nmmu.ac.za, which denotes a host called ‘nmmu’, which is in RSA (a ccTLD) and is a research or academic institution (a second level domain name).
4.2 E-mail

Electronic mail (e-mail) was one of the first uses of the Internet. An example of an e-mail address is marilyn@telkomsa.net. It consists of a unique ID, “marilyn” with the domain of the e-mail server, this case Telkom. The message will be routed along the Internet backbone where the routers will use the domain name to send it to the Telkom e-mail server. Once it reaches Telkom, it will be held in a mail box until the user logs onto the Internet to read e-mail. There are two types of e-mail:

- Post Office Protocol 3 (POP3) e-mail’s are stored on a dedicated server and which can be accessed by a user via an e-mail application such as Microsoft Outlook.

- Web based e-mail is where an e-mail service provider allocates a certain amount of space to subscribers for e-mail boxes. To retrieve messages, users must link to the e-mail service provider’s website through the use of a web browser. The user therefore does not need an e-mail application, only a web browser.

4.3 File Transfer Protocol

FTP is the transmission of data in the form of files from one host to another. The files can be text, video, sound, animation or images. These files can be opened by the receiving host if it has the necessary application. A FTP site is therefore a collection of data which can be accessed via download by users. FTP can be used for: downloading of files from a website; uploading of files from a website; backing up of data to any computer anywhere in the world; allowing users to gain access to data files that would exceed e-mail box limits.

---

94 Jordaan “Information Technology” in E-Commerce 32-33; Evans et al Technology in Action 536; Smith Internet Law 4.
95 Jordaan “Information Technology” in E-Commerce 32-33; Evans et al Technology in Action 536; Smith Internet Law 4.
97 Jordaan “Information Technology” in E-Commerce32-33; Evans et al Technology in Action 86; Snell Sams Teach Yourself the Internet in 24 Hours (2002) 90.
98 Jordaan “Information Technology” in E-Commerce 33-34; Stallings Data and Computer Communications 43; Dean Enhanced Network 75, 570-573; Evans et al Technology in Action 76, 529.
99 Reed Internet Law 31; Jordaan “Information Technology” in E-Commerce 29; Evans et al Technology in Action 76, 529.
100 Jordaan “Information Technology” in E-Commerce 33-34; Dean Enhanced Network 570-573; Hofman Cyberlaw 22.
4 4 Chat Rooms and Instant Messaging

Chat rooms are sites where users with similar interests can communicate with each other in real time. They are usually public and users can chat about different subjects in different ‘rooms’. 101

Instant messaging (IM) is a form of private real time communication. IM is performed through dedicated software and users are free to decide with whom they want to communicate with. 102

4 5 Newsgroups and Blogs

Newsgroups (also referred to as bulletin boards) 103 are forums for discussion that allow users to post information of a specialist nature onto servers that can be accessed by users who have similar interests. Newsgroups are groups of users that post questions, answers and opinions onto a website forum that another user can log on and respond to. 104

A blog is a frequently updated personal website which provides a space for the user running it (a blogger) to post any content of their choosing. Blogs have evolved into online journals or diaries, containing the bloggers personal views, links or other content that is regularly updated. Some blogs are engineered to allow other users to post responses should they wish. 105

5 Role players on the Internet

The discussion supra provides only some of the Internet applications that are available. It is in respect of these common applications that many legal questions have been raised, especially in the USA. To attach legal consequences to a particular action in any of these applications, it is necessary to identify the role players involved. 106

---

102 Evans et al Technology in Action 88, 90, 539; Snell Sams Teach Yourself 116-117; Kent Complete Idiots Guide 143.
103 Snell Sams Teach Yourself 18; Kent Complete Idiots Guide 150.
104 Jordaan “Information Technology” in E-Commerce 34; Reed Internet Law 28-29; Snell Sams Teach Yourself 134-135; Kent Complete Idiots Guide 150-151.
106 Smith Internet Law 4-5; Reed Internet Law 20, 24; Burns Communications Law 379.
5 1 Internet backbone
The backbone of the Internet consists of routers, switches, hosts and transmission media. The first three can be owned by government or private organizations whose computers are permanently connected to the Internet. The transmission media or pipes are the cable or wireless connections between the computers and are typically owned by telecommunication companies.

5 2 Administrators
There are a number of international and national organisations whose task it is to deal with the administration and regulation of the Internet. Many of these bodies are associated with the Internet Society, who initially developed the Internet protocols. An organisation already mentioned is ICANN which deals with the Internets technical co-ordination and management. An example of a local organisation is Namespace ZA which deals with the administration of the .za namespace.

5 3 Hosts
Hosts are simply computers that store data. The type of data as well as the manner in which it is stored can vary, from e-mail’s to websites. A host can also be referred to as a server. The level of control a host has over that data raises many different legal consequences. The liability that attaches to the owner of a host that not only stores but actively controls data, would be greater than a host that is simply used as storage space.

---

107 Smith Internet Law 5-6.
108 Smith Internet Law 150-157; Reed Internet Law 26-27; Alhadeff & Cohen “Functionality of VANS” in Cyberlaw 232; Evans et al Technology in Action 73-74; Molyneux The Internet Under the Hood 109-110.
109 Greenberg “Trademarks” in Cyberlaw 34; Smith Internet Law 8-9; Molyneux The Internet Under the Hood 30-31.
110 Smith Internet Law 150-157; Greenberg “Trademarks” in Cyberlaw 34; Molyneux The Internet Under the Hood 30-31.
111 Greenberg “Trademarks” in Cyberlaw 34; Smith Internet Law and Regulation 150-157; Molyneux The Internet Under the Hood 30-31.
112 Greenberg “Trademarks” in Cyberlaw 35.
113 Smith Internet Law 9; Reed Internet Law 27; Dean Enhanced Network 8-9, 77; Legal Instruments for Combating Racism 50.
114 Smith Internet Law 9; Dean Enhanced Network 8-9, 77.
115 Smith Internet Law 9-10; Nel “Freedom of expression” in Cyberlaw 197, 200-201; Reed Internet Law 28.
5 4 Content Providers
The content, being data, comes in many forms ranging from text to video. Government institutions, companies as well as individuals are all capable of being content providers.116

5 5 Information Location Tools
Due to the large amount of content available on the Internet, it is necessary to have a navigator. The most common forms are directories, web browsers and search engines that assist in locating content the user is searching for.117

Directories (also known as structured directories) list resources under a tree hierarchy.118 Controllers of resources register them under a particular category which is created by the controller of the directory.119 Users then look through the category lists until finding the resource they would like to access. However, directories list only registered resources, whereas web browsers/search engines create a database based on keywords found by software which automatically searches websites. When a user types a word into the web browser/search engine the word is cross-referenced to the keywords in the database. The web browser/search engine produces a list of resources which contain the words searched for.120

A web browser is software that allows users to access, view and navigate the WWW. On the other hand search engines search the web only.121 A good information location tool or navigation provider can become a strong brand and can generate income through advertising, such as Google for example.

116 Smith Internet Law 6; Legal Instruments for Combating Racism 50.
117 Reed Internet Law 33; Smith Internet Law 14; Evans et al Technology in Action 75, 79-80.
118 Reed Internet Law 33; Evans et al Technology in Action 82.
119 Reed Internet Law 33; Smith Internet Law 14; Evans et al Technology in Action 79-80.
120 Smith Internet Law 14; Reed Internet Law 33; Khumalo “Copyright and the Internet” in Cyberlaw 15-16; Evans et al Technology in Action 75-76, 79-80.
121 Evans et al Technology in Action 75-76, 79-80.
122 Smith Internet Law 14.
5 6 Internet Access Providers

There are a number of different types of Internet Access Providers (IAP’s), such as academic institutions, government bodies and companies that sell access on a commercial basis.\textsuperscript{123} They play a key role on the Internet as they provide facilities for users to access the Internet as not all computers access the Internet backbone directly.\textsuperscript{124}

6 What is an ISP?

The commercial companies that provide Internet access are often referred to as Internet Service Providers (ISP’s).\textsuperscript{125} They can be large telecommunication companies such as Telkom or commercial enterprises such as MWEB. However, ISP’s may provide additional services beyond Internet access and can perform many different functions:

- Mere conduit, such as an IAP or part of the Internet backbone
- Cache;
- Host;
- Content provider, if it has its own website that provides any sort of data;
- Software provider, if it provides programs to search the Internet and download and send e-mails, amongst others;\textsuperscript{126}
- Information location tool such as a search engine or a web browser, for example Google and Microsoft Internet Explorer respectively.\textsuperscript{127}

ISP’s are therefore very important to the functioning of the Internet. The term ‘ISP’ can be potentially confusing as it encompasses many different functions.\textsuperscript{128} These different functions can attract different standards of liability.\textsuperscript{129} What can add even more confusion is that an ISP

\textsuperscript{123} Smith Internet Law 11-12.
\textsuperscript{124} Smith Internet Law 11-12; Jordaan “Information Technology” in E-Commerce 29; Evans et al Technology in Action 73-74; Legal Instruments for Combating Racism 49.
\textsuperscript{125} Smith Internet Law 12; Jordaan “Information Technology” in E-Commerce 29; Evans et al Technology in Action 73-74.
\textsuperscript{126} Smith Internet Law 9-10; Reed Internet Law 32-33.
\textsuperscript{127} Reed Internet Law 32-33.
\textsuperscript{129} See Chapter 3 for a discussion on ISP liability for third party unlawful content and how in certain circumstances the nature and extent of their liability changes depending on the functions they are performing.
can perform many different functions at once, sometimes in the same transmission.\footnote{130}{For example: Telkom provides Internet access and e-mail facilities. When a user downloads their e-mail from Telkom’s servers, Telkom is performing the function of an access provider, mere conduit and host (as the e-mail is stored on their servers).} Further, the technology of the Internet allows for many different ISP’s to be involved in even the simplest transaction.\footnote{131}{For example: A user accessing the Internet using M-Web (an Internet Access Provider) to check their web-based e-mail on Ananzi (a host) using a Telkom broadband connection (a mere conduit).} These variables can lead to difficulty in determining the extent of their liability.

7 What is an ISP?: The legal definitions in different jurisdictions

For legal rights or responsibilities to be attached to an entity, a jurisdiction would have to first define it. It should be apparent from the discussion supra that a wide definition would be needed to encompass the wide variety of functions an ISP can perform. The definitions of an ISP from the jurisdictions to be examined in this dissertation will now be discussed.

7 1 United States of America

There are two USA statutory instruments that are relevant to this dissertation, the CDA and the DMCA. The definitions contained in these instruments encompass a wide spectrum of ISP functions.

7 1 1 Communications Decency Act

The CDA is relevant to the discussion on ISP liability for unlawful content.\footnote{132}{See Chapter 3.} The principal purpose of the CDA is to regulate the distribution of obscene and indecent material to minors.\footnote{133}{Roos “Freedom of expression” in ICT Law 418.} It also provides broad immunity from liability to ISP’s, to encourage the self-regulation of third-party content.\footnote{134}{Pink The Internet 352; Bick 101 Things You Need to Know About Internet Law (2000) 55-56; Nel “Freedom of expression” in Cyberlaw 202; Zeran v America Online Inc. 129 F 3d 327 (4th Cir 1997) 331.} The CDA does not provide a specific definition for the term ‘ISP’, but rather refers to providers of ‘interactive computer services’, which are defined as:

“…information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and
such systems operated or services offered by libraries or educational institutions.”

An access software provider is defined as a:

“provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;
(B) pick, choose, analyze, or digest content; or
(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.”

7.1.2 Digital Millennium Copyright Act

Title II of the DMCA is relevant to the discussion on the provision of limited immunity from liability to ISP’s and notice and take-down procedures. The DMCA is intended to create certainty for ISP’s in relation to their liability for third party copyright infringement and promote co-operation between ISP’s and copyright owners in the detection and managing of copyright infringements. The DMCA’s application is limited to copyright law. It does not provide a specific definition of the term ‘ISP’, but refers rather to ‘service provider’, which is defined as:

“...a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).”

135 47 USC § 230(f)(2).
137 See Chapters 5 and 6. Title II is also known as the Online Copyright Infringement Liability Infringement Act. Senate The Digital Millennium Copyright Act of 1998-Report S Rept No 105-190 (1998) 19.
138 S Rept No 105-190 20; Brown “Fortifying the safe harbours: Re-evaluating the DMCA in a Web 2.0 world” 2008 (23) Berk Tech LJ 437 445.
140 17 USC § 512(k)(1)(B).
The definition contained in subparagraph (A) is for ISP’s that are mere conduits of data, which are defined as:

“...an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.”

7.2 European Union and United Kingdom

The EU Directive is relevant to the discussion on the provision of limited immunity to ISP’s. It was adopted for the creation of a legal framework for information society services, in particular electronic commerce. There were concerns that the differences between EU member states in relation to ISP liability were preventing the “smooth functioning of the internal market”. The EU Directive was therefore necessary to remove legal obstacles to the growth of the Internet, which obstacles arose from the difference in national laws and uncertainty relating to their application. The EU Directive creates safe harbours from liability for ISP’s that fall into certain categories and meet certain conditions.

The EU Directive does not define the term ‘ISP’, but refers rather to service providers of ‘information society services’. The definition of such a service is provided in Article 1(2) of Directive 98/34/EC, as amended.
“…that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition:

- “at a distance” means that the service is provided without the parties being simultaneously present,
- “by electronic means” means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,
- “at the individual request of a recipient of services” means that the service is provided through the transmission of data on individual request.”

The EU Directive was transposed into UK law in the form of the Electronic Commerce (EC Directive) Regulations 2002 (EC Regulations).\textsuperscript{150} The same definitions as provided in the Directive were kept.\textsuperscript{151}

\textbf{7 3 South Africa}

There are a number of legal definitions relevant to ISP’s in RSA law.\textsuperscript{152} However, only the definitions in the ECTA and the Films and Publications Act 65 of 1996 are relevant for the purposes of this dissertation.

\textbf{7 3 1 ECTA}

The ECTA does not provide a specific definition for the term ‘ISP’. Chapter XI of the ECTA, entitled ‘Limitation of Liability of Service Providers’, provides that for the purposes of that

\textsuperscript{150} Statutory Instrument (SI) 2002/2013.
\textsuperscript{151} S2of SI 2002/2013. The safe harbours are contained in s17-19 of SI 2002/2013.
\textsuperscript{152} For example see: s1 of the Electronic Communications Act 26 of 2005, provides a definition of ‘electronic communications service’; s1 of The Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002, provides a definition for ‘Internet Service Provider’. The full definitions are not provided as they are not directly relevant to this dissertation, but are raised to inform the reader that ISP’s must be aware that there are other pieces of legislation relevant to the conduct of their business as a whole.
chapter ‘service providers’ means any person providing ‘information system services’, which are defined as including:

“...the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service”

An ‘information system’: 

“means a system for generating, sending, receiving, storing, displaying, or otherwise processing data messages and includes the Internet”

7.3.2 Films and Publications Act

The Films and Publications Act 65 of 1996 (FPA) is relevant to the discussion on certain types of unlawful content. It provides a definition for the term ‘Internet Service Provider’, which is defined as any person whose business it is to provide access to the Internet by any means. This definition is narrower than the ECTA as it refers specifically to commercial IAP’s. It is wide enough to include entities from Internet Cafes to large corporations. On 26 August 2009, the president assented to the Films and Publications Amendment Act 3 of 2009. The date of commencement is yet to be proclaimed. The amendment Act will not affect the definition.

7.4 Potential problems with legal definitions of an ISP

It is necessary for the legal definitions to be very wide to encompass the various functions that ISP’s perform. A further purpose for such wide definitions is that legislators wish to be able to include future unforeseen developments in the Internet technology without having to

---

154 S1.
155 Ibid.
156 S1 of Act 65 of 1996.
promulgate new legislation after each development. This is demonstrated in some of the definitions in that there is no reference to the Internet at all, but rather to information services. In the RSA, this contention is supported by one of the objects of the ECTA, which is to promote technology neutrality in the application of legislation to electronic communications and transactions.\textsuperscript{158} The author is of the opinion that in terms of the definitions contained in the ECTA, that the entities listed below can fall under its provisions:

- Value Added Network Services (VANS), examples: MWEB and Ananzi;
- Mobile telephone companies, since they provide a connection and access to information systems as well as transmit or route data between points specified by a user, examples: MTN, Cell C and Vodacom;
- Mobile telephony content providers, companies that sell items such as ringtones or photos for mobile phones as they operate facilities for information systems, examples: MTN, Vodacom, Glomobi etc;
- Universities, since they provide access to information services;
- Online banking, since they not only provide access to an information system, but are also operating a facility for an information system;
- FTP sites since they process and store data as well as provide access to information system services, example being Musica or other download websites;
- The hosts and controllers of newsgroups or online forums since they provide access to information systems as well as store and process data at the individual request of the recipient of the service;
- Online newspapers since they are operating a facility for an information system;
- It is submitted that even individual users who control blogs, even if hosted by another entity, could be included in this definition as the very act of creating and updating of websites means they are operating a facility for a system for generating, storing, displaying and processing of data messages;
- Social networking websites, such as Twitter or Facebook.

\textsuperscript{158} S2(f) of Act 25 of 2002.
A possible consequence of this approach is that the provisions of these laws may be applied to entities that the legislature never considered or intended, thus resulting in those entities receiving protection or having obligations imposed on them. This may not always be desirable, for instance in the case of social networking website. It may also mean that entities are, unbeknownst to them, being exposed to liability.

8 Conclusion

It is through understanding how the Internet works, that the reader may understand the many functions that an ISP can perform. In any given transmission of data, these different functions can be performed by different ISP’s or just one. It is therefore obvious how important ISP’s are to the Internet.

The possibility of ISP’s performing multiple functions in the same transaction can result in uncertainty as to the extent of their liability since these different functions can attract different standards of liability. The ECTA removes this uncertainty to an extent since it is apparent that an ISP falls under the ECTA’s definition of an information service provider. This leads to the imposition of certain duties and the provision of a degree of protection. However, the possible negative effects of such a wide definition cannot be ignored as it could potentially result in duties imposed on, or protection for, entities not originally intended by the legislature.

Understanding the technology of the Internet will assist in identifying the potential legal liability and duties of an ISP. It will also assist in identifying the problems encountered with such associations and the solutions.
CHAPTER THREE: ISP LIABILITY IN THE ABSENCE OF THE ECTA

1 Introduction
The explosion of the Internet left jurisdictions around the world facing the same challenge: how did one apply existing law to the Internet? There was debate over whether existing law could be effectively applied to the Internet, or whether new Internet specific legislation was required. There was concern that the numerous laws that exposed ISP’s to liability threatened the effective functioning of the Internet.\textsuperscript{159} \textsuperscript{160}

The Internet in the RSA is currently regulated by the common law, non-Internet specific legislation and Internet specific legislation. In terms of Chapter XI of the ECTA, an ISP’s liability is limited if it complies with certain requirements.\textsuperscript{161} Failure to comply will result in the ISP not being protected by the provisions of Chapter XI.\textsuperscript{162} This is a difficult determination to make due to the lack of authority. To establish what the legal position might be, it is useful to examine USA and UK law where ISP liability in the absence of Internet specific legislation has been determined. The focus will fall on the prevalent issues of online defamation, hate speech and obscenity and indecency.

2 Defamation
Defamation is the publication to a third party of words or actions that undermine a person’s reputation, good name or their standing in the community.\textsuperscript{163} All parties to the publication process may be exposed to the risk of liability, with the party exerting greater control over the material\textsuperscript{164} exposed to greater risk.\textsuperscript{165} Commonly identified parties to the abovementioned

\textsuperscript{159}Burchell \textit{Personality Rights} 121; Burns \textit{Communications Law} 379; Trudel “Liability in Cyberspace” in \textit{Law of Cyberspace} 189, 193-194; Reed & Angel \textit{Computer Law} 366-367; Reed \textit{Internet Law} 94, 122.
\textsuperscript{160}Zeran \textit{v America Online Inc} 129 F 3d 327 (4th Cir 1997) 330; Recital 40 of Directive 2000/31/EC; GG 29474 6.
\textsuperscript{161}Ss72-77 of Act 25 of 2002. See Chapters 4-6 for a further discussion on these requirements.
\textsuperscript{162}Roos “Freedom of expression” in \textit{ICT Law} 429; Nel “Freedom of expression” in \textit{Cyberlaw} 205.
\textsuperscript{163}Nel “Freedom of expression” in \textit{Cyberlaw} 197; Lloyd \textit{IT Law} 573; Smith \textit{Internet Law} 315; Reed \textit{Internet Law} 112.
\textsuperscript{164}The term ‘material’ will be used for the physical world context and the term ‘content’ for the Internet context.
\textsuperscript{165}Pink \textit{The Internet} 348; Burns \textit{Communications Law} 393; Nel “Freedom of expression” in \textit{Cyberlaw} 200-201; Nel 2008 \textit{Responsa Meridiana} 104, 106.
process are authors, editors, publishers, distributors and mere or passive conduits.\(^{166}\) An ISP is capable of being all of these parties at once,\(^{167}\) thus creating difficulty in the determination of its liability.\(^{168}\) Beyond these basic principles, the law of defamation differs in each jurisdiction.\(^{169}\) The discussion of each jurisdiction will commence with an outline of the general principles of defamation in order to provide a context for the case discussions and other legal developments.

### 21 Defamation: United States of America

#### 211 The law of defamation in the United States of America

The USA law of defamation consists of the twin torts of libel and slander.\(^{170}\) Defamation is defined as the injury to reputation by words that tend to expose one to public hatred, shame, contempt or disgrace. To prove that a person has been defamed, it must be established that:

- A false and defamatory statement of fact concerning another was made;\(^{171}\)
- The statement must harm a living plaintiff by diminishing his status in society or result in others avoiding associating or dealing with him.\(^{172}\) The plaintiff must establish that the statement is *prima facie* defamatory.\(^{173}\)

---

\(^{166}\) Nel “Freedom of expression” in *Cyberlaw* 201; Reed *Internet Law* 115; Smith *Internet Law* 318.

\(^{167}\) See 6 on page 20 in Chapter Two for a discussion on this point.

\(^{168}\) For example: Hard copy publishing involves the selection, collation and the wrapping between covers of the defamatory material. Primary publishers are those who assist in the wrapped products creation, while the distributors are those who receive and then pass it on. In electronic publishing, a large amount of the content is unwrapped. It is therefore not easy to ascertain publisher or distributor liability. See Smith *Internet Law* 321.

\(^{169}\) For example: In the USA, a statement about a public figure is only deemed to be defamatory if malice, on the part of the author, can be proved. This does not exist in the UK. Reed & Angel *Computer Law* 375; Reed *Internet Law* 113; Roos “Freedom of expression” in *ICT Law* 401.


\(^{171}\) Pink *The Internet* 344; Powers *The Internet Legal Guide* 50; Carter et al *Mass Communication Law* 48; Nieto & Schmitt *A Student’s Guide* 56; Kionka *Torts* 379.

\(^{172}\) Carter et al *Mass Communication Law* 48; Kionka *Torts* 380-381.

\(^{173}\) Nieto & Schmitt *A Student’s Guide* 55.
There was unprivileged publication to a third party;\textsuperscript{174} There are two types of privilege: absolute\textsuperscript{175} and qualified\textsuperscript{176} privilege. Publication is the communication of the defamatory statement to a third party.\textsuperscript{177}

Identification;\textsuperscript{178} The plaintiff must be able to establish that he was the target of the statement.\textsuperscript{179} It is not necessary that the plaintiff be specifically named.\textsuperscript{180}

There was fault on the part of the publisher;\textsuperscript{181} There are different degrees of fault depending on the plaintiff’s status. If the plaintiff is a private person, the degree of fault required is negligence.\textsuperscript{182} For public figures, the degree of fault required is malice.\textsuperscript{183}

Caused damage to the plaintiff.\textsuperscript{184} In certain circumstances, the plaintiff must prove special damages depending on whether the communication falls underneath particular forms of libel or slander.\textsuperscript{185}

\textsuperscript{174} Pink The Internet 345; Powers The Internet Legal Guide 50; Nieto & Schmitt A Student’s Guide 57; Siegel Communications Law 84; Kionka Torts 379.
\textsuperscript{175} For example: Statements made in judicial proceedings. Pink The Internet 345-346; Carter et al Mass Communication Law 71-72; Nieto & Schmitt A Student’s Guide 62.
\textsuperscript{176} For example: A party did not have knowledge of the falsity of the material. Pink The Internet 345-346; Carter et al Mass Communication Law 73-73; Nieto & Schmitt A Student’s Guide 62.
\textsuperscript{177} Carter et al Mass Communication Law 52; Nieto & Schmitt A Student’s Guide 55; Siegel Communications Law 85; Kionka Torts 385.
\textsuperscript{178} Carter et al Mass Communication Law 54; Nieto & Schmitt A Student’s Guide 57; Siegel Communications Law 84.
\textsuperscript{179} Carter et al Mass Communication Law 54; Nieto & Schmitt A Student’s Guide 57; Kionka Torts 382.
\textsuperscript{180} Nieto & Schmitt A Student’s Guide 57.
\textsuperscript{181} Pink The Internet 346; Powers The Internet Legal Guide 50; Nieto & Schmitt A Student’s Guide 57; Siegel Communications Law 85; Kionka Torts 380.
\textsuperscript{182} Pink The Internet 346; Powers The Internet Legal Guide 50; Nieto & Schmitt A Student’s Guide 58; Kionka Torts 389; Frits 2004-2005 Kentucky LJ 768.
\textsuperscript{183} Pink The Internet 346; Powers The Internet Legal Guide 50; Nieto & Schmitt A Student’s Guide 57; Kionka Torts 387-388; Frits 2004-2005 Kentucky LJ 768. It must be proved that the publisher had published with knowledge of the falsity of the material or with a reckless disregard to its veracity or falsity. The threat of litigation by public figures could hinder the publication of material that is in the public interest, thus impeding the freedoms of speech and the press. New York Times Co v Sullivan 376 US 254 (1964).
\textsuperscript{184} Pink The Internet 347; Powers The Internet Legal Guide 50; Carter et al Mass Communication Law 57; Nieto & Schmitt A Student’s Guide 58.
\textsuperscript{185} Carter et al Mass Communication Law 57; Kionka Torts 384-385. For example: Libels per quod are only actionable if there are special damages. Carter et al Mass Communication Law 62; Nieto & Schmitt A Student’s Guide 56; Kionka Torts 379. Libel per quod is where the statement is libellous if other facts are added to it and the context the words are used. Nieto & Schmitt A Student’s Guide 56; Siegel Communications Law 85. A further discussion of these classifications is not necessary for the purposes of this dissertation.
Parties to the publication process are liable if they: exert editorial control over the defamatory material;\(^{186}\) repeat or republish the material;\(^{187}\) fail to remove the material when in a position to do so.\(^{188}\) A party has editorial control when they have a choice over the materials contents, or make a decision over its limitations, size and content.\(^ {189}\) Some exceptions to these general principles of liability are:

- **Distributors:**\(^ {190}\)
  
  Distributors are publishers since they intend to make the materials they possess available to others,\(^ {191}\) however they are only liable if they knew or had reason to know of the defamatory material.\(^ {192}\) Upon notification, or gaining knowledge of the defamatory nature of the material, a distributor is placed in the position of a traditional publisher and must decide whether to publish, edit or withdraw the material.\(^ {193}\) This different standard of liability exists due to policy considerations,\(^ {194}\) as it is unreasonable to expect a distributor to examine all of his material for defamatory statements.\(^ {195}\) Such an onerous duty would be an unreasonable restriction on the freedom of speech and the free flow of information as distributors would only distribute material they had examined. This would amount in far fewer reading materials being made available to the public.\(^ {196}\)

---


\(^{188}\) *Zeran v America Online Inc* 129 F 3d 327 (4th Cir 1997) 333.


\(^{190}\) Examples: news vendors, book stores or libraries.

\(^{191}\) *Zeran v America Online Inc* 129 F 3d 327 (4th Cir 1997) 333.


\(^{193}\) *Zeran v America Online Inc* 129 F 3d 327 (4th Cir 1997) 332.

\(^{194}\) *Cubby Inc v CompuServe Inc* 776 F Supp 135 (SD NY 1991) 139-140.


Common Carriers
These are mere conduits through which the defamatory material is transmitted, for example telegraph and telephone companies.\textsuperscript{197} Telegraph companies are publishers due to staff’s active participation in transmission of messages, but have been granted qualified immunity.\textsuperscript{198} Telephone companies have been held not be publishers as they do not directly participate, therefore it cannot be liable for defamatory statements.\textsuperscript{199}

Examination of the following cases will indicate how these basic principles were applied to ISP’s. It will further indicate why development to broad immunity for ISP’s took place.

\textit{2 1 2 Cubby Inc v CompuServe Inc}\textsuperscript{200}
This is one of the first USA cases to deal with ISP liability for third party defamatory statements. The plaintiff’s instituted proceedings against the defendant ISP for defamatory statements contained in a rival electronic newsletter hosted on a forum by the ISP.\textsuperscript{201} The forum’s contents were controlled by an independent company who had contracted a third party to produce the publication.\textsuperscript{202} The ISP claimed that it was a distributor as there was no direct link between it and the third party. It further did not have an opportunity to review the publications contents before being uploaded onto the forum.\textsuperscript{203}

The court found that the ISP had little or no editorial control over the publications in its forums, the content of which was controlled by an independent company. The court held that the ISP was similar to a distributor, finding that the policy considerations for not holding traditional distributors liable applied to ISP’s performing this role, especially due to the sheer

\textsuperscript{197} Siegel \textit{Communications Law} 98.
\textsuperscript{198} Lunney \textit{v Prodigy Services Company} 683 NYS 2d 560 (SD NY 1998).
\textsuperscript{200} 776 F Supp 135 (SD NY 1991).
\textsuperscript{201} 138.
\textsuperscript{202} 137.
\textsuperscript{203} \textit{Ibid.}
Upon application of the distributor test, the court found that the plaintiff's failed to prove that the defendant knew or had reason to know of the defamatory statements.

213 **Stratton Oakmont v Prodigy Services Company**

The plaintiff claimed that defamatory statements were published about it by an unknown user on the defendant ISP’s bulletin board. The plaintiff argued that the ISP should be deemed a publisher as it had previously likened itself to a newspaper and expressly stated that it exercised editorial control over the messages posted on its bulletin boards. Further, that the ISP had content guidelines which stated that it would remove undesirable statements upon notification. Finally, the ISP used software to automatically screen messages for offensive language and contracted board leaders, granting them editorial powers to enforce the guidelines and remove undesirable content. The ISP argued it was a distributor. Its editorial policy had changed and it no longer reviewed all the postings made. Due to the sheer volume of messages, in excess of 60,000 a day, it was not feasible to manually review each one. Its board leaders could not be construed as editors simply because they had the power to remove messages that violated the guidelines.

The court confirmed the decision in Cubby's case, but held that the ISP’s position in this case was analogous to that of a newspaper and not a distributor. It had made a conscience choice to gain editorial control through its policy, technology and staffing decisions. It had placed itself in a position to decide for its users what was desirable to submit and view, even though this control was not exercised consistently. The court found that the ISP had not changed its policies or communicated such change to others. The court found that the ISP had created a board of editorial staff to monitor and censor all transmissions, but wished to avoid
the legal liability that attaches to being a censor. The court stated that the ISP’s policies may have a ‘chilling effect’ on the freedom of expression, which the ISP may have desired. The ISP was found to be a publisher of the defamatory statements. The court stated its decision would not cause other ISP’s to abandon editorial control of their forums as the market would reward them for maintaining control.

215

2 1 4 Criticisms of the Stratton case

The court in Stratton’s made an incorrect finding on fact and failed to take into account the technology of the Internet and certain policy considerations.

The defendant did not have real or effective editorial control and should not have been found to be a publisher for the following reasons:

- Content guidelines do not indicate editorial control. The ISP did not routinely examine or approve the statements that were posted. The guidelines were merely a warning to users to respect others, to refrain from making posts of a certain nature and that undesirable posts will be removed once brought to the ISP’s attention. This indicates that the ISP would be reactive, which does not constitute effective editorial control or an assumption of publisher responsibility as editors or publishers are proactive in choosing content.

- The court failed to take the technology of the Internet into account as ISP’s cannot be expected to monitor all transmissions made by users due to sheer volume.

- The court failed to take the technology of the Internet into account by failing to properly consider the limitations of automatic screening software and that it is not a sign of intelligent, effective editorial control.

216

241.

217

242.

218

233.

219

This had been noted and properly considered in Cubby Inc v CompuServe Inc 776 F Supp 135 (SD NY 1991) 140, and again in the subsequent cases of Zeran v America Online Inc 129 F 3d 327 (4th Cir 1997) 333 and Lunney v Prodigy Services Company 723 NE 2d 539 (NY 1999) 249.

219

In Lunney v Prodigy Services Company 683 NYS 2d 557 (SD NY 1998) 561, the court noted that offensive messages can be impeccably composed, while offensive words can be used humorously or even affectionately. The court properly considered automatic screening software and found it not to be a sign of intelligent, effective editorial control. The software amounted to an “unintelligent automated word-exclusion program” and the court found that intelligent editorial control involved the use of judgment. This case was
In *Stratton* the court failed to take into account a variety of policy considerations:

- It failed to properly consider the effect that this decision would have on the Internet and its development. It discouraged the development and use of filtering and blocking software by ISP’s. It further removed any incentive for ISP’s to monitor their networks for offensive content and encouraged them to ignore content to attain distributor status. It failed to properly consider that the higher the volume of transmissions over an ISP’s network, the greater their exposure to liability and potential risk of large damage awards. The risk would thus negate any ‘reward’ the market may have had for ISP’s maintaining control. ISP’s would therefore be unwilling to regulate the Internet for fear of publisher liability, thus leading to a potential increase in online unlawful content.

- The legislative history of the CDA indicates that one of the primary reasons for the development of section 230 was to overrule *Stratton’s* case, as it was considered incorrect to impose publisher liability on ISP’s where they voluntarily edited content.

- In *Zeran v. America Online Inc* it was held that it is impossible for ISP’s to screen all of the content transmitted due to sheer volume. Facing potential liability, ISP’s could choose to restrict the amount and type of content being transmitted, thus threatening the freedom of expression.

---

an appeal, however this decision was taken on appeal in *Lunney v Prodigy Services Company* 723 N E 2d 539 (NY 1999).


221. Nel “Freedom of expression” in *Cyberlaw* 202; Nel 2008 *Responsa Meridiana* 109-110; Frits 2004-2005 *Kentucky LJ* 773-774. In *Lunney v Prodigy Services Company* 683 NYS 2d 560 (SD NY 1998) 562 the court stated that the decision in *Stratton* was unfair as Prodigy was found liable for conduct which it had no legal duty to perform and the decision discouraged the conduct which the plaintiff argued should be encouraged.


224. 129 F 3d 327 (4th Cir 1997).

225. 331.
The court in *Stratton* appeared to express disapproval of an ISP exercising editorial control. ISP’s would have to weigh up the possibility of facing such disapproval in the event of litigation, against any ‘market reward’.\(^{226}\)

### 2.1.5 The effect of the *Stratton* case: The Communications Decency Act

The *Stratton* case illustrates that existing USA law could not be effectively applied to the Internet. It also illustrates the risk that the judiciary may not always possess sufficient knowledge of Internet technology to apply the law correctly. The US Congress was concerned with the possible effects that the decision could have on the freedom of speech, regulation of unlawful content, and on the Internet and its development.\(^{227}\) As a result, section 230 of the CDA was promulgated to counteract these effects and provide broad protection to ISP’s to self regulate third-party content without being exposed to liability.\(^{228}\) Since the CDA is a radical departure from UK and RSA law,\(^{229}\) subsequent developments will be briefly examined to complete the discussion on the law of defamation in the USA.

### 2.1.6 Post Communications Decency Act case law

In terms of section 230(c)(1) of the CDA, a provider or user of interactive computer service shall not be treated as a publisher or speaker of third party content.\(^{230}\) This was interpreted as granting ISP’s broad immunity in *Zeran v America Online Inc*.\(^{231}\) Anonymous posts on the defendant ISP’s bulletin boards advertised t-shirts praising the Oklahoma City bombings and falsely provided the plaintiff’s contact details for those interested in purchasing them.\(^{232}\) In response to the death threats received, the plaintiff contacted the ISP to remove the postings, who failed to act in a timely manner. It further refused to post retractions of those posts and

---


\(^{228}\) *Zeran v America Online Inc* 129 F 3d 327 (4th Cir 1997) 331; Roos “Freedom of expression” in *ICT Law* 418; Pink *The Internet* 352; Bick *101 Things* 55-56; Nel “Freedom of expression” in *Cyberlaw* 202; Frits 2004-2005 *Kentucky LJ* 774; *Legal Instruments for Combating Racism* 116. However, it should be noted that the principal purpose of the CDA was to regulate the distribution of obscene and indecent content to minors. Roos “Freedom of expression” in *ICT Law* 418.

\(^{229}\) Nel 2008 *Responsa Meridiana* 127.

\(^{230}\) See 7.11 on page 21 in Chapter 2 for the CDA’s definition of such a service.

\(^{231}\) 129 F 3d 327 (4th Cir 1997).

\(^{232}\) 329.
screen for similar postings thereafter. The plaintiff argued that the ISP was a distributor and liable as it failed the test for distributor knowledge. However, the court found that the plaintiff was creating an artificial distinction between the liability of a publisher and a distributor in defamation law. Distributors are a type of publisher with a different standard of liability applicable to them. The court held that the defendant was a publisher and escaped liability due to section 230(c)(1) of the CDA.

In *Blumenthal v Drudge and America Online Inc*, the plaintiff sued the ISP for defamatory statements contained in its online gossip column. The ISP had entered into a licence agreement with the third party to produce the column for its subscribers. In terms of the agreement, the ISP had right of editorial control and the third party would receive royalties. The court found that the ISP would have been a publisher in terms of pre-CDA defamation law, however the CDA granted it immunity from liability. This immunity was granted as an incentive to ISP’s to monitor for unlawful content and exists even when their attempts are unsuccessful or not attempted at all.

The broad immunity has been expanded to a variety of entities on the basis of the provision of information system services to multiple users, such as online auctioneers, online retail stores, chat rooms, users who repost messages on their own newsgroups, e-mail mailing lists, and libraries and commercial establishments that offer Internet access.

---

233. 328.
234. 331.
235. 332.
236. See the discussion on distributor liability on page 32 supra.
237. 129 F 3d 327 (4th Cir 1997) 332. See Frits 2004-2005 *Kentucky LJ* 775-778 for criticisms of this decision, the principle criticism being that the court confused distributor and publisher liability.
239. 47.
240. 51.
241. 52.
242. 53. See Frits 2004-2005 *Kentucky LJ* 780 for criticisms of this decision.
247. *Batzel v Smith* 333 F 3d 1018 (9th Cir 2003).
21 7 Lunney v Prodigy Services Company

The facts giving rise to this case occurred prior to the CDA. The court therefore relied on common law principles to determine liability. An unknown third party pretended to be the plaintiff and opened Internet accounts with the defendant ISP. The third party proceeded to post two offensive messages on the ISP’s bulletin boards and sent a threatening, vulgar, e-mail to a third person. The plaintiff sued for damage caused by being falsely identified as the author of the messages.

The court held that the messages were not defamatory. If they were, the ISP was not a publisher as its position was analogous to that of a telephone company in that it was a passive conduit for the transmission of the e-mail. If it were found to be a publisher, the ISP’s position would then be analogous to that of a telegraph company and afforded qualified privilege. The needs of the public would not be met if ISP’s were forced to screen the vast volume of material for defamatory content.

21 8 ISP liability for third party defamatory content in the United States of America

The current position in the USA appears to be that ISP’s receive special protection compared to analogous offline entities. ISP’s receive immunity when they perform the role of a primary publisher and have a beneficial relationship with the third party or where they are aware of the defamatory statements and fail to act. ISP’s were granted broad immunity to monitor for unlawful content, however the CDA does not create an incentive for ISP’s to do so. It would therefore appear that the CDA and Stratton’s case are similar in this respect.

249 723 N E 2d 539 (NY 1999). This is the appeal of Lunney v Prodigy Services Company 250 AD2d 230 (SD NY 1998).

250 539.

251 541.

252 542.


254 Siegel Communications Law 494; Nel 2008 Responsa Meridiana 104. As in Blumenthal and Zeran’s cases. In Barrett v Rosenthal 112 Cal App 4th 749 (2003), the Californian Court of Appeal held that s230 of the CDA did not override the common law rule of distributor liability. However, this was overturned on appeal: Barrett v Rosenthal SC Cal Alameda County Ct App 1/2 A096451.

The CDA creates an unsafe environment for innocent users, with no means of redress against ISP’s who do not remove or prevent the posting of unlawful content.  

2.1.9 Relevance of United States law to South Africa

USA pre-CDA law of defamation is relevant as it provides examples of how the principles of distributor, publisher and mere conduit liability have been applied to determine ISP liability. This application has been done by way of analogy. However, Hofman states that these cases serve as examples of how analogies can become strained, as they failed to take into account that an ISP can be an author, publisher or distributor all at the same time.

The following principles are useful to the RSA legal position:

- If an ISP exerts little or no editorial control over the third party content it transmits, it should be deemed to be a distributor and the appropriate test for liability is applicable;

- If an ISP exerts editorial control or is actively involved in the third party content it transmits, it should be deemed to be a publisher;

- If an ISP merely transmits a third parties e-mail, it should be deemed to be a mere conduit;

2.2 Defamation: United Kingdom

The UK law of defamation has developed differently to the USA in relation to ISP liability.

2.2.1 Basic principles of defamation law in the United Kingdom

The UK law of defamation consists of the twin torts of libel and slander. The following elements must be proved to be successful in a claim of defamation:

---

256 Ibid; Frits 2004-2005 Kentucky LJ 778; Akdeniz Internet Child Pornography 232. 
257 Hofman Cyberlaw 130. 
259 Stratton Oakmont v Prodigy Services Co 1995 NY Misc LEXIS 229. It is submitted that this was an incorrect finding on fact and that Blumenthal’s case serves as a better illustration of the facts that should lead to this determination. 
260 Lunney v Prodigy Services Company 723 NE 2d 539 (NY 1999). 
• The statement must be defamatory.\textsuperscript{262} UK law has not developed a comprehensive definition of a defamatory statement.\textsuperscript{263} A simple definition is that it is a statement that lowers the claimant in the view of right thinking members of society, causing him to be regarded with feelings of hatred, contempt, ridicule, fear and disesteem.\textsuperscript{264}

• It must refer to the claimant.\textsuperscript{265} It is not necessary that the statement must refer to the claimant by name or for everyone who sees the statement to be aware that it refers to the claimant. However, it must be proved that anyone who knew the claimant or had special knowledge of the facts would be aware that the statement referred to the claimant.\textsuperscript{266}

• It must be published.\textsuperscript{267} To be published, the defamatory statement must be made known to a third party. This includes drawing attention to the statement.\textsuperscript{268} Publication to third parties is the essence of the claim for defamation, as the aim is to protect the claimant’s reputation in the community. It does not aim to satisfy the claimants hurt feelings or protect the claimant’s own opinion of himself.\textsuperscript{269}

All those party to the publication of defamatory statements will be liable,\textsuperscript{270} specifically those who intended or should have reasonably foreseen publication.\textsuperscript{271}

\textsuperscript{262} Murphy Street on Torts 481; Rogers Winfield & Jolowicz on Tort 405; Harpwood Modern Tort Law 337.
\textsuperscript{263} Rogers Winfield & Jolowicz on Tort 411; Murphy Street on Torts 482.
\textsuperscript{264} Sim v Stretch (1936) 2 All ER 1237; Rogers Winfield & Jolowicz on Tort 411.
\textsuperscript{265} Murphy Street on Torts 481; Rogers Winfield & Jolowicz on Tort 405; Harpwood Modern Tort Law 337.
\textsuperscript{266} Murphy Street on Torts 489; Rogers Winfield & Jolowicz on Tort 405; Harwood Modern Tort Law 342.
\textsuperscript{267} Murphy Street on Torts 481; Rogers Winfield & Jolowicz on Tort 405; Harpwood Modern Tort Law 337.
\textsuperscript{268} Murphy Street on Torts 492; Rogers Winfield & Jolowicz on Tort 425; Harpwood Modern Tort Law 338.
\textsuperscript{269} Murphy Street on Torts 492; Rogers Winfield & Jolowicz on Tort 425.
\textsuperscript{270} For example: authors, editors and publishers. Smith Internet Law 328; Murphy Street on Torts 492; Rogers Winfield & Jolowicz on Tort 405.
\textsuperscript{271} Murphy Street on Torts 505; Rogers Winfield & Jolowicz on Tort 426.
It is possible for a party who is ignorant of the defamatory nature of the material to be found liable for its publication.\textsuperscript{272}

Fault is only required for particular classes of publishers.\textsuperscript{273} Unless a defence exists, it is \textit{prima facie} unlawful to print defamatory statements and a party will be liable if all the above elements are proved.\textsuperscript{274} Examples of defences are absolute or qualified privilege or innocent dissemination.\textsuperscript{275} At common law, a defence of innocent dissemination existed if a party could prove that they were not a primary publisher of the defamatory statement and played a subordinate part in its dissemination.\textsuperscript{276} The party had to show a non-negligent lack of knowledge of the defamatory nature of the disseminated material and that no reason existed to believe that the material was defamatory.\textsuperscript{277}

\textbf{2.2.2 Defamation Act}

The UK common law of defamation has been updated and codified by the Defamation Act of 1996,\textsuperscript{278} which expands the innocent dissemination defence.\textsuperscript{279} A party can rely on this defence if they can prove that they:

- Were not the author, editor or publisher of the defamatory statement;

  The definitions of the above parties must be read with section 1(3) of the Act. This section makes provision for five categories of persons who will not be considered to be one of the above if they are involved in certain activities in relation to the statements publication. The two categories that would be of most relevance to an ISP are contained in subsections 1(3)(c) and 1(3)(e), in terms of which a party will not be considered to be an author, editor or publisher if it is only involved:

\begin{itemize}
  \item \textsuperscript{272} \textit{Godfrey v Demon Internet Ltd} QBD (1999) 4 All ER 342.
  \item \textsuperscript{273} Nel 2008 \textit{Responsa Meridiana} 104.
  \item \textsuperscript{274} British Law Commission \textit{Defamation and the Internet-A preliminary investigation-Scoping study II} (2002) 9; Harpwood \textit{Modern Tort Law} 9; Smith \textit{Internet Law} 328; \textit{Godfrey v Demon Internet Ltd} QBD (1999) 4 All ER 342.
  \item \textsuperscript{275} Murphy \textit{Street on Torts} 505-513; Rogers \textit{Winfield & Jolowicz on Tort} 426-429; Harpwood \textit{Modern Tort Law} 343, 349-351.
  \item \textsuperscript{276} Vitzetelly \textit{v Mudie’s Select Library Ltd} (1900) 2 QB 170; Murphy \textit{Street on Torts} 505; Rogers \textit{Winfield & Jolowicz on Tort} 427; Harpwood \textit{Modern Tort Law} 343;
  \item \textsuperscript{277} Ibid.
  \item \textsuperscript{278} Smith \textit{Internet Law} 323; Lloyd \textit{Information Technology Law} 579.
  \item \textsuperscript{279} Smith \textit{Internet Law} 320; Murphy \textit{Street on Torts} 506-507; Rogers \textit{Winfield & Jolowicz on Tort} 427; Harpwood \textit{Modern Tort Law} 344; Nel 2008 \textit{Responsa Meridiana} 113.
\end{itemize}
“c) in processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form;
d) …
e) as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.”

- Took reasonable care in relation to the statements publication;
  Section 1(5) of the Act provides that, when making this determination, regard must be had to the extent of the party’s responsibility for the statement or the decision to publish it; the nature or circumstances of the publication; and that party’s previous conduct or character. The reasonable care condition requires a certain degree of positive action by an ISP in relation to the content it disseminates. An inactive ISP would lose the innocent dissemination defence as it would not satisfy the reasonable care requirement. However, an over-active ISP may be deemed to have editorial control, thus also losing the defence.

- Did not have reason to believe that it had caused or contributed to the statements publication.
  Section 1(5) of the Act, also applies to the making of this determination.

280 S1(3) of the Defamation Act of 1996.
281 S1(5).
282 However, this requirement cannot be interpreted as imposing a general obligation on ISP’s to monitor their material as this would contravene Art of Directive 2000/31/EC which prevents member states from creating such an obligation.
283 Reed Internet Law 116-117; Nel “Freedom of expression” in Cyberlaw 204; Smith Internet Law 338; Roos “Freedom of expression” in ICT Law 418.
284 Reed Internet Law 116-117; Reed & Angel Computer Law 378; Roos “Freedom of expression” in ICT Law 418.
285 S1(1)(a)-(c) of the Defamation Act of 1996.
Godfrey v Demon Internet Ltd

This is the first UK case to deal with ISP liability for defamatory statements. An unknown third party pretended to be the plaintiff and posted a defamatory statement about him on a newsgroup hosted on the defendant ISP server. The plaintiff faxed a demand for the removal of the posting to the ISP’s managing director. The ISP admitted receiving the fax, but denied that it was personally received by the managing director. The defamatory statement was only deleted as part of normal routine two weeks later. It was not disputed that the post could have been deleted earlier. The ISP relied on section 1 of the Defamation Act and claimed that it was not a publisher of the statement in terms of the common law.

The court found that the ISP was not a publisher in terms of the Act; however it had not exercised reasonable care in relation to publication of the content as it had failed to remove it upon notification. It could therefore not rely on the Acts innocent dissemination defence. The court found that at common law publication did occur and that the ISP was liable. By using analogies of circulating libraries and distributors, the court held that the posting was published each time it was accessed and viewed by subscribers. Publication is usually a positive act; however there is authority for a party to be considered a publisher where they fail to remove the defamatory material, as they are responsible for the materials continued existence. The court did not accept that the ISP had played a passive role in relation to the defamatory content as it had chosen to store the newsgroup on its servers and was able to remove the content.

The court did not find USA case law to be of assistance because of the differences in the law. Using Lunney’s case as an example, the court found that on the same set of facts the ISP would be considered a publisher of the statements in the UK, and not a passive conduit as was held.

286 QBD (1999) 4 All ER 342.
287 343.
288 345.
289 342.
290 346.
291 348.
292 348.
293 352.
2 2 4 Criticism of the Godfrey case
Cyber-Rights & Cyber-Liberties (UK) stated that the Godfrey case would make the UK a hostile environment for network development and would have a “chilling effect” on the Internet. The case illustrated that the Defamation Act did not provide adequate protection for ISP’s. They submitted that the notification of the existence of a defamatory statement should not be enough to impose liability on ISP’s as this would result in it becoming the “judge and jury” in determining the validity of the complaints raised in such notices.294

2 2 5 Electronic Communications (European Community Directive) Regulations
The Defamation Act must be read with the EC Regulations.295 For an ISP performing the function of a host to obtain the limited liability provided by the EC Regulations, it must not have knowledge of the unlawful content and upon gaining such knowledge must expeditiously remove the content.296 There is a debate as to whether the EC Regulations change the Defamation Act’s knowledge criterion for unlawfulness from knowledge of a \textit{prima facie} defamatory statement to knowledge of an actionable statement.297 The British Law Commission found that ISP’s tend to remove content automatically upon receipt of a complaint notice. Removal occurred without consideration as to whether the content was is in the public interest or true. The Commission noted that this put pressure on the freedom of speech.298 It also exposes ISP’s to potential liability for breach of contract, should the content be found to be justified.299

2 2 6 Bunt v Tilley300
This case was decided after the EC Regulations were promulgated. It deals extensively with the application of the common law to ISP’s who are passive conduits.301 The plaintiff sought to hold three ISP defendants liable for the defamatory statements of three other defendants.

\footnotesize
295 Defamation and the Internet 7; Edwards “The fall” in Law and the Internet 53.
297 Smith Internet Law 336-337 378-379; Lloyd JT Law 584; Roos “Freedom of expression” in ICT Law 429; Defamation and the Internet 9. ‘Knowledge of actionability’ is knowledge as to the strengths or weaknesses of available defences. Smith Internet Law 336-337.
298 Defamation and the Internet 3.
299 Roos “Freedom of expression” in ICT Law 429; Defamation and the Internet 12.
301 341.
The ISP’s merely provided the Internet connection that made it possible for the other three defendants to transmit the content. The plaintiff relied on aspects of the decision in the Godfrey case which appeared to indicate that passive conduits could be held liable.

The court found that at common law, knowing involvement in the process of publication of the relevant defamatory words was required to impose liability on a party. Liability could not be imposed where a party performed a passive function in the publication process. The court held that the ISP’s were analogous to telephone companies in this instance, as they were passive conduits and did not publish the content, they could therefore not be deemed to be publishers or distributors at common law.

2 2 7 Web 2.0
An important Internet development has been the rise of a phenomenon known as ‘Web 2.0’. Web 2.0 websites are programmed by ISP’s, but the sites content, growth and development is predominantly due to the active participation of the sites users. Well known examples of Web 2.0 websites are YouTube, MySpace and Facebook. Recent cases have indicated that liability can arise for users from comment made while blogging and on Facebook.

2 2 8 ISP liability for third party defamatory content in the United Kingdom
ISP’s in the UK do not have the benefit of the broad immunity that exists in the USA. ISP’s can utilize the defence provided in the Defamation Act as they are not publishers in terms of section 1(3). However, cognizance of the remaining two requirements must be taken. Most importantly they must take reasonable steps upon gaining notice of the defamatory content.

---

302 338.
303 341.
304 343.
305 345.
306 It should be noted that there is not a universal recognition of Web 2.0. Older Internet developers state that ‘Web 2.0’ websites are simply different and do not denote a progression or new phase of Internet development. Regardless, it is a meme which defines a ‘particular cultural practice’. Brown 2008 Berk Tech LJ 441.
Where they fail to act on such notice, they may be deemed not to have taken reasonable care and lose the protection of the Act. Due to the uncertainty relating to the knowledge criterion, ISP’s would be best served by removing the content upon receipt of a reasonable complaint.

2.2.9 Relevance of the law of the United Kingdom to South Africa

The UK decisions serve as further examples for RSA law of how analogies are drawn and the legal principles applied to them. It is submitted that both of the above decisions applied the legal principles correctly to the facts before them. The following principles are useful to the RSA legal position:

- ISP’s who act as distributors should remove the content upon receipt of a reasonable complaint;\(^{310}\)

- IAP’s should not be considered publishers if there is not a knowing involvement in the process of the publication of the content as they are passive conduits.\(^{311}\)

2.3 Defamation: South Africa

2.3.1 Basic principles of defamation law in South African law

Defamation is part of the *actio iniuriarum*, which is an action for satisfaction for the wrongful and intentional injury to personality.\(^{312}\) Defamation can be defined as the wrongful, intentional publication of words or behaviour concerning another person which has the effect of injuring his status, good name or reputation.\(^{313}\) The elements are:

- Publication:
  
  Defamation relates to an injury to the opinion that others have of the claimant, thus publication to a third party is required. The claimant must prove that the other party

---

\(^{310}\) Godfrey v Demon Internet Ltd QBD (1999) 4 All ER 342; Nel 2008 *Responsa Meridiana* 114.


was aware or should have been reasonably aware of publication. A party, who repeats, confirms or draws attention to defamatory material can be found to have published it. 314

- Wrongfulness of the defamatory effect:
This is an objective test, based on the reasonable person who must be of the opinion that: the material was defamatory; referred to the claimant; and that there was an injury to the reputation of the claimant. 315 If the test is positive, then presumptions of wrongfulness and intention are created which the other party must rebut. 316 The presumption of wrongfulness can be rebutted by raising a ground of justification, such as absolute or qualified privilege. 317 The presumption of intention (discussed under animus iniurandi below) can be rebutted by raising a ground that excludes fault, such as mistake or jest. 318

- Animus iniurandi:
It must be proved that a party had the mental disposition to will the relevant consequences, with the knowledge that the consequence will be attained in a wrongful or unlawful manner. 319 Liability is therefore based on intention, unless the guilty party is the mass media in which case liability is based on negligence. 320 The reason for this difference began in Suid-Afrikaanse Uitsaakorporasie v O’Malley. 321 The court stated that defamatory statements made by the media cause greater harm than those made by an individual due to the media’s wider audience. The court stated further that it was

315 Neethling et al Law of Delict 309-310; Van der Walt & Midgley Principles of Delict 118-119; Kinghorn/Brand LAWSA 7 para 239; Burns Communications Law 158-160; Burchell Personality Rights 198; Neethling et al Law of Personality 135-136, 139-140.
316 Neethling et al Law of Delict 316; Van der Walt & Midgley Principles of Delict 119; Kinghorn/Brand LAWSA 7 para 234; Burns Communications Law 157-158; Burchell Personality Rights 207; Neethling et al Law of Personality 163.
318 Neethling et al Law of Delict 316-317; Van der Walt & Midgley Principles of Delict 163; Kinghorn/Brand LAWSA 7 para 245; Burns Communications Law 158; Neethling et al Law of Personality 164.
319 Neethling et al Law of Delict 316; Van der Walt & Midgley Principles of Delict 118-120; Kinghorn/Brand LAWSA 7 para 235; Burns Communications Law 170; Neethling et al Law of Personality 163.
321 1977 3 SA 394 (A).
difficult for an individual to prove intent on the part of the media.\textsuperscript{322} The case of \textit{Pakendorf v De Flamingh},\textsuperscript{323} citing the above reasons, found that strict liability should be imposed on newspaper owners, printers, publishers and editors.\textsuperscript{324} The result was that the media could not rely on defences excluding fault, only wrongfulness.

This position changed in \textit{National Media Ltd v Bogoshi}.\textsuperscript{325} The court found that the common law had always recognized the freedom of speech, the freedom of the press and the right to ones reputation. The protection of these rights is of the utmost importance to a democratic society and it would be incorrect to find either of these interests more important that the other.\textsuperscript{326} It stated that the press plays a large role in the free flow of information and the formation of public opinion, which serves the common good. The court held that strict liability has a chilling effect on this.\textsuperscript{327} The court held that the \textit{Pakendorf} case had incorrectly reflected the common law.\textsuperscript{328} However, the court found that due to the press’s powerful position it could not be treated in the same manner as private individuals. The press could rely too easily on the absence of knowledge of wrongfulness as a defence; therefore the form of fault for the press is negligence.\textsuperscript{329}

The test for negligence is an objective one, based on whether a reasonable person in the position of the defendant would foresee the reasonable possibility of his conduct causing damage and take reasonable steps to guard against such a result. If the defendant failed to take steps to do so, liability arises.\textsuperscript{330} Therefore the press will not be liable where it can show that under the circumstances that it was reasonable in publishing the material.\textsuperscript{331}

\textsuperscript{322} 404-405.
\textsuperscript{323} 1982 3 SA 146 (A).
\textsuperscript{324} Strict liability in this instance means that fault is attributed to the offending party automatically upon proof of harm as a result of the defamatory statement. Van der Walt & Midgley \textit{Principles of Delict} 159; Neethling et al \textit{Law of Delict} 329-331.
\textsuperscript{326} \textit{National Media Ltd v Bogoshi} 1998 4 All SA 347 (A) 356-357.
\textsuperscript{327} 360.
\textsuperscript{328} 366.
\textsuperscript{329} 364. Confirmed by \textit{Mthembi-Mahanye v Mail &Guardian Ltd and another} 2004 (6) SA 329 (SCA).
\textsuperscript{330} Neethling et al \textit{Law of Delict} 116-118; Van der Walt & Midgley \textit{Principles of Delict} 168; Burns \textit{Communications Law} 170-171. Test was formulated in \textit{Kruger v Coetzee} 1966 2 SA 428 (A) 430.
\textsuperscript{331} \textit{Mthembi-Mahanye v Mail &Guardian Ltd and another} 2004 (6) SA 329 (SCA) 46.
Bogoshi’s case further confirmed the decision in Trimble v Central News Agency\textsuperscript{332}, which dealt with distributor liability. A distributor has a defence if he proves:

- that he did not know that the newspaper at the time it was sold contained defamatory statements about the plaintiff;
- that it was not due to negligence on the vendor’s part that he did not know that there were any defamatory statements in the newspaper;
- that the newsvendor did not know that the paper was of such a character that it was likely to contain defamatory matter, nor ought he have known.\textsuperscript{333}

2 3 2 Tsichlas v Touchline Media (Pty) Ltd\textsuperscript{334}

This is the first reported case to deal with defamatory content on the Internet. The respondent ISP owned and published a soccer magazine website that provided a ‘chat forum’ for soccer fans.\textsuperscript{335} There had been a number of allegedly defamatory statements made about the applicant by users of the forum on the respondent’s website.\textsuperscript{336} The applicant sought to interdict the respondent from publishing defamatory statements about the applicant; an order for the respondent to remove the defamatory statements complained of; and an order that the respondent was to monitor its website and remove any defamatory content within an hour of its publication.\textsuperscript{337} The respondent, raised a number of defences, amongst which that it was protected by the ECTA.\textsuperscript{338}

The court viewed the orders for the removal of and further monitoring for defamatory statements as permanent interdicts. As such, the applicant had to prove certain elements to obtain such an order. The applicant failed to do so.\textsuperscript{339} The court also found that the interdicts for past and future publication would amount to a drastic infringement of the freedom of expression.\textsuperscript{340} The court rejected the respondents defence as it found that it did not fall under the definition of a service provider as it was a principal purveyor of information. The court

\textsuperscript{332} 1934 AD 43.
\textsuperscript{333} Trimble v Central News Agency 1934 AD 43.
\textsuperscript{334} 2004 (2) SA 112 (W).
\textsuperscript{335} 117.
\textsuperscript{336} 117-118.
\textsuperscript{337} 115.
\textsuperscript{338} 123.
\textsuperscript{339} 129-131.
\textsuperscript{340} 129.
elected not to make a binding decision relating to the administration, management and control of websites with chat forums as it believed that it was not necessary or appropriate.  

It is submitted that the court rightly dismissed the respondents defence, but for the wrong reasons. The correct reason why the respondent could not succeed in this defence was that it was not a member of an IRB. It has been suggested that the court mistakenly found that the respondent was a principal purveyor of information and as such, did not fall within the ECTA definition of a service provider. It therefore appears that the court misunderstood the meaning of a service provider to be that of only a mere conduit. The respondent was not a mere conduit, but it was a host and therefore should have been able to rely on the ECTA if it had complied with the other requirements to attain limited liability. This is another example of a court not fully understanding the technology of the Internet.

2.3.3 Suggestions for determining ISP liability for third party defamatory content in South Africa

USA and UK law illustrate that due to the myriad of roles that an ISP can perform, common law cannot provide one rule that can be used to determine ISP liability. Therefore, an ISP’s liability will have to be determined according to the facts of a particular case. Without sufficient authority, this can create an uncertain working environment for ISP’s. However, the examination of the jurisdictions does assist in suggesting how ISP liability may be determined.

ISP’s are intermediaries of content. An examination of the law of the different jurisdictions reveals three levels of intermediary activity, each with an increasing degree of risk of liability:

- Information carriers:
  Information carriers are intermediaries which merely convey content from one place to another without examining the content. Physical world examples are telephone companies. Information carriers are considered immune from liability.

---

341 123.
343 Roos “Freedom of expression” in ICT Law 432.
344 Reed Internet Law 115; Reed & Angel Computer Law 376; Roos “Freedom of expression” in ICT Law 417.
345 Reed Internet Law 115; Reed & Angel Computer Law 377; Roos “Freedom of expression” in ICT Law 417.
Information distributors
Information distributors also convey content, but there is a legal presumption that they have had an opportunity to examine the content. As a result, the law imposes additional conditions on them to avoid liability,\textsuperscript{346} examples are newsvendors. Each jurisdiction may differ as to what entity may be an information carrier or distributor.\textsuperscript{347}

Information controllers
Information controllers examine the content they transmit and prevent the transmission of unlawful content. These intermediaries can be held liable for third party content.\textsuperscript{348}

The examination further reveals common principles and practical examples in relation to ISP liability. It is now possible to suggest how ISP liability may be determined in RSA law. It is apparent that an ISP’s liability is dependent on the function it performs. Some of these functions are listed below with a determination of potential liability:

- Mere conduit:
  Examples of this function are IAP’s and e-mail service providers. These ISP’s are conduits for content and the function is performed in an automatic and passive manner. They are therefore analogous to a telephone company.\textsuperscript{349} As passive conduits they are not publishers and cannot be found liable.\textsuperscript{350}

- Hosts:
  ISP’s host a variety of information and have different relationships to it depending on the circumstances.

An ISP often performs its functions automatically through the use of technology that requires little human intervention, if any. In such circumstances it does not have real

\textsuperscript{346} Reed Internet Law 115-116; Reed & Angel Computer Law 377; Roos “Freedom of expression” in ICT Law 418.

\textsuperscript{347} Reed Internet Law 116; Reed & Angel Computer Law 377; Roos “Freedom of expression” in ICT Law 418.

\textsuperscript{348} Reed Internet Law 116; Reed & Angel Computer Law 378; Roos “Freedom of expression” in ICT Law 418.

\textsuperscript{349} Internet access providers were found to be analogous to telephone companies in Bunt v Tilley (2006) EWHC 407 (QB) 339. E-mail service providers were found to be analogous to telephone companies in Lunney v Prodigy Services Company 723 NE 2d 539 (NY 1999).

\textsuperscript{350} As found in the Bunt and Lunney’s cases.
knowledge of the nature of the content it disseminates. It therefore does not exercise real and effective editorial control, even if it makes use of automatic screening software.\footnote{Lunney \textit{v} Prodigy Services Company 683 NYS 2d 560(SD NY 1998).} Further, it cannot be expected to monitor all the content it disseminates due to volume.\footnote{Cubby \textit{v} CompuServe Inc 776 F Supp 135 (SD NY 1991); Zeran \textit{v} America Online Inc 129 F 3d 327 (4\textsuperscript{th} Cir 1997).} An ISP in this position is analogous to that of a distributor and the \textit{Trimble} distributor test for liability should be applied.\footnote{See Cubby \textit{v} CompuServe Inc 776 F Supp 135 (SD NY 1991); Godfrey \textit{v} Demon Internet Ltd QBD (1999) 4 All ER 342; Stratton Oakmont \textit{v} Prodigy Services Co 1995 NY Misc LEXIS 229 for examples of ISP’s performing this function.} Should the ISP gain knowledge of the content,\footnote{As occurred in Godfrey and Zeran’s cases.} the ISP will then fail the distributor test and should be found to be a publisher of the content.

It is submitted that an ISP should be considered to be a distributor where it makes similar technology, staffing and policy decisions to that of the defendant in \textit{Stratton}. If it is found to be a publisher in such circumstances it will have a negative effect on the Internet and prevent its further growth and innovation. However, should it be determined to be a publisher, then the principles of the \textit{Bogoshi} case should be applied.\footnote{See Van Zyl “Online defamation: Who is to blame?” 2006 (69) \textit{THRHR} 139, for an extensive discussion on why \textit{Bogoshi’s} case should always be applied to ISP’s who publish on bulletin boards, web pages and chat rooms.}

If the ISP’s position is analogous to that of a traditional publisher,\footnote{An example is Blumenthal \textit{v} Drudge and America Online Inc 992 F Supp 44 (DDC April 22 1998) Van Zyl 2006 \textit{THRHR} 146.} then \textit{Bogoshi’s} case should be followed.\footnote{Neethling et al \textit{Law of Delict} 308; Van der Walt \& Midgley \textit{Principles of Delict} 117-118; Kinghorn/Brand \textit{LAWSA} 7 para 236; Burns \textit{Communications Law} 155-156.} Fault should therefore be determined through the application of the negligence test. If an ISP is not considered to be part of the mass media, fault should be determined by the test for intention.

\begin{itemize}
  \item Information location tool:
  In the RSA, drawing attention to defamatory material can be deemed to be publication.\footnote{Neethling et al \textit{Law of Delict} 308; Van der Walt \& Midgley \textit{Principles of Delict} 117-118; Kinghorn/Brand \textit{LAWSA} 7 para 236; Burns \textit{Communications Law} 155-156.}
\end{itemize}
Where there was human intervention in the creation of a link or real knowledge of the link, it is submitted that an ISP can be potentially liable. If the ISP is considered to be part of the mass media, fault should be determined through the application of the negligence test. It must therefore be proved that the reasonable ISP would have acted differently. If the test for intention is used, then direction of will and consciousness of wrongfulness on the part of the ISP will have to be proved. The ISP’s liability will then depend on the nature of the link.\textsuperscript{359}

However, if the link is contained in the search results from a search engine ISP, the above tests will be difficult to prove due to the automatic nature of this function.\textsuperscript{360} As there is no human intervention or actual knowledge on the part of the ISP due to the automatic nature of this function, it is submitted that the ISP should be considered to be a passive conduit.\textsuperscript{361}

\section*{3 Hate speech}

The freedom of speech is recognized as a fundamental right in international law.\textsuperscript{362} It is however not an absolute right and certain types of speech are prohibited, such as hate speech.\textsuperscript{363} Hate speech can be regarded as disparaging, abusive, intimidating, harassing and hateful epithets, words or phrases that incite persons to violence, hatred or discrimination. It is directed at individuals or groups who represent a specific race, religion, ethnic background, gender or sexual preference.\textsuperscript{364} There is debate over the best way to deal with hate speech. There is the view that hate speech can be remedied through more speech, not by restricting speech.\textsuperscript{365} This argument is based on the market place of ideas theory that democracy is best

\textsuperscript{359} For example: A link to the particular section of the page where the defamatory statement appears could be considered to indicate intention as opposed to a link to the page or website where the statement is to be found.

\textsuperscript{360} See 5 5 on page 19 in Chapter 2 for a brief discussion on how such an ISP performs this function.

\textsuperscript{361} However, there is the view that search engines are analogous to libraries as the search results are a sophisticated version of a libraries card index. As are result they are distributors of content. See Smith \textit{Internet Law} 334.

\textsuperscript{362} Art 19 of the Universal Declaration of Human Rights (UN Res 217 A 1948); Art 19 of the International Covenant on Civil and Political Rights (UN Res 2200A 1966).

\textsuperscript{363} Art 20(2) of the International Covenant on Civil and Political Rights; Article 4 of the International Covenant on the Elimination of All Forms of Racial Discrimination (UN Res 2106 1966).


served by a process of the free expression of ideas and opinions through which the truth will emerge. Restricting speech is dangerous as it could eventually lead to the abolition of the freedom of speech. The counter argument is that hate speech should be remedied through restricting speech, as an absolute approach to free speech ignores the negative effects of hate speech. Tolerance of discrimination can lead to eventual tolerance of acts of violence being perpetrated against the target group.

The Internet provides extremist groups with an inexpensive organizing, recruiting and propaganda dissemination tool that grants them access to a wide audience. In an attempt to resolve this problem, the Additional Protocol to the Convention of Cybercrime was drafted. The Protocol requires signatories to criminalise the commission of racist or xenophobic acts through computer systems. The USA, UK and RSA are all signatories to the Convention on Cybercrime. The USA has not signed the Protocol, citing


Art 1 of the Additional Protocol (ETS no 189). These acts include the dissemination of racist or xenophobic material; racist or xenophobic motivated threat of the commission of a major criminal offence; racist or xenophobic motivated public insult; distributing of denial, gross minimisation, approval or justification of genocide or crimes against humanity. Art 3-6 of the Additional Protocol (ETS no 189).

The Convention on Cybercrime (Budapest 23 November 2001 ETS no 185) was drafted by the European Council with the assistance of the USA and RSA, due to international concern about crime committed through the use of the Internet. The Convention is the first international treaty to deal with Cybercrime and its objectives include the establishing of a common policy between signatories in identifying and investigating cybercrime, and improve international co-operation in cybercrime investigations. Preamble to the Convention on Cybercrime (ETS no 185); Council of Europe Convention on Cybercrime-Explanatory Report http://conventions.coe.int/ Treaty/en/Reports/Html/185.htm (accessed 20-05-2009) and subsequently Convention on Cybercrime-Explanatory Report; Council of Europe “Council of Europe Convention on Cybercrime: Frequently asked Questions and Answers” www.cybercrime.gov/COEFAQs.htm (accessed 23-05-2009) and subsequently United States Department of Justice “COEFAQ’s”.
inconsistencies with the freedom of expression. This highlights the difficulty in regulating online content different countries have different norms.

### 3.1 Hate Speech: United States of America

The freedom of speech is contained in the First Amendment of the constitution of the USA. It is not an absolute right as it can be restricted. It was decided in *Chaplinsky v New Hampshire*, that speech that is lewd, obscene, profane, libelous, insulting or constitutes fighting words is not protected. The USA however affords the freedom of speech wide protection, the underlying principle being that the government cannot prohibit the expression of ideas on the basis that society finds them “distasteful or discomforting”. As a result, federal legislation prohibiting hate speech does not currently exist. Legislation meant to regulate hate speech has often been found to be an unconstitutional restraint of the freedom of speech. The US Supreme Court developed a general rule in *Brandenburg v Ohio* that state law cannot forbid the advocacy of either the use of force or the violation of the law, unless such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action. Other countries, which have promulgated legislation that criminalizes hate speech, have criticized the USA for constitutionally

---

375 United States Department of Justice “COEFAQ’s” underneath ‘Information on other issues’.
376 An example is Yahoo! Inc v LICRA 145 F Supp 2d 1181 (ND Cal 2001), where an USA court found that it could not enforce a French judgment which found Yahoo! guilty of distributing Nazi memorabilia as this judgment was in conflict with the USA First Amendment. However, this decision has subsequently been overturned by the Ninth US Circuit Court of Appeals for procedural reasons. Roos “Freedom of expression” in *ICT Law* 443.
378 325 US 568 (1942).
379 Fighting words are words that are an incitement to violence. *Chaplinsky v New Hampshire* 325 US 568 (1942).
380 Burns Communications Law 116; Nel “Freedom of expression” in *Cyberlaw* 223; Reed Internet Law 258; Roos “Freedom of expression” in *ICT Law* 443; Brenner “Constitutional rights” in *IT Law Series* 257; Kende “Regulating Internet pornography aimed at children: A comparative Constitutional perspective on passing the camel through the needle’s eye” 2007 (6) Brigham Young University LR 1623 1623; Legal Instruments for Combating Racism 56.
382 Legal Instruments for Combating Racism 57.
385 447.
protecting it.\footnote{Leets 2001 \textit{Comm Law and Policy} 295.} It is argued that the USA is a safe harbour for hate organization websites, thus hampering other countries' efforts to restrict hate speech.\footnote{Nemes 2002 \textit{ICT Law} 195, 201; Leets 2001 \textit{Comm Law and Policy} 296.}

The \textit{Brandenburg} test has resulted in the courts generally not finding authors of texts to be capable of producing imminent lawless action, due to the separation of time and space between the author and his readers.\footnote{Carter et al \textit{Mass Communication Law} 46. Examples are: Davidson \textit{v} Time Warner Inc 1997 US Dist LEXIS 21559 (SD Tex 1997); Herceg \textit{v} Hustler Magazine 814 F 2d 1020 (5\textsuperscript{th} Circ 1987); Olivia \textit{v} NBC 178 Cal Rptr 888 (Ct App 1981). A notable exception is Rice \textit{v} Paladin Enterprises 128 F 3d 233 (4\textsuperscript{th} Circ 1997), which is the first mass-distributed book to be found to meet the \textit{Brandenburg} test for imminence. It was a how-to book for hitmen, and the information was used to perpetrate a contract killing.} It is also rare for the print media to be found liable for the actions of third parties.\footnote{968 F 2d 1110 (11\textsuperscript{th} Cir 1992).} An exception is \textit{Braun \textit{v} Soldier of Fortune Magazine},\footnote{Carter et al \textit{Mass Communication Law} 46.} where Michael Savage advertised himself in the magazine as a gun for hire and a mercenary who would consider any job. He was hired to commit a murder, which he proceeded to do. The magazine was sued and found liable as it had created a “clearly identifiable unreasonable risk of harm to the public”.\footnote{Azriel 2005 \textit{Comm Law and Policy} 495; Nel “Freedom of expression” in \textit{Cyberlaw} 223-224. However, see Columbia/Williamette Inc \textit{v} American Coalition of Life Advocates 290 F 3d 1058 (9th Cir 2002) where the \textit{Brandenburg} test was applied to an anti-abortion website which contained a list of personal details of over 200 abortion providers that appeared on an anti-abortion website. The list kept track of who was alive, injured and dead. 290 F 3d 1058 (9th Cir 2002) 1063-1065. The court found that the content was not protected speech as it was a score card, contained too much personal information and constituted a threat against those who appeared on the list. 290 F 3d 1058 (9th Cir 2002) 1088. It is submitted that the \textit{Brandenburg} test was applied incorrectly by the court as the test requires imminent lawless action, of which there was no evidence.}

### 3.1.1 Hate speech and the Internet

The imminence requirement cannot be properly applied to the Internet due to unknown variables for example: the length of time it may take before a user accesses the hate speech online or the geographical distance between users and a particular target.\footnote{Azriel 2005 \textit{Comm Law and Policy} 495. Nemes 2002 \textit{ICT Law} 209.} It is therefore doubtful that many users of the Internet will be incited to imminent lawless action by online content.\footnote{Azriel 2005 \textit{Comm Law and Policy} 495; Nel “Freedom of expression” in \textit{Cyberlaw} 223-224. However, see Columbia/Williamette Inc \textit{v} American Coalition of Life Advocates 290 F 3d 1058 (9th Cir 2002) where the \textit{Brandenburg} test was applied to an anti-abortion website which contained a list of personal details of over 200 abortion providers that appeared on an anti-abortion website. The list kept track of who was alive, injured and dead. 290 F 3d 1058 (9th Cir 2002) 1063-1065. The court found that the content was not protected speech as it was a score card, contained too much personal information and constituted a threat against those who appeared on the list. 290 F 3d 1058 (9th Cir 2002) 1088. It is submitted that the \textit{Brandenburg} test was applied incorrectly by the court as the test requires imminent lawless action, of which there was no evidence.}
3 1 2 ISP liability for third party hate speech in the United States of America

It is submitted that the protection offered by section 230(c)(1) of the CDA is broad enough to grant ISP’s immunity from civil liability for hate speech. This means that an ISP in the position of the Soldier of Fortune Magazine would be protected, therefore highlighting the difference in protection afforded to analogous offline entities. Section 230(c)(1) does not grant ISP’s immunity from criminal liability. Due to the wide protection of the freedom of speech, it seems unlikely that an ISP could be found liable for a third party’s hate speech.

3 2 Hate Speech: United Kingdom

In the UK, the freedom of expression is contained in the Human Rights Act of 1998. The UK has acknowledged that racial hatred can disturb the public order. Speech that causes racial hatred is prohibited in Part III of the Public Order Act of 1986. Section 17 defines, racial hatred as hatred against a group of persons defined by “reference to colour, race, nationality, ethnic or national origins”. Acts which are threatening, abusive or insulting and that are intended or are likely to stir up racial hatred are criminalized. The provisions of the Public Order Act have been amended by the Racial and Religious Hatred Act of 2006 and section 74 of the Criminal Justice and Immigration Act of 2008. If an offence is committed in terms of the Public Order Act with the consent or connivance of a director, manager, secretary, member or similar officer of a corporation, both the offending party and the corporation are guilty of the offence and can be prosecuted. Authorities have indicated that ISP’s can be prosecuted in terms of the Act where they are aware of hate speech on their networks and fail to remove it. It is therefore possible for an ISP to be liable as a publisher or distributor in

394 See 2 1 6 supra.
395 42 USC § 230(c)(1) of the CDA of 1996.
396 Burns Communications Law 119; Legal Instruments for Combating Racism 95; Cucereanu Aspects of Regulating 35.
397 Such as: the use of words or behaviour; the publication, display or distribution of written material; a public performance of a play; the distribution, showing or playing of a recording of visual images or sounds; a programme with sounds or visuals; the possession of written material, or recording of visual images or sounds, with the view of displaying, distributing or publishing the material, whether by himself or another. Ss18-23 of the Public Order Act of 1986.
398 Both amending acts have expanded the ss18-23 offences to include inciting hatred against a person on the grounds of their religion or their sexual orientation (whether towards persons of the same sex, opposite sex or both) respectively.
399 In terms of ss28- 29M of the Public Order Act of 1986. A guilty party can receive a sentence of up to seven years, a fine or both in terms of s27(3) and s29L of the Public Order Act of 1986.
400 Legal Instruments for Combating Racism 96.
terms of the Public Order Act of 1986. There have however been no prosecutions in the UK for hate speech on the Internet.\textsuperscript{401} An ISP will have a defence in relation to the offences created in terms of the Public Order Act if it can prove that it did not have intention, or suspect or reasonably suspect the acts to be threatening, abusive or insulting.\textsuperscript{402}

3 2 1 ISP liability for third party hate speech in the United Kingdom

The current position in the UK is that an ISP will not be liable if it falls into one of the three categories of service providers whose liability is limited should they unknowingly transmit or store a third party's unlawful content, in terms of the EC Regulations.\textsuperscript{403} These defences deal with unlawful content in general, rather than hate speech in particular. If an ISP knowingly transmits hate speech it loses the protection of the EC Regulations and commits an offence in terms of the Public Order Act.

3 3 Hate speech: South Africa

The right to the freedom of expression is protected in RSA by section 16 of the Constitution. It is limited by section 16(2), which provides that the advocacy of hatred based on race, ethnicity, gender or religion that results in an incitement to cause harm is prohibited. ISP’s face potential liability for hate speech in terms of the FPA and the Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000 (Equality Act).

3 3 1 Films and Publications Act

The distribution of publications or films, which judged in context, amount to advocacy of hatred based on race, ethnicity, gender or religion and which constitutes an incitement to cause harm is prohibited in terms of sections 29(1)-(2) of the FPA.\textsuperscript{404} The offence can only be

\textsuperscript{401} Nel “Freedom of expression” in Cyberlaw 223; Legal Instruments for Combating Racism 96.
\textsuperscript{402} Ss18-23 and s29B-G of the Public Order Act of 1986.
\textsuperscript{403} Legal Instruments for Combating Racism 97. S21 of SI 2002/2013 expands the ss17-19 categories of mere conduits, caching & hosting to criminal proceedings as well.
\textsuperscript{404} S29(1) Act 65 of 1996 provides that it is an offence to knowingly broadcast or distribute a publication that advocates hatred based on grounds \textit{supra}. S29(2) creates a similar offence in relation to the broadcast, exhibition in public or distribution of a film. S32 of the Film and Publications Amendment Act 3 of 2009 will repeal s29 of the FPA. S29 of Act 3 of 2009 will insert s24A(2) into the FPA, in terms of which it is an offence to knowingly distribute, broadcast, exhibit in public, offer for sale or hire or advertises as such any film, game or publication that is classified as ‘refused classification’. A publication (in terms of the substituted s16(4)(a)(ii) or film (in terms of substituted s18(3)(a)(ii)) that includes the advocacy of hatred based on any ‘identifiable group characteristic’. The definition for this term expands the application of hate speech to include the advocacy of hatred on the basis of sex, pregnancy, marital status, social origin, colour sexual orientation, age, disability, conscience, belief, culture, language, birth and nationality.
committed ‘knowingly’. Persons guilty of these offences can be prosecuted and sentenced to a fine or imprisonment. It is not an offence to download or possess hate speech. ISP’s who knowingly distribute hate speech will therefore be guilty of an offence.

3.3.2 Promotion of Equality and Prevention of Unfair Discrimination Act

The legislature noted that social, economic and systemic inequalities and unfair discrimination, created by RSA’s past, remain deeply entrenched in social structures, practices and attitudes. The Equality Act was therefore promulgated with the object of preventing and prohibiting unfair discrimination, harassment and hate speech; and to promote equality and eliminate unfair discrimination.

It is submitted that there are at least two sections of the Equality Act which impose duties on ISP’s. Section 10(1) of the Act provides that no person may publish, propagate, advocate or communicate words, which fall within the prohibited grounds, against another person that could demonstrate a clear intention to be hurtful, harmful, incite harm or promote or propagate hatred. It is not necessary that the hate speech cause actual harm. Section 10 is subject to the proviso contained in section 12 of the Equality Act which provides that the offences do not preclude bona fide engagement in artistic creativity, academic and scientific inquiry, fair and accurate reporting in the public interest or publication of any information, advertisement or notice in accordance with section 16 of the Constitution. A further obligation is placed on ISP’s in terms of section 12 which provides that a person may not

---

406 S30(1) of Act 65 of 1996 the offender can be fined or imprisoned for a period not exceeding five years or both.
408 Preamble to Act 4 of 2000.
410 In terms of s1(xxii) of Act 4 of 2000, the prohibited grounds are: (a) race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth; or (b) any other ground where discrimination based on that other ground (i) causes or perpetuates systematic disadvantage; (ii) undermines human dignity; or (iii) adversely affects the equal enjoyment of a person’s rights and freedoms in a serious manner that is comparable to discrimination on a ground in para (a).
411 Teichner 2003 SAJHR 369.
disseminate or broadcast any information, or publish or display any advertisement or notice, which amounts to speech that clearly intends to unfairly discriminate against any person.

These sections place a duty on persons to monitor speech that they propagate or disseminate for particular forms of offending speech. It is submitted that this places a duty on ISP’s to monitor the material they transmit for hate speech and for speech that unfairly discriminates against any person. A breach of the statutory duties created in terms of the Equality Act is merely an indication of wrongfulness. For a party to be liable, all of the general principles of liability should be applied. As this is a legal duty, it is submitted that fault in the form of negligence would have to be present.412

ISP’s that fail to perform their duties in terms of the Equality Act expose themselves to a large group of potential litigants.413 An order of the Equality Court has the effect of a civil court order.414 The Equality Court however has a wide discretion as to the nature of the order it may grant, exposing an ISP not only to financial loss but also to onerous administrative obligations.415 Further, the Equality Court has the discretion to forward the matter to the

412 Midgley & Van Der Walt “Breach of a statutory duty or negligent exercise of a statutory power” LAWSA 8(1) (2005) para 74. It is submitted that due to the importance of this legislation in relation to healing the negative effects of RSA’s past, these duties do not impose a standard of care, but rather a duty in absolute terms. In Lascon Properties (Pty) Ltd v Wadeville Investment Co (Pty) Ltd and another 1997 (4) SA 578 (W), the court found that a particular regulation had imposed a legal duty in absolute terms, as opposed to a standard of care, on mining companies to prevent noxious water escaping. The court found that those harmed by an escape of such water could claim compensation. Midgley & Van Der Walt suggest in LAWSA 8(1) para 74 that fault in the form of negligence applies in this circumstance, despite the court not clearly indicating so. As the duties in the Equality Act are to ensure that persons do not let ‘noxious’ speech escape, it is submitted that fault in the form of negligence applies.

413 In terms of s20(1) of Act 4 2000, persons acting: in their own interest; on behalf of another person who cannot act in their names; as a member of an interest group; in the public interest; any association in the interests of its members; South African Human Rights Commission; Commission for Gender Equality. Therefore, unlike defamation actions, an ISP can be litigated against by a potentially well resourced individual or group.

414 S21(3) of Act 4 of 2000.

415 In terms of s21(2) of Act 4 of 2000 an ISP could be ordered to: pay damages; take specific steps against the hate speeches publication; implementation of special measures to address the hate speech; make an unconditional apology; undergo an audit of specific policies or practices as determined by the court. Further the order may be deterrent in nature, including the recommendation to the appropriate authority, to suspend or revoke the licence of a person; a directive requiring the respondent to make regular progress reports to the court or to the relevant constitutional institution regarding the implementation of the court’s order; an order directing the clerk of the Equality Court to submit the matter to the Director of Public Prosecutions having jurisdiction for the possible institution of criminal proceedings in terms of the common law or relevant legislation; an appropriate order of costs against any party to the proceedings; an order to comply with any provision of the Act.
Director of Public Prosecutions for the institution of criminal proceedings.\textsuperscript{416}

The advantage of the Equality Act is that it provides protection to more groups of people compared to the other jurisdictions examined. It does however place a potentially onerous burden on ISP’s that does not exist in the other jurisdictions. It could therefore lead to ISP’s moving offshore to limit the duties they must perform and liability they potentially face. This would obviously negatively effect the growth and development of the Internet in RSA.

\textbf{3 3 3 Suggestions as to the extent of ISP liability for third party hate speech in South Africa}

In terms of the FPA, ISP’s can only be found criminally liable for knowingly distributing hate speech.\textsuperscript{417} It is suggested that the Equality Act\textsuperscript{418} imposes a duty on ISP’s to monitor the content they transmit for hate speech and for speech that unfairly discriminates against any person. An ISP which negligently fails to perform this task exposes itself to financial loss or onerous administrative obligations imposed by an order of the Equality Court.

\textbf{4 Obscenity and indecency}

There is international consensus that a country should control the possession and dissemination of obscene and indecent material. There is however not consensus on what is obscene and indecent.\textsuperscript{419} Due to reports by the media of the prevalence of obscene and indecent content on the Internet, there are questions as to the extent of ISP liability for this content.\textsuperscript{420}

\textsuperscript{416} S10(2) of Act 4 2000.
\textsuperscript{417} S29(1)-(2) of Act 65 of 1996.
\textsuperscript{418} S10 and 12.
\textsuperscript{419} For example: In some countries it is acceptable to depict naked adults, whereas in others it is not only unacceptable but unlawful. Further, differences can exist as to what is child pornography as there could be a difference in the age of consent to sexual activity. Reed & Angel Computer Law 380; Reed Internet Law 106; Nair “Internet Content Regulation: Is it a global community standard a fallacy or the only way out?” 2007 (21) International Review of Law, Comp & Tech 15 19; Roos “Freedom of expression” in ICT Law 450, 452.
\textsuperscript{420} Reed & Angel Computer Law 380; Nel “Freedom of expression” in Cyberlaw 210; Lloyd IT Law 249; Roos “Freedom of expression” in ICT Law 418, 449-450.
There is however international consensus that a particular type of obscene material, child pornography, is unlawful. Further, there is growing concern as to the extent that the Internet is becoming the primary method of dissemination of this content and assisting in the facilitation of sexual offences against children. It was therefore felt that an international legal instrument was required to combat this disturbing trend which ultimately resulted in, the Convention on Cybercrime. The Convention contains model offences for signatories to implement in their national law. In terms of the Convention intent is required in order to commit any of the offences related to child pornography. ISP’s would therefore only be liable where they have knowledge of the child pornography and fail to remove it. The USA, UK and RSA are signatories to this Convention and have undertaken to promulgate legislation that will implement the principles contained in the Convention.

4.1 Obscenity and indecency: United States of America

4.1.1 The test for obscenity in the United States of America

In the USA obscene material is limited to sexual material. The US Supreme Court held in Miller v California that obscene material has low constitutional value and is therefore not protected by the First Amendment. The court developed a three part test to determine whether material can be considered obscene:

---

421 Reed Internet Law 107; Roos “Freedom of expression” in ICT Law 450.
423 Ibid.
424 The Convention on Cybercrime (Budapest 23 November 2001 ETS no 185).
425 Preamble to the Convention on Cybercrime (ETS no 185).
426 Art 9 of the Convention on Cybercrime (ETS no 185). These offences include the intentional production for distribution; offering or making available; distribution and dissemination; procurement and possession of child pornography. In terms of art 9(4), parties to the convention can elect not to apply in whole or in part the provisions relating to the criminalizing of the procuring or possession of child pornography.
428 Reed & Angel Computer Law 380; Reed Internet Law 106; Siegel Communications Law 391. A variety of offences exist in relation to obscene material in the United States Code, such as the importation or transporting of obscene material, including via the Internet. The penalty for this offence is a fine, or imprisonment of up to five years, or both. 18 USC § 1462. The United States Code is the codification by subject of the general and permanent laws of the United States. It is published by the Office of the Law Revision Counsel of the U.S. House of Representatives. GPO Access “United States Code-About” http://www.gpoaccess.gov/uscode/about.html (accessed on 1-06-2009).
“(a) whether the average person, applying contemporary community standards, would find that the work, taken as a whole, appeals to the prurient interest, (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law, and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.”

Pornography can be prohibited if determined to be obscene in terms of the Miller test. The test is based on the local standards of acceptable depiction of sexual activity and any applicable state law. The test is not based on the effects that the material may have on individuals or the community. This test can be criticized because of the difference between communities as to what is obscene and therefore what is legal, thus creating uncertainty for publishers and ISP's.

In New York v Ferber, it was held that child pornography may be prohibited regardless of whether it is obscene because of the government’s interest in protecting minors from sexual exploitation. The Child Pornography Prevention Act of 1996 prohibited the visual depiction of real or virtual minors engaged in sexual conduct. However, the Supreme Court found in Ashcroft v Free Speech Coalition that the prohibition of virtual child pornography was unconstitutional as it prohibited speech that was neither obscene nor child pornography.

430 24.
431 Nunziato “Technology and pornography” 2007 (6) Brigham Young University LR 1535 1539; Siegel Communications Law 401.
432 Reed 106; Reed & Angel 380; Brenner “Constitutional rights” in IT Law Series 257; Roos “Freedom of expression” in ICT Law 450-451.
433 Reed 106; Reed & Angel 380.
434 Reed 106; Reed & Angel 380; Brenner “Constitutional rights” in Information Technology 257; Roos “Freedom of expression” in ICT Law 451. For example: In United States v Thomas 74 F 3d 701 (6th Cir) cert denied 117 S Ct 74 (1996), a bulletin board operator faced criminal charges in Tennessee for material stored on a computer in California. The operator was extradited from the state of California to the state of Tennessee, where he argued that the material was not obscene by Californian standards. However he was found guilty as the court applied the standards of Tennessee as this was where the material was received and viewed.
436 458 US 747 (1982); Siegel Communications Law 407-408. It is an offence to knowingly transport, receive, distribute, reproduce, advertise or promote, sell or possess to sell or possess child pornography. These offences can also be committed via the Internet.18 USC § 2252A. The penalty for these offences is a fine and 5-20 years imprisonment. 18 USC § 2252A(b).
It also prohibited speech of a serious literary, artistic, political, or scientific value.\textsuperscript{440} Congress found that the \textit{Free Speech Coalition} case had an adverse effect on prosecutions of child pornography and made it increasingly difficult to enforce child pornography laws online.\textsuperscript{441} In response the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003 (PROTECT Act)\textsuperscript{442} was promulgated to enable the effective prosecution of online child pornography.\textsuperscript{443} The Act made various amendments to USA law including expanding the definition of child pornography to include virtual child pornography.\textsuperscript{444} The PROTECT Act further amends the Victims of Child Abuse Act of 1990, by imposing a duty on ISP’s to report the existence of child pornography to authorities.\textsuperscript{445} ISP’s are however not required to monitor for child pornography.\textsuperscript{446} The PROTECT Act has survived constitutional scrutiny in the Supreme Court.\textsuperscript{447}

\textbf{4 1 2 Indecency in the United States of America}

In \textit{Reno v American Civil Liberties Union},\textsuperscript{448} the Supreme Court referred to authority that material that contains indecent (i.e. not obscene) sexual expression is protected by the First Amendment. Offensive material does not justify its suppression. Therefore, generally available commercial pornography can be considered indecent, but is protected by the First Amendment.\textsuperscript{449} There have been attempts for legislation to be enacted that recognizes

\begin{itemize}
  \item \textsuperscript{440} 535 US 234 (2002); Roos “Freedom of expression” in ICT Law 453; Carter et al \textit{Mass Communication Law} 204-205.
  \item \textsuperscript{441} Ss501(9), 501(13) of the Prosecutorial Remedies and Other Tools to End the Exploitation of children today Act of 2003 Pub L No 108-21.
  \item \textsuperscript{442} 18 USC § 2422 ff Pub L No 108-21.
  \item \textsuperscript{443} S501(15) of PROTECT Act of 2003.
  \item \textsuperscript{444} 18 USC § 2256(8)(B).
  \item \textsuperscript{445} 42 USC § 13032(b). An ISP that fails to report the existence of child pornography shall be fined not more than $50 000 for an initial failure and not more than $100 000 for a second or subsequent failure. 42 USC § 13032(b)(4); Akdeniz \textit{Internet Child Pornography} 245.
  \item \textsuperscript{446} 42 USC § 13032(e); Akdeniz \textit{Internet Child Pornography} 245.
  \item \textsuperscript{447} United States v Williams 553 US 285 (2008).
  \item \textsuperscript{448} 521 US 844 (1997).
  \item \textsuperscript{449} Fee “Obscenity and the World Wide Web” 2007 (6) \textit{Brigham Young LR} 1691 1695-1696; Nunziato “Technology and pornography” 2007 (6) \textit{Brigham Young University LR} 1538; Kende 2007 \textit{Brigham Young University LR} 1623; Siegel \textit{Communications Law} 391.
\end{itemize}
It is possible in the USA for distributors to be found guilty of distributing pornographic material to minors.\textsuperscript{451} In \textit{Ginsberg v New York},\textsuperscript{452} the owner of a store was found guilty in terms of a New York statute for selling pornographic material to a minor. The Supreme Court found this to be a constitutional restriction.\textsuperscript{453} The court held that the concept of what is obscene would change depending on the audience. Therefore the material would not be obscene to majors but considered obscene for minors when the obscenity test was adapted for that particular audience.\textsuperscript{454}

4 1 3 Regulation of obscenity and indecency on the Internet

The USA government became concerned with the ease that minors could access obscene and indecent content on the Internet.\textsuperscript{455} There have been a number of attempts by the government to regulate minors access to such content. The courts have found that the government has a legitimate interest in limiting minor’s access to obscene and indecent material, but that it does not have a legitimate interest in limiting adults access to such material.\textsuperscript{456}

The first attempt was the CDA which created a number of criminal offences in relation to displaying obscene or indecent content to minors. The constitutionality of the CDA was challenged in \textit{Reno v American Civil Liberties Union}.\textsuperscript{457} The court found the anti-indecency

\begin{thebibliography}{9}
\bibitem{450} Burns \textit{Communications Law} 141; Siegel \textit{Communications Law} 410-411; Carter et al \textit{Mass Communication Law} 209.
\bibitem{451} \textit{Ginsberg v New York} 390 US 629 (1968); Siegel \textit{Communications Law} 405; Nunziato 2007 \textit{Brigham Young University LR} 1542; Carter et al \textit{Mass Communication Law} 199.
\bibitem{452} 390 US 629 (1968).
\bibitem{453} 639.
\bibitem{454} 646; Siegel \textit{Communications Law} 405; Nunziato 2007 \textit{Brigham Young University LR} 1542.
\bibitem{455} Nunziato 2007 \textit{Brigham Young University LR} 1535; Carter et al \textit{Mass Communication Law} 642.
\bibitem{456} \textit{Reno v American Civil Liberties Union} 521 US 844 (1997); Nunziato 2007 \textit{Brigham Young University LR} 1538; Carter et al \textit{Mass Communication Law} 643.
\bibitem{457} 521 US 844 (1997).
\end{thebibliography}
provisions unconstitutional, but upheld the provisions in so far as obscenity or pedophilic content was concerned. The second attempt was the Child Online Protection Act of 1998. However, in American Civil Liberties Union v Reno a preliminary injunction prohibiting the implementation of the Act was granted. The federal district court found that the applicant could possibly prove that there were less restrictive means to protect minors from harmful content, such as filtering and blocking technology. Over the next decade the USA Department of Justice made a number of attempts the appeal courts to have the legislation enacted, with the Supreme Court refusing to hear the last appeal in 2009. The only legislation to be successfully implemented thus far has been the Children’s Internet Protection Act of 2000. In terms of this legislation government funded schools and libraries are required to use filtering technology to block obscene content and content that is harmful to minors under the age of seventeen years. When an adult uses the computer, the filtering technology should block obscene content. Challenges on the basis of the legislation creating an unconstitutional prior restraint of the freedom of speech have met with mixed success.

---

458 896-897. The court found that sections of the CDA unconstitutionally infringed the First Amendment as the terms used were too general and undefined, therefore potentially restricting constitutionally protected material that had educational or other value. 521 US 844 (1997) 874.
459 47 USC § 231 ff Pub L No 105-277.
460 31 F Supp 2d 473 (ED Pa 1999).
466 In the US District Court of the Eastern District of Virginia case of Mainstream Loudon v Board of the Loudoun County Library 2 F Supp 2d 783 794-95 (ED Va 1998), the legislation was found to be unconstitutional. However, a similar decision in US District Court of the Eastern District of Pennsylvania was overturned on appeal in the Supreme Court in United States et al v American Library Association Inc et al (02-361) 539 US 194 (2003) 201 F Supp 2d 401 reversed.
4 1 4 ISP liability for third party obscene and indecent content in the United States of America

ISP’s would not be liable for the transmission or possession of indecent content as it is protected by the First Amendment. In relation to civil liability for obscene content, ISP’s now enjoy broad immunity in terms section 230(c)(1) of the CDA. However, ISP’s have an obligation to report the existence of child pornography.

4 2 Obscenity and Indecency: United Kingdom


4 2 1 Obscene Publications Act

This Act provides that material is obscene if it has a tendency to deprave or corrupt those exposed to it.\textsuperscript{467} Unlike the USA, obscenity in the UK is not limited to sexual material.\textsuperscript{468} It is an offence to publish and possess obscene material.\textsuperscript{469} A person may also be liable for obscene material contained in a recorded or live programme service.\textsuperscript{470} An ISP could be liable for a third party’s obscene content if it was aware of facts that should have caused it to investigate the nature of the content.\textsuperscript{471} The Obscene Publications Act has been applied to the Internet and it has been held that:

- making obscene content available for transfer to another party, who is enabled access to it, amounts to showing the content and therefore publication;\textsuperscript{472}

\textsuperscript{467} S1 of the Obscene Publications Act of 1959.
\textsuperscript{468} For example: In the case of \textit{DPP v A and BC Chewing Gum Ltd} (1968) 1 QB 159 chewing gum cards that depicted scenes of military violence were deemed by the court to be obscene.
\textsuperscript{469} S2(1)of the Obscene Publications Act of 1959. In terms of s1(3)(a), publishing includes the distribution, circulation, selling, hiring, giving, lending or offering to sell or hiring of obscene material. In terms of s1(3)(b), publishing includes the showing, playing, projecting or transmission of the material if it is stored electronically. A person convicted for contravening the act can be fined or imprisoned for a period of up to three years or both. S2(1)(b) of the Obscene Publications Act of 1959.
\textsuperscript{470} S1(4)-(6) of the Obscene Publications Act of 1959; Smith \textit{Internet Law} 961. In terms of s201 of the Broadcasting Act of 1990 a programme service is a service whereby sounds, visual images or both are sent by an electronic communications network for reception at two or more places in the UK. The Broadcasting Act provides that obscene material will be considered as being kept by a party for publication for gain where that party has such obscene material in his possession, ownership or control and intends to include the material in a programme. Schedule 15 at par 3 of the Broadcasting Act of 1990.
\textsuperscript{471} Smith \textit{Internet Law} 963; Reed \textit{Internet Law} 108.
\textsuperscript{472} \textit{R v Fellows, R v Arnold} (1997) 2 All ER 548 CA.
- the uploading of obscene content to a foreign server amounts to publication;\textsuperscript{473}
- the transmission of the obscene content into the UK amounts to publication.\textsuperscript{474}

An ISP would have a defence if it can prove that it did not examine the content and that it did not have a reasonable cause to suspect that the publication or possession of the content would be an offence in terms of the Act.\textsuperscript{475} These defences exist independently of those contained in the EC Regulations 2002.\textsuperscript{476} There have been no prosecutions of an ISP for a third parties obscene content.\textsuperscript{477}

4 2 2 Protection of Children Act

In terms of the Protection of Children Act of 1978, it is an offence to produce, distribute, possess and publish child pornography.\textsuperscript{478} The definition of a ‘photograph’ was amended by the Criminal Justice and Public Order Act of 1994 to include data stored on an electronic medium that is capable of conversion into a photograph.\textsuperscript{479} It also introduced the term ‘pseudo-photograph’, which is defined as an image that appears to be a photograph.\textsuperscript{480} This was included to cover computer generated and manipulated images.\textsuperscript{481} If an offence is committed in terms of the Act with the consent or connivance of a director, manager, secretary, member or similar officer of a corporation, both the offending party and the corporation are guilty of the offence and can be prosecuted.\textsuperscript{482} The PCA has been applied to the Internet, and courts have held that:

- a person who downloads images or prints them in the UK is ‘making’ the images, i.e. creating new material;\textsuperscript{483}

\textsuperscript{473} R v Waddon (2000) All ER (D) 502.
\textsuperscript{474} R v Perrin (2002) EWCA Crim 747.
\textsuperscript{475} S1(5) of the Obscene Publications Act of 1959 in relation to publication and possession; Broadcasting Act 1990 Sch 15 5(1) in relation to programming.
\textsuperscript{476} Defences of mere conduit, cache and host contained in reg 17-19 SI 2002/2013.
\textsuperscript{477} Sutter “Don’t shoot the messenger? The UK and online intermediary liability” 2003(17) International Review of Law, Computers & Tech 73 75; Akdeniz Internet Child Pornography 231-232; Edwards “Pornography” in Law and the Internet 623.
\textsuperscript{478} S1 of the Protection of Children Act 1978.
\textsuperscript{479} S7 of the Protection of Children Act of 1994.
\textsuperscript{480} S7(7).
\textsuperscript{481} Smith Internet Law 964; Cucereanu Aspects of Regulating 54.
\textsuperscript{482} S3 of the Protection of Children Act of 1994. A person found guilty of an offence in can be sentenced to ten years imprisonment, a fine or both. S6(2) of the Protection of Children Act of 1994.
unintentional copying does not constitute making of the images;\textsuperscript{484}

searching the Internet and selecting images to appear on the computers monitor constitutes making the images.\textsuperscript{485}

An ISP may utilise the defence provided in section 1(4) of Act, if it can show that: it had legitimate reasons for distributing, showing or possessing the content; or that it had not seen the content; or had no reason to know or suspect them to be indecent. It is therefore possible for ISP’s to be liable for possession, distribution or publication of a third party’s child pornography if cause existed for it to know or suspect that the content was in fact child pornography.\textsuperscript{486}

\textbf{4 2 3 Criminal Justice and Immigration Act}

It is an offence to be in possession of an extreme pornographic image.\textsuperscript{487} An image includes a moving image, still image, or data in any form that can be converted to a moving or still image.\textsuperscript{488} To be guilty of this offence one must have seen the image and known, or had cause to suspect, that the image was an extreme pornographic image.\textsuperscript{489} Therefore if an ISP fails to remove an image that it is aware is an extreme pornographic image it is committing an offence.

\textbf{4 2 4 ISP liability for third party obscene and indecent content in the United Kingdom}

There have not been decided cases in the UK in relation to ISP liability for a third party’s obscene content.\textsuperscript{490} However, it appears that they could be liable in terms of the legislation \textit{supra} should they have knowledge of the content and fail to act appropriately. Knowledge would exclude the defences available in terms of the EC Regulations.

\textsuperscript{484} Atkins v DPP (2000) 2 All ER 425 QBD Divisional Court.
\textsuperscript{485} R v Smith and Jayson (2002) EWCA Crim 683.
\textsuperscript{486} Smith Internet Law 963; Reed Internet Law 108; Akdeniz Internet Child Pornography 232; Edwards “Pornography” in Law and the Internet 623.
\textsuperscript{487} In terms of s63(7) of the Criminal Justice and Immigration Act of 2008 an image is extreme if it depicts an act that: threatens a persons life; which results or could result in serious injury to a persons anus, breast or genitals; involves the sexual interference with a human corpse; or a person performing sexual intercourse with an alive or dead animal.
\textsuperscript{488} S63(8) of the Criminal Justice and Immigration Act of 2008.
\textsuperscript{489} S65 (2)(b).
\textsuperscript{490} Sutter 2003 International Review of Law, Computers & Tech 75; Akdeniz Internet Child Pornography 231-232.
### 4.3 Obscenity and Indecency: South Africa

The FPA regulates the creation, production, possession and distribution of certain publications and films by way of: classification; the imposition of age restrictions; and provision of consumer advice. One of the FPA’s objects is to provide protection to children from sexual exploitation in publications, films and the Internet. The definitions for ‘publication’ and ‘film’ is very wide, covering all forms of Internet content.

#### 4.3.1 Classification in terms of the Films and Publications Act

A classification committee of the Films and Publications Board deals with the classifications of any publication or film. Publications are only classified upon receipt of a complaint. However, persons who wish to distribute or exhibit any film must submit it for classification. Persons who intend to distribute or exhibit any film must register with the Films and Publications Board. Publications and films can be classified as XX.

---

491 Act 65 of 1996. Act 3 of 2009 will expand this to the classification of games. Games are defined as meaning a computer game, video game or other interactive computer software for interactive game playing, where the results achieved at various stages of the game are determined in response to the decisions, inputs and direct involvement of the game player or players. s1 of Act 3 of 2009.

492 S2 of Act 65 of 1996.

493 S1, provides a wide definition for publication, which includes any message, communication or visual presentation placed on any distributed network including, but not limited to the Internet. Visual presentation is defined as any drawing, picture, illustration, painting, photograph, image or combination thereof; including those produced through or by means of computer software on a screen or computer printout. Film is defined as any sequence of visual images recorded onto any substance, whether film, magnetic tape, disc or any other material in such a manner that by using such substance such images will be capable of being seen as a moving picture. These definitions are wide enough to include content on the Internet. S1 of Act 3 of 2009 will amend the definition of film to mean any sequence of visual images recorded in such a manner that by using such recording such images will be capable of being seen as a moving picture, and includes any picture intended for exhibition through any medium or device.

494 S16 of Act 65 of 1996 in relation to publications and S18 in relation to films. S16 will be substituted in terms of s19 of Act 3 of 2009. It will still allow for the classification of publications, but instead of by ‘complaint’ it will be on ‘request’. S18 will be amended by s21 of Act 3 of 2009, to include the classification of games.

495 S16 of Act 65 of 1996.

496 S18(1A)(b).

497 S18(1A).

498 S17. This section will be repealed by s20 of Act 3 of 2009. The s16 substituted by s19 of Act 3 of 2009 will regulate the classification of publications on request.

499 S18(4)(a) of Act 65 of 1996.

500 In terms of schedule 1(a) of Act 65 of 1996, if the publication contains visual presentations of explicit violent sexual conduct; bestiality, incest or rape; explicit sexual conduct which violates or shows disrespect for the right to human dignity or degrades a person and which constitutes incitement to cause harm; or the explicit infliction or effect of extreme violence which constitutes incitement to cause harm. Schedule 6 of Act 65 of 1996, applies the above provisions for the XX classification of films. These schedules are to be repealed by s37 of Act 3 of 2009. Publications will be classified as XX in terms of s16(4)(b) substituted by s19 of Act 3 of 2009. Films and games will be classified as XX in terms of s18(3)(b) as substituted by s21 of Act 3 of 2009. These amendments will cover similar depictions as is currently provided in terms of the schedules, although will specifically include depictions of domestic violence.
X18, age restrictions can be imposed or it may be deemed to be suitable for all ages. Publications or films that do not fall into these classifications can be freely distributed. It is an offence to knowingly distribute film in RSA which has not been submitted for classification by the Film and Publications Board.

4 3 2 Offences related to classified content

It is an offence to knowingly distribute XX and X18 publications or films. The XX and X18 classifications do not apply to publications or films that are bona fide scientific, documentary, dramatic or artistic in nature. However, this exemption does not apply to publications or films containing child pornography. The definition for child pornography is wide enough to include real, virtual and online child pornography. It is an offence to create,

---

501 In terms of schedule 2 of Act 65 of 1996, if the publication is a simulated or real visual depiction of explicit sexual conduct, including an explicit depiction of the genitals. Schedule 7 of Act 65 of 1996 contains the similar provision for the X18 classification of films. S37 of Act 3 of 2009 repeals the schedules. Publications with such depictions will be classified as X18 in terms of S16(4)(c), as substituted by s19 of Act 3 of 2009. Films and games with such depictions will be classified as X18 in terms of s18(3)(c), as substituted by s21 of Act 3 of 2009.

502 In terms of schedule 3 of Act 65 of 1996, if the publication constitutes material that is harmful or disturbing to children then an age limit of up to 18 years can be placed on the publication with a notice of that age restriction appearing on the publication. Schedule 7 of Act 65 of 1996 contains the similar provision for films. In terms of s19 of Act 3 of 2009, publications will receive age restrictions in terms of the substituted s16(4)(d). For films and games it will be in terms of the substituted s18(3)(d).

503 In relation to films. S17of Act 65 of 1996.

504 S26(1) of Act 65 of 1996. In terms of S30(1) of Act 65 of 1996, a person may be sentenced to a fine, imprisonment of up to 5 years, or if aggravating circumstances exist, both. Distribute is defined by the FPA, without derogating from the ordinary meaning, includes sell, hire out or offer to keep for sale or hire and in terms of s25(a)-(c), s26(a)-(b) and s28(1)-(2) includes to hand or exhibit a film or a publication to a minor and also fail to take reasonable steps to prevent a minors access thereto. S26 will be repealed by s30 of Act 3 of 2009. The offence will be in terms of s24A(2)(a) inserted by s29 of Act 3 of 2009 and will relate to films, games and publications that have been classified by request.

505 S25 and s26 of Act 65 of 1996 in relation to publications and films respectively. These sections will be repealed by s30 of Act 3 of 2009. These offences will now be contained in terms of s24A inserted by s29 of Act 3 2009.

506 Schedule 5 and Schedule 9 of Act 65 of 1996 for publications and films respectively. As the schedules will be repealed, these offences will be in terms of the substituted s16(4)(b)-(c) and s18(3)(b)-(c) of Act 3 of 2009.

507 Child pornography is defined in s1 of Act 65 of 1996 as any real or simulated image or description, however created, depicting or describing a person who is or who is appears as being under the age of 18 years; engaged, participating or assisting another person to participate in sexual conduct; or displaying, describing the body or parts thereof which amounts to or can be used for sexual exploitation. In terms of the substituted s16(4)(a) and s18(3)(a) a new classification called ‘refused classifications’ will be created for child pornography and for hate speech. It will be an offence to knowingly distribute refused classifications in terms of s24A(2)(b).

produce, import, export, distribute or possesses a publication or film which contains child pornography. Fault is required for the commission of these offences. Failure to report to the police ones knowledge or suspicion that any of these offences have been committed is an offence. Buys suggests that a person cannot be liable for merely viewing the content on a browser as they are not downloading it onto their computer. It is submitted that this is incorrect, if the user views the content voluntarily. A temporary copy is cached on the computer, therefore constituting possession. Further, the act of viewing the image on the computer screen constitutes creation.

433 Duties imposed on ISP's

It is compulsory for entities that fall under the Acts definition of ‘Internet Service Provider’ to register with the Films and Publications Board. It was suggested in Chapter Two that this appears to be a definition for IAP’s, which are a type of ISP. Where the FPA refers to

509 S27(1) of Act 65 of 1996. In terms of s30(1A) of Act 65 of 1996, a person who is found guilty of this offence can be fined or imprisoned for a period not exceeding ten years or to both a fine and imprisonment. S27(1) will be repealed by s30 of Act 3 of 2009. However, these offences will exist in relation to publications, films and games in terms of s24B, inserted by s29 of Act 3 of 2009.

510 The Internet Service Provider Association (ISPA) noted with concern that some of the offences did not expressly state that knowledge was required, yet other offences in the same section did. It appeared that the FPA created strict liability for certain offences. Massel & Molosiwa ISPA Submissions on the Film and Publications Act Amendment Bill (2003) www.ispa.org.za/regcom/submissions/ispa-sub-films-pub-amendment-bill.doc 5 (accessed on 2nd June 2009) and subsequently Massel & Molosiwa ISPA Submissions. However, in De Reuck v Director of Public Prosecutions 2004 (1) SA 406 (CC) 439 the Constitutional Court held that a determination of whether a person is committing an offence in relation to child pornography, in terms of the FPA, would involve an examination of lawfulness, mens rea (i.e. fault), justification, necessity and the constitutional concept of a fair trial.

511 S27(2) of Act 65 of 1996. A person found guilty of this offence can be fine or imprisoned for a period not exceeding five years or to both a fine and imprisonment.

512 Nel “Freedom of expression” in Cyberlaw 218.

513 Possession is defined in s1 of Act 65 of 1996, in relation to a film or publication, without derogating from its ordinary meaning, includes keeping or storing in or on a computer or computer system or computer data storage medium and also having custody, control or supervision on behalf of another person.

514 As was held in the UK case R v Smith and Jayson (2002) EWCA Crim 683. The court held that the voluntary viewing of the image constitutes its creation on the computer screen. Therefore, a user who voluntarily views child pornography will be liable even if they do not download the material onto their computer.

515 S27A(1)(a) of Act 65 of 1996. The ISP must register on the prescribed form contained in the regulations in GG 28 535 2006-02-20. See 732 on page 25 in Chapter 2 for the definition provided by the FPA.

516 See 56 on page 20 and 6 on pages 20-22 in Chapter 2 for a discussion on IAP’s and how they are a type of ISP.
specific obligations imposed on ‘Internet Service Providers’, the author will refer to them as IAP’s to differentiate between the Act and the broad meaning of ISP’s utilised in this dissertation.

The FPA provides that IAP’s have a duty to take all reasonable steps to prevent their services being used for hosting or distributing child pornography. 517 Should an IAP become aware that its services are being utilized for child pornography, it is required to perform particular duties. 518 Section 30(1) provides that an IAP which fails in any of these duties can be fined or the responsible parties imprisoned for five years or both. 519 In terms of the Act, the IAP can also be fined by the Films and Publications Board for a contravention of section 27(A), therefore saving them from a conviction or prosecution. 520

The Film and Publications Amendment Act 3 of 2009 will impose certain duties on child oriented services. 521 Failure to comply with these duties will be an offence and the person can be fined or imprisoned for a period not exceeding six months or both. 522

---

517 S27A(1)(b) of Act 65 of 1996. In terms of S30(1) of Act 65 of 1996, an ISP that fails to comply will be guilty of an offence and may be sentenced to a fine or to imprisonment for a period not exceeding 5 years or both.

518 S27A of Act 65 of 1996. An ISP who has knowledge that its services are being utilized to host or distribute child pornography: must take all reasonable steps to prevent access to the pornography; report its presence to the police as well as the particulars of anyone connected to that internet address; take all reasonable steps to preserve all evidence for possible investigation and prosecution; upon request by the police furnish them with the particulars of all users who gained or attempted to gain access to the pornography. Internet address is defined by s1, as any website, bulletin board service, an Internet chat room or newsgroup or any other Internet or shared network protocol address.

519 S30(1) of Act 65 of 1996 will be repealed by s33 of Act 3 of 2009. S31 of Act 3 of 2009 will insert s27A(4). In terms of this section, ISP’s that fail to register with the Board or who do not take reasonable steps will be guilty of an offence and can be fined or sentenced to imprisonment for a period not exceeding 6 months or both. ISP’s that fail to comply with their reporting duties or fail to provide information to the SAPS on request will be guilty of an offence. The responsible person will face a fine or imprisonment for a period not exceeding 5 years or both.

520 S30(4)(c) of Act 65 of 1996.

521 S29 of Act 3 of 2009 will insert s24C into Act 65 of 1996. Child orientated service will be defined, in terms of 24C(1)(a) as a contact service and includes a “content service which is specifically targeted at children.” Contact services will be defined in terms of 24C(1)(b) as a service “intended to enable people previously unacquainted with each other to make initial contact and to communicate with each other”. Content services will be defined in terms of s24C(1)(c) as a service providing content; or exercising editorial control over content transmitted over a communications network, as defined in the Electronic Communications Act 35 of 2005, to the public or sections thereof.

522 Some of the duties are: moderating and monitoring their services to ensure that they were not being used by predators; prominently display Internet safety messages on their web pages, in a language that will be clearly understood by children; providing mechanisms to enable children to report suspicious behaviour in a chat-room to the provider; ISP’s having to report details of suspicious on-line behaviour towards any child to the relevant authorities; and make filtering software available, along with information on the installation and use of such software, to all their subscribers that would block children’s access to pornographic websites. This will be in terms of 24C(2)(a)-(e). The offence will be created by s24C(1)(3) as contained in s29 of Act 3 of 2009.
4 3 4 Criticisms of the Film and Publications Act

There are a number of criticisms that can be leveled at the FPA:

- It is an offence to distribute films that have not been classified.523 The Internet Service Provider Association (ISPA) raises the concern that the effect of this is that ISP’s that host automated mirrored download websites are required to ensure that any films that are on the website are classified.524 It therefore follows that ISP’s that are aware that the users of their services are utilizing their networks to distribute films,525 must ensure that the films have been classified. This would amount to an onerous and potentially expensive monitoring obligation for ISP’s. It may further raise the question as to under which circumstances an ISP would have to register as a distributor.526

- Van Zyl states that the definition of publication is wide enough to cover any content that exists on the Internet, including film.527 It is submitted that this may not be the case in relation to film available on the Internet. It appears that the definition of ‘publication’ merely covers still images, whereas the definition of film covers moving images.528 Should online film be defined as ‘film’ for purposes of the FPA, the effect would be that films made by private persons and placed on social networking websites would have to be classified as they have been placed into the public domain. ISPA notes that online multi-media content could be considered either a film or a

---

523 S26(1) of Act 65 of 1996. In terms of S30(1) of Act 65 of 1996, a person may be sentenced to a fine, imprisonment of up to 5 years, or if aggravating circumstances exist, both. See n504 supra for the definition of distribute provided by the FPA. The ordinary meaning of the word as provided in Makins (ed) **Collins Concise Dictionary of the English Language** 3 ed (1998) 375, is to give out in shares; to hand out or deliver; to spread throughout an area. S26 will be repealed by s30 of Act 3 of 2009. The offence will be in terms of s24A(2)(a) inserted by s29 of Act 3 of 2009 and will relate to films, games and publications that have been classified by request.


525 For example: Their users may host a website where movies can be downloaded.

526 All persons who intend to distribute films must register as a distributor. S18(1A)(a) of Act 65 of 1996. South African versions of You Tube would then potentially be affected by this.

527 Van Zyl 2008 **THRHR** 229.

528 The definition of publication includes “any presentation or communication, including a visual presentation” placed on the Internet. The definition for visual presentation includes “drawing, picture, illustration, painting, photograph or image or any combination thereof”. The definition for ‘film’ is any sequence of visual images recorded on any substance and in such a manner that by using such substance such images will be capable of being seen as a moving picture. S1 of Act 65 of 1996.
publication. This creates uncertainty in relation as to what duties must be performed in relation to Internet content.

- ISPA argues that the problem of child pornography will not be solved by bringing IAP’s under the jurisdiction of the Act as IAP’s do not produce, distribute or offer child pornography. The FPA seeks to regulate content, therefore responsibilities should be placed on content providers and not IAP’s.

- IAP’s are required to report to the police the particulars of anyone associated with an Internet address where child pornography is found. ISPA points out that the definition of ‘Internet Address’ is very wide and includes chat rooms. ISPA has conducted research showing that many chat rooms are not controlled by IAP’s. ISPA has raised the concern that IAP’s therefore do not have access to that information, yet could be guilty of an offence by failing to provide it. IAP’s are therefore required to perform tasks that they are not capable of.

- The Act imposes the duty on IAP’s to take all reasonable steps to prevent their services being used for hosting or distributing child pornography. However, it is not clear what constitutes reasonable steps, Van Zyl is of the view that ordinary delictual principles should be applied to make this determination. Despite this, the author is of the opinion that a certain degree of uncertainty still exists, therefore potentially exposing IAP’s to criminal liability for failing to perform this duty.

There are at least two different technical options that exist to restrict content: content blocking and content filtering. Several different variants in respect of each of these technical options exist.

---

529 ISPA Amendment Bill Presentation 14.
530 Massel & Molosiwa ISPA Submissions 4.
531 ISPA Amendment Bill Presentation 10.
532 S27(A)(2)(b) of Act 65 of 1996.
533 Massel & Molosiwa ISPA Submissions 3-4. ‘Internet Address’ is defined at s1 of the Act 65 of 1996, as any website, bulletin board service, an Internet chat room or newsgroup or any other Internet or shared network protocol address.
534 Massel & Molosiwa ISPA Submissions 3-4.
535 S27A (1)(b) of Act 65 of 1996.
536 Van Zyl 2008 THRHR 233.
537 Ibid.
538 S30(1) of Act 65 of 1996.
539 Content blocking is the ‘absolute denial’ of the content associated with a blocked URL or IP address to an end user. Content filtering allows unrestricted material to be transmitted to the end user and stops restricted material. Esselaar What ISP’s can do about Undesirable Content (2008)
Each option has substantial weaknesses,\(^{541}\) are costly to implement and reduce Internet speed.\(^{542}\) It is therefore not clear what amounts to reasonable steps, especially as the definition of IAP includes entities ranging from small Internet Cafes to large commercial entities.

A recent Films and Publications Board survey recommended that IAP’s should install filtering software. It further recommended that IAP’s provide adult users with the option of requesting unfiltered access through reliable age verification and password systems,\(^{543}\) also known as an opt-in/opt-out system. This provides some indication as to what may be considered to be reasonable. However, both of these recommendations have their flaws.\(^{544}\) The cost of these steps and the resources


540 In relation to content blocking, there are three: URL based restrictions, this method blocks content from an established list of URL’s; IP address restrictions, this method blocks content from an established list of IP addresses; Domain name system (DNS) blocklisting, this method stops the DNS from providing the correct host IP address, directing the user to another IP address. Esselaar What ISP’s can do 13. See 3 1 on pages 11-12 and 4 1 on pages 13-15 in Chapter 2 for a discussion on URL’s, IP addresses and DNS. Content filtering has different variants in the form of proprietary software which is not available to the general public. Each variant differs greatly in terms of resource use, cost and effectiveness. Esselaar What ISP’s can do 18.

541 For example: A list of blocked sites actually informs persons who wish to access unlawful content as to the location of such content; a list of blocked sites can be circumvented through the use of easily available online technology; websites cannot be blocked or filtered if they are encrypted, encryption is easy and cheap; the greater amount of websites blocked increases the chances of the accidental blocking of websites that are not carrying unlawful content. Esselaar What ISP’s can do 17-18. There is also the effect on the freedom of speech. Legislation in Pennsylvania empowered the Attorney General or district attorney to bring an ex parte application to designate web pages, by their URL’s, as providing access to child pornography. Once the order had been granted, ISP’s had to remove the content or face criminal sanctions. The effect was that due to commercial and technical practicalities, ISP’s disabled access to approximately 1.19 million innocent websites. The legislation was found to be unconstitutional in Center for Democracy & Technology v Pappert 337 F Supp 2d 606 (ED Pa 2004).

542 There are costs for creating a list, maintaining the list, dealing with complaints, hardware and software. Esselaar What ISP’s can do 18-19. In relation to reduction in speed, ISP’s have reported reductions in speed of up to 78% depending on the filtering software and content type. Esselaar What ISP’s can do 20.

543 Chetty & Basson Report on Internet usage 57.

544 See n542 supra for the weaknesses and negative effects of filtering software. In relation to opt-in/opt-out systems, they would require ISP’s to: have additional resources to handle requests; verification software to prevent unauthorised access to blocked content; technical difficulties in routing data for filtered and unfiltered addresses; cost and maintenance of such a routing system. Esselaar What ISP’s can do 14.
required is of a particular problem for small, under-resourced or emerging IAP’s.\(^{545}\) This potentially threatens Internet development. The FPA has placed a large burden on IAP’s.\(^{546}\) It is submitted that the duty has been imposed on the wrong entity, and should have been potentially place on ISP’s performing the function of host. It should be pointed out that more unlawful content, such as child pornography, is being transmitted over encrypted person to person networks than on the WWW.\(^{547}\)

- The criticisms expressed \textit{supra} also show that the technology of the Internet was not properly taken into account during the drafting of the FPA.

- ISPA raised the points that certain terms are not defined at all, creating uncertainty;\(^{548}\)

- ISPA argues that the FPA creates unnecessary multiple registration requirements for IAP’s;\(^{549}\)

It is submitted that the FPA fails to fully take the technology of the Internet into account, creating uncertainty and requires ISP’s to perform tasks that they are not capable of. The effect is that it does not promote Internet development and potentially results in the FPA failing to meet its objective of protecting children. This in turn conflicts with the objects of the ECTA, in particular: preventing barriers developing in the use of the Internet; promoting legal certainty; promoting investment and innovation of the Internet; and assisting in creating a safe, secure and effective environment for all users.\(^{550}\)

\(^{545}\) The cost of an Irish ISP to deploy a filtering system for its 560 000 subscribers was an estimated €3.3 million a year. McIntyre “Filter or else! Music industry sues Irish ISP” \textit{SCL.com} (03-04-2008) http://www.scl.org/site.aspx?i=ed1049 (accessed 19-10-2009) subsequently McIntyre \textit{SCL.com} (03-04-2008).

\(^{546}\) Watney 2006 \textit{THRHR} 385.

\(^{547}\) Edwards “Pornography” in \textit{Law and the Internet} 665.

\(^{548}\) Examples of terms that are not defined are “creates”, “in any way contributes to”, “imports”, or “obtain or access” in s27 of Act 65 of 1996. Massel & Molosiwa \textit{ISPA Submissions} 5.

\(^{549}\) In relation to multiple registration requirements, the ISPA is referring to the fact that IAP’s have to register with two different bodies in terms of two different acts thus creating a potential burden for small IAP’s. Massel & Molosiwa \textit{ISPA Submissions} 6-7. IAP’s are required to register with ICASA in terms of s5 of the Electronic Communications Act 36 of 2005.

\(^{550}\) S2(1)(d)-(e), (i)-(j) of Act No. 25 of 2002 respectively.
4 3 5 Recommendations in relation to the Films and Publications Act

It is recommended that the FPA be amended in the following manner:

- the term ‘Internet Service Provider’ should be amended to Internet Access Provider (IAP) to avoid confusion;
- exclude IAP’s from the classification requirements for films, should such a duty exist;
- exclude automated mirrors for moderated international download sites from the classification requirements for films;
- amend the reporting requirements for child pornography to better reflect information that IAP’s can provide;
- remove multiple registration requirements for IAP’s that fall underneath the Electronic Communications Act and the FPA;
- clarity as to whether multimedia content is a film or a publication.

It is further recommended that the Films and Publications Board indicate what steps are considered reasonable for IAP’s to take to prevent their networks being utilised for child pornography. It should be further established exactly what ISP’s responsibilities are in relation to the classification requirements for online content and any registration requirements. Clarity should also be provided as to the extent of ISP responsibility for the distribution and classification of films.

4 3 6 Suggestions as to the extent of ISP liability for obscenity and indecency in South Africa

The FPA contains a number of offences that could be committed by ISP’s, however only if it has knowledge of the unlawful nature of the content it transmits or hosts. IAP’s are required to take all reasonable steps to prevent their services being used for hosting or distributing child pornography. They are further required to perform certain duties should they become aware that their services are being used for offences related to child pornography. There are strict penalties imposed on IAP’s which fail to perform these duties.
5 Conclusion

ISP’s that are not protected by Chapter XI of the ECTA face uncertainty as to the extent that they are liable for third party unlawful content in RSA law.

In relation to defamatory content, ISP liability should be determined by its relationship to the defamatory content. It is apparent that courts have at times struggled to ascertain the nature of this relationship. This appears to be a result of a failure by the courts to fully understand the technology of the Internet. This failure can lead to an ISP being erroneously found liable.

It has been submitted that the Equality Act imposes a duty on all ISP’s to monitor their content in order to ensure that they do not disseminate hate speech or speech that unfairly discriminates against another person. This is a potentially onerous burden and appears to be contrary to USA and UK law where ISP’s have been increasingly afforded greater protection from liability. It further has the potential to negatively effect the growth and development of the Internet.

It has been argued that the FPA does not take the technology of the Internet fully into account, creates uncertainty and imposes unreasonable burdens on ISP’s. The effect is that the Act may not be able to meet its objectives and may not promote Internet development. The Act may therefore conflict with certain objectives of the ECTA.

For ISP liability to be correctly determined by the RSA courts, the technology of the Internet must be properly considered. Cognizance must be had of the important role that ISP’s play in the free flow of information and the regulation of the unlawful Internet content. The courts decisions should also promote the objectives of the ECTA.
CHAPTER FOUR: REQUIREMENTS TO OBTAIN LIMITED LIABILITY IN TERMS OF THE ECTA

1 Introduction

Various jurisdictions found that the law threatened the continued existence of ISP’s and the effective functioning of the Internet by exposing ISP’s to an unreasonable risk of potential criminal and civil liability. The RSA legislature addressed this threat in Chapter XI of the ECTA. The legislature’s approach was to emphasise self regulation of the Internet by the Internet industry and the provision of safe harbours from liability to providers of ‘information system services’. The safe harbours are only available to providers that meet certain threshold requirements, which are related to membership of an IRB recognized by the Minister of Communications. An IRB must comply with certain requirements to obtain recognition. This chapter will examine both sets of requirements and their relevance.

2 Conditions for eligibility

The provisions of Chapter XI only apply to persons who provide ‘information system services’, which ISP’s do. However, to obtain the protection of Chapter XI, ISP’s must comply with two threshold requirements. The ISP must:

- be a member of an IRB that has been recognized by the Minister of Communications;
- have adopted the IRB’s code of conduct and implemented its provisions;

Once an ISP has complied with these requirements, it may make use of the safe harbours if it:

- performs certain functions in a particular manner in relation to the unlawful material;
- has responded in a reasonable time to a legitimate take-down notice.

552 GG 29474 7.
553 GG 29474 6-7; Roos “Freedom of expression” in ICT Law 429-434; Nel “Freedom of expression” in Cyberlaw 205-207.
555 See 7 4 on pages 25-26 in Chapter 2.
557 S72(a) of Act 25 of 2002.
558 S72(b).
559 Ss73-76. These are the mere conduit, cache, host or information location tool functions. These will be discussed in Chapter 5.
Unlike in USA and UK law, the threshold requirements Chapter XI’s make the IRB an integral element in the limitation of an ISP’s liability. An examination of the legislative requirements which an IRB must comply with to be recognized by the minister becomes relevant. This recognition process arises from a duty placed on the Department of Communications (the Department) by the ECTA, which is to ensure that IRB’s establish an acceptable minimum level of professional conduct for their members to qualify for limited liability. The requirements for recognition are broadly outlined in Section 71 of the ECTA. The minister must be satisfied that: an IRB’s members are subject to a code of conduct; adequate membership criteria exist; the code of conduct requires continued adherence to adequate standards of conduct; and that the IRB is able to adequately monitor and enforce its code of conduct. These requirements therefore appear to have an affect on the ISP’s threshold requirements. The ECTA does not provide the necessary detail for an IRB’s successful application for recognition. This is provided by a schedule to the ECTA, entitled ‘Guidelines for recognition of Industry Representative Bodies of Information System Service Providers’ (Guidelines).

3 Guidelines for the recognition of Industry Representative Bodies

The Guidelines were published on 14th December 2006. The Guidelines include the following: a description of the ECTA’s background; the Guidelines founding principles; its objective and scope; a Best Practice Code of Conduct that contains minimum and preferred standards of conduct by an IRB’s members; a checklist of the adequate criteria

560 S77 of Act 25 of 2002. This will be discussed in Chapter 6. This requirement does not apply to mere conduits. S73 of Act 25 of 2002.
562 This is the interpretation provided by the Department in GG 29474 9.
564 S71(2)(b).
565 S71(2)(c).
566 S71(2)(d).
567 ISPA was unable to successfully apply for recognition due to this. Brooks “Question 2” in Re: Questions for the committee in relation to recognition of an IRB (26-10-2009) E-Mail to N.D. O’Brien (copy on file with author), subsequently Brooks Re: Questions for the committee. Mr. Brooks is ISPA’s General Manager.
568 GN 1283 GG 29474. They were therefore published approximately four years after the ECTA.
569 6-7.
570 8-9.
571 10-11.
572 11-22. The Guidelines assist IRB’s in complying with s71(2)(a) of Act 25 of 2002 and s71(2)(c) as the Best Practice Code of Conduct indicates what the minister considers adequate compliance.
necessary for membership; and the considerations the minister is to take into account when determining whether an IRB is capable of adequately monitoring and enforcing its own code of conduct. They are important as they provide IRB’s with the necessary detail of the minimum standards required for recognition by the minister. They further provide standards of conduct that an IRB’s members should strive for.

3.1 Principles upon which the Guidelines are based

The Guidelines are based on a variety of principles and stress the legislature’s intention that the regulation of content and conduct on the Internet should be carried out by the industry as opposed to the state. There should be voluntary acceptance of this policy by the industry. The self regulation must be effective, using practical and realistic methods that respect and promote RSA’s constitutional values. It is not the intention of the legislature for ISP’s to assume the role of the law enforcement authorities and they therefore do not have a general obligation to monitor for illegal conduct or content. However, ISP’s cannot ignore illegal activities and are obliged to report such activities to the law enforcement authorities. Further, the requirements for recognition should be fair on ISP’s and not affect their economic viability. The requirements should promote equality and technological neutrality so that other entities can benefit from the ECTA, such as wireless access providers. The Guidelines contain a Best Practice Code of Conduct which reflects one of the aims of Chapter XI, viz to provide users with remedies against unlawful content.

The Best Practice Code of Conduct is discussed extensively at 3.3 infra.

3.2 Objective and scope

---

573 Therefore assisting IRB’s in complying with s71(2)(b) of Act 25 of 2002.
574 Therefore assisting IRB’s in complying with s71(2)(d) of Act 25 of 2002.
575 GG 29474 7.
576 GG 29474 8-9.
577 7-8.
578 8.
579 Ibid.
580 9.
581 Ibid.
582 8-9.
The Guidelines are applicable to all information system service providers, but were prepared for a specific category, namely ISP’s. If other categories of providers are unable to fully comply with the Guidelines due to technological differences, the IRB for that category of information system service providers must indicate to the minister how it will comply in a different manner.

One of the key aims of the Guidelines is to ensure that IRB’s and their members comply with the provisions of the ECTA before receiving the protection of Chapter XI. The Guidelines aim to assist in developing a safe, secure and efficient Internet for users and promote confidence in its use by: specifying and ensuring compliance with minimum standards of acceptable content and conduct; containing the preferred standards ISP’s should ultimately strive for based on the ECTA and international best practice; increasing the Internet's legality, integrity and safety; preventing its unlawful or offensive use; and ensuring affordable, quick, effective, fair, unbiased and transparent complaint and disciplinary procedures for the public.

3 3 Best practice code of conduct

Section 71(2)(a) of the ECTA provides that the minister may only recognize an IRB if he is satisfied that its members are subject to a code of conduct. The Guidelines provide a Best Practice Code of Conduct that contains both minimum and preferred requirements based on international best practice. The minimum requirements are mandatory for IRB’s to comply with to be recognized by the minister. The preferred requirements are optional and indicate the standards that the industry should strive to achieve. The requirements set the standards by which an ISP must interact with the public, recipients of its services, other ISP’s, its IRB and the relevant law enforcement authorities. The code reflects the principles and aims of the Guidelines and covers sixteen different areas, each will be discussed more fully infra. The

---

583 See 7 3 1 on pages 24-25 in Chapter 2 for the definition of information system service providers.
584 GG 29474 10. The Guidelines provide the following example, a wireless application service provider (which appears not to be considered the same as an ISP) may not have a website to comply with the Guidelines informational requirements to provide a link to the IRB’s code of conduct. That provider can propose to comply by ending all its SMS messages with Code of Conduct>www.nameofirb.co.za.
585 GG 29474 10.
586 10-11.
587 8-9.
588 7-8.
discussion of each area will begin with the minimum mandatory requirements, followed by a
discussion on any preferred requirements that may applicable to that particular area.

- Professional Conduct:
  An IRB member is required to conduct itself in a professional and lawful manner at
all times.\(^589\) It must comply with all legal requirements and co-operate with authorities
when obliged to do so.

The preferred requirements do not expand on the above.\(^590\)

- Standard terms of agreement

Members of the IRB must have Standard Terms of Agreement accessible on their
websites containing all the terms relevant to the relationship with the recipients of its
services.\(^591\) The terms must include certain commitments and undertakings by the
recipients of the member’s services\(^592\) which must be accompanied by a right of the
member to remove content that it considers illegal or upon receipt of a take down
notice. The member must have the right to terminate a recipient’s services in the event
of non-compliance with these or other contractual obligations.\(^593\)

The preferred requirements provide that the terms should contain commitments by
recipients of the member’s services to: the consumer protection and privacy
provisions of the ECTA, if applicable;\(^594\) and to ensure that adequate systems will be
in place to regulate minors’ access to content.\(^595\)

\(^{589}\) It must conduct itself in this manner with the recipients of its services, the public, other ISP’s and its’ IRB.

\(^{590}\) GG 29474 12, 18.

\(^{591}\) The terms must be accessible by potential users prior to the conclusion of a service agreement. GG 29474 12.

\(^{592}\) They must commit to not: conducting themselves in an unlawful manner; knowingly creating, storing or
disseminating unlawful content. They are further required to make undertakings not to: knowingly infringe
the copyright or intellectual property rights of others; and send or promote the sending of spam. GG 29474
12.

\(^{593}\) 12.

\(^{594}\) The consumer protection provisions and the privacy provisions are contained in Chapter VII and Chapter
VIII of Act 25 of 2002 respectively.

\(^{595}\) GG 29474 18.
• Service levels
IRB members may only offer service levels that are feasible taking into account all practical considerations.\textsuperscript{596} Members are required to act professionally, fairly and reasonably in all dealings with consumers, businesses and other members.\textsuperscript{597}

The preferred requirements provide that members should commit themselves to providing the minimum service levels contained in the members Standard Terms and Conditions. However members should not be liable where performance to such a level is not possible due to circumstances beyond their control. The preferred requirements also deal with issues pertaining to registration and transfer of domain names.\textsuperscript{598}

• Content control
Where a member becomes aware of unlawful online activities by a recipient of its services, it is obliged to act by terminating the offending recipient’s services and reporting their activities to the relevant authorities within a reasonable time. Members may not engage in unlawful conduct or knowingly host or link unlawful content. Further, they must adhere to their IRB’s code of conduct, disciplinary procedure and decisions. Members shall keep a copy or record of all take down notices, and the material removed as result thereof, for a period of three years.\textsuperscript{599}

The preferred requirements provide that members should utilize an Acceptable Use Policy that binds all the recipients of its services and it should contain a commitment not to contravene the FPA. Members should further require their recipients to adopt and use a content classification system that indicates whether their content or services are educational, suitable for children or of an adult nature.\textsuperscript{600}

\textsuperscript{596} Such as the members technical capabilities and knowledge. GG 29474 13.
\textsuperscript{597} Ibid.
\textsuperscript{598} Such as, members who register domain names for users must inform them of the terms and conditions of use and restriction that apply. Members should also allow users to keep the registered domain name when they wish to transfer it to another ISP, plus the member should provide a redirection service for a reasonable period at a reasonable cost to that user. Members should take reasonable steps to respect and implement the caching directions or restrictions of their users. GG 29474 18-19.
\textsuperscript{599} However, if it is an offence to possess such material it must be delivered to the authorities. GG 29474 13.
\textsuperscript{600} 19.
- **Consumer protection**

  The minimum requirements require members to commit to honest and fair dealing. They must also comply with all applicable advertising standards and regulations.\(^{601}\)

  The preferred requirements provide that members must comply with the consumer protection provisions of Chapter VII of the ECTA. Members should act in an open, honest, fair and professional manner with their users, while providing them with full information of their services and products.\(^{602}\)

- **Privacy and confidentiality protection**

  The minimum requirements oblige members to respect the recipients of their services constitutional right to privacy of their personal information and communications.\(^{603}\)

  The preferred requirements oblige members, and where applicable their recipients, to comply with certain provisions of three separate pieces of legislation and provide users with certain information and protection.\(^{604}\)

---

\(^{601}\) 13-14.

\(^{602}\) The requirements are numerous and include members: not using illegal, offensive or deceptive advertising; not knowingly disseminating false information; not knowingly exploit the recipients of their services lack of knowledge; shall have a clear refund and exchange policy; shall provide prospective recipients with the full details of software licences; shall, when offering consultancy services, provide full details on the professional qualifications of the experts; shall give adequate notice of any possible change that will affect the service delivered; and contractually require recipients of their services to comply with Chapter VII of Act 25 of 2002 and the above-mentioned obligations where applicable. GG 29474 19-20.

\(^{603}\) The requirements state that members may not to deal in the recipients of their services personal information unless it is for that members own needs or they have the recipients prior written permission; members must respect the confidentiality of the recipients electronic communications; and shall not disclose a recipients confidential information unless required to do so by law or without the recipients prior written permission. GG 29474 14.

\(^{604}\) Members, and where necessary, the recipients of their services must: comply with the privacy provisions of Chapter VIII of Act 25 of 2002; comply with Chapter Two of the Regulation of Interception of Communications and Provision of Communications-related Information Act 70 of 2002; comply with Part Three, Chapter 4 and 5 of the Promotion of Access to Information Act 2 of 2002 (PAIA); to have their PAIA manuals available on their website; advise users on appropriate tools to protect their privacy; to take all reasonable precautions in the storage of confidential information. GG 29474 20.
- Copyright and intellectual property protection
  The minimum requirements contain an obligation by members to respect and not to knowingly infringe the intellectual property rights of others.\textsuperscript{605}

  The preferred requirements oblige members who provide web design services to ensure that copyright ownership is agreed on with the user before work is commenced.\textsuperscript{606}

- Spam protection
  Members shall not send or promote the sending of spam. They should further ensure that their networks are not utilized for this purpose. Members should provide a complaint facility for the public in relation to any spam originating on the members network. They should react in a reasonable time to complaints received.\textsuperscript{607}

  The preferred requirements require members to follow best industry practice in providing anti-spam software to their users.\textsuperscript{608}

- Protection of minors
  Members are required not to offer subscription services to minors without their legal guardian’s assistance and to take reasonable steps to ensure that unassisted minors cannot receive such services. Members must provide recipients of their services with information as to methods of regulating and monitoring minors’ Internet access.\textsuperscript{609}

  Members who provide services to corporate recipients do not have to take the above steps.

  The preferred requirements merely refer the reader to the content control requirements.\textsuperscript{610}

\textsuperscript{605} 14.
\textsuperscript{606} 21.
\textsuperscript{607} 14.
\textsuperscript{608} 21.
\textsuperscript{609} 14.
\textsuperscript{610} 21.

Such as content labeling systems and filtering software. GG 29474
• Cyber crime
Members must take all reasonable steps to prevent unauthorized access, interception or interference with data residing on its network or otherwise under its control.611

In terms of the preferred requirements, members should take all reasonable steps to prevent cybercrime, such as providing recipients of their services with information as to software and other measures to protect themselves.612

• Complaints procedure
The IRB must establish a complaints procedure for the use of the public.613 It must be published on the IRB’s website and all its members shall provide a link to it. All IRB members must commit to receiving, investigating and resolving complaints that were made in good faith and in terms of the procedure. Members must comply with the IRB’s decisions.614

The preferred requirements deal both with complaints procedure and take down notices, despite being dealt with separately in the minimum requirements. Members should provide recipients of their services and the public with a twenty-four hour complaints hotline to receive complaints, take-down notifications and reports of illegal activities.615

• Disciplinary procedure
The IRB should establish a disciplinary procedure for members who contravene the code of conduct. The IRB shall have the right to investigate any contravention, and members shall be obliged to co-operate with the IRB in the performance of its rights and duties in terms of the disciplinary procedure. Should the IRB find that the

611
15.

612 Further requirements include members taking all reasonable steps to ascertain and record the identity of the recipients of their services and retain these records; reporting any illegal or suspected illegal conduct or content to the relevant authorities; and providing a twenty-four hour point of contact to authorities. GG 29474 21.

613 The procedure must provide for a reasonable time to deal with complaints. If a complaint is not resolved timeously, the complaint should be directed to the IRB for resolution. The procedure should also allow for the direct referral to the IRB of complaints involving a member’s contravention of the IRB’s code of conduct. The IRB may then elect to refer it to the member in question. GG 29474 15.

614 Ibid.

615 21.
member has transgressed the IRB’s code of conduct, the IRB may take a variety of actions against that member. The IRB must store the records of all proceedings for a period of three years.

The preferred requirements do not expand further on the above.

- Monitoring and compliance
  Members must provide the IRB with a full report, within a reasonable time, of all steps taken as a result of receipt of a take down notice. Members must further provide the IRB with an annual statement confirming their compliance with the IRB’s code of conduct. The IRB can investigate a member’s compliance with the code of conduct and institute disciplinary hearings where necessary.

This heading is not provided for under the preferred requirements.

- Informational requirements
  The IRB must publish its code of conduct on its website and all its members must provide a link to it on their websites. Members are required to prominently display the IRB membership logo and provide full contact details to enable adequate identification on their websites.

The preferred requirements contain a commitment by members to educate the public on a wide array of internet issues.

---

616 The actions that the IRB may take are to order a take down of material in accordance with a take down notice; reprimand the member; temporarily suspend the member; expel the member; publish details of the transgressing member, the transgression and the action taken; and report illegal content to the relevant authorities. GG 29474 16.

617 16, 21.

618 16.

619 The details listed, although not limited to, registered name, electronic contact details, physical address and telephone and fax numbers. GG 29474 16.

620 Such as: providing information on different cybercrimes such as hacking and intellectual property infringement; to inform the public of available software to prevent and limit cybercrime, spam and access to unwanted content; members are also to provide information on establishing a website, its management and associated costs. GG 29474 21-22.
• Take down procedure
The IRB must establish a take down procedure that is applicable to all its members and complies with the relevant provisions of the ECTA. The IRB must publish the procedure on its website and all its members must provide a link to it. The procedure must allow for a reasonable time for dealing with a take down notice.

The preferred requirements are dealt with jointly under the heading of complaints and take-down procedures. 621

• Review and amendment
The IRB is entitled to review and amend its code of conduct at any time. Amendments must be reported to the minister. The amendments must be binding on all members.

This heading is not dealt with under the preferred requirements. 622

3 4 Adequate criteria for membership
The Guidelines assist IRB’s in complying with section 71(2)(b) of the ECTA, by providing a checklist of adequate criteria for membership. 623 The checklist requires all potential members of the IRB to comply with a list of minimum criteria within 30 days from date of their membership application. 624 The minimum criteria appear to be largely based on the minimum requirements outlined above. However, the checklist does differ in some respects to the minimum requirements. 625

621 17, 21.
622 17.
623 S72(2)(b) provides that membership to an IRB should be subject to adequate criteria.
624 GG 29474 23.
625 There are inconsistencies between the Best Practice Code of Conduct and the checklist. The checklist does not contain the heading of one of the areas covered under the Code of Conduct, namely “Take down Procedure”. However, the checklist creates a new heading, “Commitment to the Code of Conduct”. Under this new heading a requirement from another area is repeated, involving a member providing a link to the IRB’s complaints procedure (mentioned at 11.3 and 12.1 on page 25 of the Guidelines under separate headings in the checklist). The new heading contains requirements listed underneath at least five different headings in the minimum requirements section. The adequate criteria further leave out the obligation by the member to comply with the IRB decisions (minimum requirement 5.11.6 on page 15) as well as the obligation to provide their co-operation to the IRB in accordance with the disciplinary procedure (minimum requirement 5.12.3 on page 16).
3.5 Monitoring and enforcement of the IRB’s code of conduct

Section 71(2)(d) of the ECTA requires IRB’s to be able to monitor and enforce its code of conduct. When determining whether an IRB has complied with this section the minister must take into account the following aspects.\footnote{626 GG 29474 27-30.}

\begin{itemize}
\item Nature and independence
The minister must consider whether the IRB is appropriately structured and constituted. The minister must therefore consider: how representative the IRB is of the industry; its independence and bias; and whether it has a proper constitution making provision for a variety of aspects.\footnote{627 These aspects are: regular elections of a board that can act independently; sufficient staff to perform the IRB’s functions; a properly constituted and effective complaints committee; and an adequate membership application procedure that screens potential members to ensure they comply with the necessary requirements for membership. GG 29474 28.}

\item Complaints, disciplinary and take-down procedures
The IRB’s complaints, disciplinary and take down procedures will only be considered effective where there is wide spread knowledge of the code of conduct and the aforementioned procedures amongst the IRB’s members and the public.\footnote{628 This will rely on sufficient notice of the above information on the members websites. The IRB should require its members to display this information prominently and for this to be checked regularly by the IRB. GG 29474 28-29.} The procedures must be effective and binding.\footnote{629 A proper record of the full process from complaint stage right through to appeal stage must be kept. The IRB should be able to instigate investigations by itself. Decisions should be binding with adequately severe punishments for transgressors. GG 29474 28-29.}

\item Monitoring procedures
The minister should consider whether there is an effective monitoring and enforcement policy in place. The policy should include procedures for: regular compliance spot checks; initiating investigations or following up complaints; and checking compliance of conditions set down as result of complaints or disciplinary proceedings. It should also include annual compliance statements from members and compulsory reporting by members of take down notices.\footnote{630}
\end{itemize}
Reporting duties
To receive continued recognition, an IRB must report any changes to the IRB’s constitution, article of association and code of conduct to the minister. The minister must then evaluate whether the IRB is still eligible for recognition. The IRB must also provide an annual report by 28th February each year on the following: membership of the IRB; statistics on take down notices and complaints received; disciplinary proceedings against members; and any other information the minister may require.631

From the discussions on the IRB’s recognition requirements supra, it is obvious that the Guidelines provide the standards required for an ISP to comply with its threshold requirements. Section 72(b) of the ECTA provides that the ISP must adopt and apply the IRB’s Code of Conduct. The Guidelines indicate what is required of ISP’s to satisfy this requirement, such as: a commitment by prospective members of the IRB to adhere to the IRB’s Code of Conduct; and the submission by members of an annual statement confirming their compliance with the IRB’s Code of Conduct.

4 Internet Service Providers Association
ISPA is a non-profit industry representative body established in 1996 with a current membership of approximately 150 ISP’s.632 ISPA participated in the formulation of the ECTA and applied for recognition as an IRB shortly after the Act was promulgated. Its application was rejected as the Department did not have sufficient guidelines for an application for recognition.633 Due to pressure exerted by ISPA, a draft of the Guidelines was published by the Department approximately two years after the promulgation of the ECTA.634

631 29-30.
633 Brooks “Question 2” in Re: Questions for the committee.
ISPA made extensive submissions on the draft Guidelines,\textsuperscript{635} holding that they were wide ranging and unworkable as written.\textsuperscript{636} The Department was receptive to ISPA’s submissions in relation to the minimum guidelines, but appears to have largely ignored the submissions made in relation to the preferred requirements. ISPA second application, made after the Guidelines became a schedule to the Act, took approximately two years to complete.\textsuperscript{637} ISPA states that it has incurred great expense in complying with the Guidelines. One of its greatest expenses incurred was as a result of the development of a Code of Conduct Compliance Wizard to assist ISPA members in compliance with its code and enable ISPA to easily monitor compliance.\textsuperscript{638} ISPA was formally recognized by the minister on 22\textsuperscript{nd} May 2009.\textsuperscript{639} It is the first and currently only IRB to be recognized by the minister.\textsuperscript{640}

5 Comparison of the South African approach to the European Union

The USA and the EU are both global leaders in technological development and can provide examples of regulation for developing nations to examine when establishing their own regulatory frameworks.\textsuperscript{641} Both these jurisdictions emphasise self regulation of the Internet,\textsuperscript{642} which is an international trend.\textsuperscript{643} RSA is following this trend by emphasizing self regulation.\textsuperscript{644}

Since it appears that RSA has adopted similar liability limiting legislation as the EU,\textsuperscript{645} and that there is an emphasis in the Guidelines on international standards and best

\textsuperscript{635} GN 1954 Notice inviting comment on proposed Guidelines for recognition of Industry Representative Bodies in terms of Chapter XI of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002) GG26768.


\textsuperscript{637} Brooks “Question 4” and “Question 5” in Re: Questions for the committee.

\textsuperscript{638} Brooks “Question 6” in Re: Questions for the committee.

\textsuperscript{639} GN 588 Recognition of the Internet Service Provider’s Association as an industry representative body for internet service provider GG32252.

\textsuperscript{640} “ISPA gets Ministers recognition” IT Online (21-05-2009) http://www.it-online.co.za/content/view/945534/129/ (accessed on 28-07-2009).


\textsuperscript{643} Prins & Schellekens “Fighting untrustworthy Internet content: In search of regulatory scenarios” 2005 (10) Information Polity 129 132; Bonnici IT & Law Series 14; Price & Verhulst Self Regulation and the Internet (2005) 1. However see Engel “The role of the law in the governance of the Internet” 2006 International Review of Law, Comp & Tech 201 for a discussion on the role that law can still play in Internet regulation.

\textsuperscript{644} GG 29474 7.

\textsuperscript{645} Roos “Freedom of expression” in ICT Law 429.
practice, it is submitted that it is relevant to briefly examine the EU position for comparison purposes.

There are a number of regulatory models that can be utilized by governments, for example: command and control or self regulation. Each model has its strengths and weaknesses generally and in the context of the Internet. The argument is that no one method of regulation can be entirely effective for the Internet, necessitating in a blend of regulatory methods. The EU emphasizes co-regulation which is a compromise between self regulation and command and control, as being a more suitable form of regulation for the Internet. The EU considers the co-regulation approach to be more flexible, adaptable and effective than traditional government regulation and legislation. Further, it involves multiple stake holders, namely public authorities, industry and other interested parties. An EU commissioned report on self regulation of the Internet identified that co-regulation is a finely balanced concept as direct government involvement may result in the benefits of self regulation being lost.

---

646 Ibid.
647 Some methods are: 1) command and control or top-down governance, which is government regulation (May et al 2004 ICT Law 261; Engel 2006 International Review 203; Bonnici IT & Law Series 24; Price & Verhulst Self Regulation 1); 2) co-regulation, which involves the public authorities, industry and other interested parties in developing a regulatory framework (Programme in Comparative Media Law and Policy Self Regulation of Digital Media Converging on the Internet: Industry Codes of Conduct in Sectoral Analysis (2004) 9); 3) self-regulation, also termed soft law or bottom-up governance, refers to norms that are voluntarily developed, accepted and regulated by a particular community (Prins & Schellekens 2005 Information Polity 132; Cannataci & Bonnici “Can self regulation satisfy the transnational requisite of successful internet regulation?” 2003 (17) International Review of Law, Comp & Tech 51 54).
648 An example of a criticism of command and control regulation in the context of the Internet is that it takes to long to develop and therefore cannot keep pace with the rapid development of the Internet (Engel 2006 International Review 206). An example of a criticism of self regulation is that it is biased in favour of the industry by which the regime is created (Bonnici & de Vey Mestdagh “Right vision, wrong expectations: The European Union and self-regulation of harmful Internet content” 2005 (14) ICT 133 144).
649 Cannataci & Bonnici 2003 International Review 52; Bonnici IT & Law Series 15.
652 Self Regulation of Digital Media 9.
Co-regulation is emphasized in the EU Directive. Member states are required to encourage the drafting of codes of conduct by trade, professional and consumer associations so as to facilitate the proper implementation of the Directives provisions. The adoption of these codes should however be voluntary. Adhering to a particular code of conduct or IRB membership is therefore not required by an EU ISP in order to obtain limited liability. EU member states cannot add additional requirements that ISP’s must comply with in order to benefit from the protection. However, it was not the EU E-Commerce Directive that resulted in extensive drafting and implementation of codes of conduct, but rather an earlier EU Council Recommendation followed by the EU’s Safer Internet Plan which both focused on the development of a safer environment for Internet users with a particular focus on the protection of minors and human dignity.

---

654 Ibid.
655 Recital 49 and art 16 of Directive 2000/31/EC.
657 Recommendation 98/560/EC. Recommendations have no binding force, but can be utilized for interpreting national or Community legal measures. Mathijsen A Guide to European Law 29. Recommendation 98/560/EC was a direct result of the EU’s Commission of European Communities Green Paper on Protection of Minors and Human Dignity in Audiovisual and Information Services (COM (1996) 483 final).
In comparison, the RSA approach has been to create additional requirements that ISP’s must comply with to obtain limited liability. It appears that the RSA approach is a form of co-regulation, as it provides for regulation of the industry by an entity staffed by members of a non-government organization. Issues of ISP liability and ISP regulation are dealt with separately in the EU. RSA has combined these issues by making ISP regulation an element for limited liability.

6 Criticism of the threshold requirements

It is submitted that a number of criticisms can be leveled at the threshold requirements and the requirements for IRB recognition as they appear in Chapter XI of the ECTA and the Guidelines:

- Both sets of requirements are unnecessary in the context of limited liability
  The Department has a duty to ensure that only responsible ISP’s benefit from the protection of the ECTA. It is submitted that the necessity of such a duty is misguided and contrary to the logic of the safe harbour provisions. The purpose of sections 73-76 is to protect ISP’s from liability for performing their technical functions. An ISP will lose the protection of the ECTA where it does not perform its functions in a technical, passive and automatic manner, thus making the question of whether it is a responsible ISP redundant. It is submitted that this question would only be relevant had RSA adopted the USA approach. The effect of the creation of these extra requirements has been too unnecessarily expose ISP’s to liability for four years, during the drafting and recognition processes, and the waste of time, money and manpower of ISP’s, IRB’s and the Department.

---

660 In both the USA and the EU, ISP’s are granted immunity without having to be responsible ISP’s. See 47 USC § 230 (CDA), 17 USC § 512 (DMCA) and Directive 2000/31/EC.
661 GG 29474 6.
662 The safe harbours are discussed further in Chapter 5.
663 In other words, if RSA had granted ISP’s broad immunity. The negative effects of such legislation was noted in 2 1 8 on page 38 in Chapter 3. It is submitted that the question of responsible ISP’s would go towards limiting those effects.
The Guidelines do not promote self regulation

Unlike the EU, the Department has failed to find the fine balance required for a co-regulatory framework as it was established in the form of legislation. This results in a loss of the benefits of co-regulation and self regulation, in particular flexibility and speedy adaptability to change,\(^{664}\) as legislation is more cumbersome and expensive to change.\(^{665}\) Further, the Department is granted the power to consider nearly every aspect of an IRB from its formation and regulation to even its future aims. This would appear to be contrary to the principle of self regulation. It is submitted that with the extent of government control granted by the Guidelines, the industry is funding an entity that can potentially become an extension of the Department therefore the public authority. Despite the principle of self regulation contained in the ECTA and the Guidelines, the RSA approach may not promote self regulation in practice. Finally, the acceptance of the Guidelines by ISP’s cannot be considered to be entirely voluntary due to it being a requirement for obtaining limited liability. Therefore, it appears that the RSA position is not in keeping with international standards and is not ideal.

Lack of equality and technological neutrality

The definition for information service providers is wide and it has been established that an unwanted side effect may be limited liability being granted to entities that the legislature did not intend.\(^{666}\) The requirement of membership to an IRB is a way to limit that effect. This may however be to the detriment of non-commercial entities and other categories of information service system providers.

Non-commercial entities do not necessarily have the funds to defend legal actions or create IRB’s, whereas large commercial entities, which may have access to such funds, are more likely to form IRB’s and receive protection.\(^{667}\)

---


\(^{666}\) See \(^{7 4}\) on page 25 in Chapter 2.

\(^{667}\) It is positive to note that the ISPA management committee does bestow honorary ISPA membership on educational or non-profit entities. These members do not have to pay any fees. They however do not have any voting rights. Therefore, their interests will not be necessarily promoted. ISPA “ISPA Membership Basics” http://www.ispa.org.za/apply/index.shtml (accessed 18-07-2009).
would appear to limit the access to the safe harbours to largely commercial enterprises, to the potential detriment of non-commercial entities such as education institutions or possibly non-profit organizations.\textsuperscript{668} Should an IRB, established for commercial entities, be burdened with non-commercial entities, it may not effectively represent non-commercial entities interests as the IRB would be orientated to promoting commercial interests.

The Guidelines do not necessarily promote one of the objectives of the ECTA, which is to promote technological neutrality.\textsuperscript{669} The Guidelines were prepared specifically for ISP’s, which are only one category of Information System Service Providers. It is submitted that this places an extra barrier to the recognition of an IRB for another category of information system service providers and as a result unfairly prejudices them. It took approximately two years for an IRB, for which the Guidelines were specifically drafted, to be recognized by the minister. The author is of the opinion that it is possible that the recognition process for an IRB of another type of provider will take longer. It will have to spend more time and resources to determine how to comply with the Guidelines. Further, it will have to convince the minister that it is necessary to recognize another IRB and that it has complied with all the requirements. During this time, its members will not benefit from the same protection afforded to ISP’s. It is submitted that the current position favours a potential monopoly by one IRB which could ultimately have negative effects for the industry.\textsuperscript{670}

It is therefore submitted that the threshold requirements unfairly prejudice non-commercial entities and other categories of information service system providers by effectively creating a barrier to the protection afforded by the ECTA. The effect of this is a lack of equality and technological neutrality.

\textsuperscript{668} Such as university networks. This would be worrying due to the fact that the Internet developed due to the pioneering work of universities. See Engel 2006 International Review 205 for a brief description of the relevance of the universities in Internet development.

\textsuperscript{669} S2(1)(f) of Act 25 of 2002.

\textsuperscript{670} A worst case scenario would be that there would only be one recognized IRB as it would be difficult for another IRB to be recognized either because it has smaller membership than the recognized IRB or because its members deal with different technologies that make it difficult to comply with the Guidelines. This does not assist in promoting new technologies. It could also result in the industry being dominated by one group and technology.
Not in keeping with international best practice
It is apparent from the criticisms raised supra, that there are certain aspects of the threshold requirements that are not in keeping with international best practice:

- Membership of an IRB as a requirement for limited liability;
- The adoption of the policy and standards contained in the Guidelines by ISP’s is not truly voluntary;
- The Guidelines do not appear to promote self regulation;
- Lack of equality and technological neutrality.

Therefore, despite the Department’s insistence on international best practice and standards, it appears that they have failed to meet them.

The content of the Guidelines are in conflict with its principles
As the contents of the Guidelines appear not to promote self regulation, equality and technological neutrality, it appears that the content of the Guidelines conflict with its own principles and aims.

Guidelines are too broad
ISPA submits that the purpose of Chapter XI is to provide ISP’s immunity from third party content and not to regulate ISP’s business practices. It therefore contends that the Guidelines should deal with an ISP’s ability to implement and process take down notice procedures.671 However, the Guidelines deal with issues that are not connected to ISP liability for third party content.672 The Guidelines are therefore considered to be unnecessarily extensive to give effect to a five line section of the ECTA.673

---

671 ISPA ISPA submission on proposed Guidelines 1-2. The Electronic Communication and Transaction Bill B8-2002 had a Memorandum on the Objects of the Electronic Communications and Transaction Bill annexed thereto. S75-76 of the bill are ostensibly the same as s71-72 of the ECTA, yet it is interesting to note that the memorandum does not raise the duty that the Department has identified in the Guidelines.

672 Such as: professional conduct; standard terms and conditions; service levels; consumer protection; privacy and confidentiality protection; spam protection; and regulation of minors access to subscription services.

673 Brooks “Question 1” in Re: Questions for the committee.
ISPA nearly did not complete the recognition process as the Guidelines were too broad and difficult to comply with. The effect of the Guidelines in practice was that an IRB nearly considered obtaining limited liability for its members not to be worth the effort of compliance. This is despite the threat that civil and criminal liability posed to ISP’s, a threat which the ECTA was attempting to remove. However, ISPA changed its approach to focusing only on the minimum requirements and providing extensive explanations to the Department on areas that ISPA did not agree with.

- **Poor drafting**
  
  Despite the lengthy period that the Department took to produce the Guidelines there are a number of issues that indicate poor drafting such as:

  - Certain compulsory provisions of the ECTA are listed under the non-mandatory preferred requirements.
  - Lack of certain definitions and consistency in terms used;
  - Lack of consistency in layout between the minimum requirements and the adequate membership criteria.
  - Repetition of certain requirements;

---

674 Brooks “Question 9” in Re: Questions for the committee.
676 GG 29474 6.
677 Brooks “Question 9” in Re: Questions for the committee.
679 Under the minimum requirements Privacy and Confidentiality Protection section, the term ‘personal information’ is defined however the section also refers to “confidential information”, which is not defined. GG 29474 14. Further, the minimum requirements specifically refer to “recipients of services”, however the preferred requirements refer to the undefined terms of ‘user’ and ‘client’. These terms are used with ‘recipients of services’, even underneath the same section. See ‘Standard Terms of Agreement’ and ‘Service Levels’ GG 29474 18; ‘Copyright and Intellectual Property Protection’ sections under minimum requirements and preferred requirements GG 29474 14, 21 respectively.
680 For a discussion, see 3 4 supra. It is also noted that the requirement of an ISP’s commitment to co-operate with law enforcement is contained underneath the ‘Professional Conduct’ section of the minimum requirements, however it is found underneath ‘Content Control’ in the adequate criteria for membership section. GG 29474 12, 24 respectively.
681 For example, under the minimum requirements, acting in professional manner in dealings with all parties and entities is repeated under ‘Professional Conduct’ and ‘Service Levels’. GG 29474 12-13. Another example, under the adequate criteria for membership, the requirement to publish a complaints procedure is repeated under ‘Commitment to the Code of Conduct’ and ‘Complaints Procedure’
It is submitted that even though some of the above points may be minor, when the length of time of the development of the Guidelines is considered and the importance of industry, these errors should not have been made. These errors would further add to frustration in compliance.

- Disregard to the objectives of the ECTA

It is submitted that these requirements do not assist in promoting certain objectives of the ECTA. The current position demonstrates a failure by the RSA government to recognize the importance of the information economy. This is a reasonable inference due to: the length of time it took for the Department to develop largely unnecessary Guidelines and recognize an IRB, thus exposing ISP’s to liability for a lengthy period; the Guidelines appearing to favour one technology and only commercial entities; both sets of requirements create an extra barrier to ISP immunity that do not exist in other jurisdictions. The requirements do not place RSA in a favourable position to compete internationally. It is further submitted that the Department did not have a clear idea of how to effectively apply sections 71-72, due to: the length of time for development of the draft Guidelines; the numerous issues that were raised in relation to them by the ISPA; the length of time it took for the Guidelines to be passed into law; the poor drafting of the Guidelines; and the length of time for ISPA to be recognized.

The effect of the Guidelines in practice was for an IRB to consider not completing the recognition process. The Guidelines therefore appear to be in conflict with the primary purpose of Chapter XI of the ECTA, which is the provision of limited liability to ISP’s.

It is possible that other objectives of the ECTA are not promoted, such as not promoting investments or innovation in the Internet and therefore creating barriers to the use of the Internet.682

---

682 The threshold requirements do not promote large investment or innovation in the Internet as jurisdictions with a more favourable immunity regime would be seen as a better option. Therefore the regime potentially does not promote s2(1)(i). By failing to encourage investment or innovation results in a failure to promote the development of services that are responsive to the needs of users. Therefore the regime potentially does not promote s2(1)(k). A lack of investment, innovation and development of services that are responsive to the needs of users can result in a lack in the growth of the amount of electronic transactions in RSA. Therefore the regime potentially does not promote s2(1)(c). The regime does not promote the development of SMME’s. Such entities are forced to bear various costs that would not be necessary in other jurisdictions with a more favourable regime. Some of these costs they are forced to incur are: the cost of ensuring that
7 Recommendations

The need for EU member states to encourage the drafting of voluntary codes of conduct appears to be based on human rights issues and ensuring the protection of minors. In comparison, it appears the focus of the Guidelines is consumer protection. It is therefore recommended that that the Guidelines should be incorporated into consumer protection legislation, and that the requirements for IRB membership should not be required for access to the limited liability. Alternatively the requirements need to be rethought to be less of an unnecessary barrier to obtaining limited liability.

8 Conclusion

The RSA legislature and the Department have adopted a similar approach to ISP liability as exists in the EU, but have added extra requirements for ISP’s to meet in order to access the safe harbours created in Chapter XI of the ECTA. Of these extra requirements, membership of an IRB which has been recognized by the minister is an integral element. It can be gleaned from ISPA’s recognition process, that recognition from the minister is not easy to attain and is potentially costly in terms of time and money. It has been argued that both the threshold requirements and IRB recognition requirements are unnecessary in the context of limited liability. The Department has created needless barriers to limited liability that could possibly have a serious affect on the industry as a whole. As a result, the Department has failed to meet the objectives of the ECTA and the Guidelines. The overall effect is to indicate a failure on the part of government to recognize the importance of the Internet industry, potentially stifle investment and development in the Internet, and place RSA in an unfavourable position to compete internationally.

---

they comply with adequate membership criteria to an IRB; continued cost of compliance; and the IRB membership cost. Therefore the regime potentially does not promote s2(1)(p). Should the regime in fact result in the above, it would result in a failure to promote universal access, especially to primarily underserviced areas. Therefore the regime potentially does not promote s2(1)(b).

683 As illustrated under 5 supra.
CHAPTER FIVE: DEFENCES AVAILABLE TO ISP’S IN TERMS OF THE ECTA

1 Introduction
When an ISP has complied with the threshold requirements discussed supra, the ISP may utilise the defences contained in sections 73-76 of Chapter XI of the ECTA. In terms of these sections, ISP’s must perform particular functions in relation to third party content in a certain manner. These sections appear to be based on provisions of the USA’s DMCA and the EU Directive. The defences provided in terms of these statutory instruments will now be examined and compared.

2 A brief comparison of safe harbour legislation
It has been established that ISP’s are essential to the functioning of the Internet.684 They are however potentially liable for third party content through the performance of their basic functions as online intermediaries.685 The laws that exposed ISP’s to liability were developed for the physical world and were not easily applicable to the Internet.686 The extent and nature of ISP liability was therefore not always clear and differed depending on the function it performed, thereby creating uncertainty.687 There were also concerns in some jurisdictions that the judiciary did not possess sufficient knowledge of Internet technology, which added to ISP uncertainty.688 The high volume of transmissions over ISP’s networks exposed them to a great degree of potential liability and financial loss through large damage awards.689 The exposure to liability and uncertainty were considered a threat to the development of the Internet.690 It was therefore considered appropriate to grant ISP’s protection from the risk of liability arising from third party unlawful content.691

684 See Chapter 2.
686 Reed Internet Law 121.
687 Reed & Angel Computer Law 367; Reed Internet Law 114; Bunt v Tilley (2006) EWHC 407 (QB) 339.
690 Reed & Angel Computer Law 367; Zeran v America Online Inc 129 F 3d 327 (4th Cir 1997) 331; Recital 40 of Directive 2000/31/EC; GG 29474 6; Reed Internet Law 122; Edwards “The fall” in Law and the Internet 61.
691 Walden “Directive 2000/31/EC” in Concise European IT Law 248; Reed Internet Law 122; GG 29474 6; Edwards “The fall” in Law and the Internet 61.
Certain jurisdictions sought to provide this protection through the promulgation of legislation that provided them with safe harbours from liability for third party content. The safe harbours are defences based on particular basic functions performed by ISP’s. For an ISP to utilise any of these defences it must perform the function in a technical, automatic and passive manner. The limitation of liability is justified on the basis that the nature of these basic functions imply that the ISP neither has knowledge nor control over the third party content. Examples of safe harbour legislation from three different jurisdictions are:

- Digital Millennium Copyright Act
  The CDA does not provide ISP’s with immunity in matters dealing with intellectual property law. The application of USA intellectual property law to the determination of ISP secondary copyright liability for third party copyright infringement had largely resulted in unfavourable decisions for ISP’s and had further created uncertainty as to the extent of their liability. In response, the Copyright Act of 1976 was amended by Title II of the DMCA by inserting section 512. It provides for the limitation of ISP liability should the ISP perform the function of a mere conduit, cache, host, or information location tool in accordance with specific requirements. Section 512 also provides for the limitation of liability for non-profit educational institutions.

- EU Directive 2000/31/EC

---

694 47 USC § 230(e)(2).
695 House of Representatives WIPO Copyright treaties implementation and on-line copyright infringement liability limitation H Rep No 105-551 Part 1 (1998) 11; S Rep No 105-190 19; Weinstein 2008 Cardozo Art and Entertainment LJ 596; Fifer & Carter 2004 JIL 16. For examples of decisions unfavourable to ISP’s see Playboy Enterprises Inc v Frena 839 F Supp 1552 (MD Fla 1993) or Sega Enterprises Inc v MAPHIA 857 F Supp 679 (ND Cal 1994). However, for an example of a favourable decision see Religious Tech Ctr v Netcom On-Line Comm Servs Inc 907 F Supp1361 (ND Cal 1995). According to the House Report on the DMCA, the amendment sought to codify this decision and overrule the unfavourable decisions, see H Rep No 105-551 11.
696 Pub L No 94-553 90 Stat 2541.
697 17 USC § S512(e).
Differences between EU member states’ legislation and case law in relation to ISP liability were considered a threat to the smooth functioning of the EU internal market.\textsuperscript{699} The EU Parliament and Committee responded by harmonising member states’ law through provisions contained in the EU Directive.\textsuperscript{700} Articles 12-14 of the EU Directive provide for the limitation of ISP’s criminal and civil liability arising from third party content should an ISP perform the function of a mere conduit, cache or host in accordance with specific requirements.\textsuperscript{701}

- **ECTA**
  
  In response to the threat that the law posed to ISP’s and the future effective functioning of the Internet, specific provisions to protect ISP’s were included in the ECTA.\textsuperscript{702} Sections 73-76 of Chapter XI of the ECTA provide for the limitation of ISP’s civil and criminal liability arising from third party content should an ISP perform the function of a mere conduit or cache in accordance with specific requirements.\textsuperscript{703} The ECTA further limits the civil liability of an ISP that performs the function of a host or information location tool in accordance with specific requirements.\textsuperscript{704}

Upon perusal of the relevant provisions of the abovementioned legislation, one is able to glean certain common general principles, for example they:

- provide for the limitation of ISP liability;\textsuperscript{705}
- do not impose new liabilities on ISP’s or deprive them of defences available under other laws;\textsuperscript{706}

\textsuperscript{699} Recital 40 of Directive 2000/31/EC.
\textsuperscript{702} GG 29474 6.
\textsuperscript{703} Ss73-74 of Act 25 of 2002; Roos “Freedom of expression” in ICT Law 429, 431-433; Pistorius “Copyright law and IT” in ICT Law 289.
\textsuperscript{704} Ss 75-76 of Act 25 of 2002; Roos “Freedom of expression” in ICT Law 429, 431-433; Pistorius “Copyright law and IT” in ICT Law 289.
have the effect that should an ISP fall outside the protection of the particular statutory instrument, its liability must be determined through the normal application of law;\footnote{106}

do not provide broad immunity but rather limited liability based on certain clearly delimited functions performed by ISP’s;\footnote{108}

limited liability is based on the performance of these functions in a technical, passive and automatic manner;\footnote{109}

do not affect the liability of the primary publisher;\footnote{110}

prevent pecuniary damages being awarded against ISP’s. They do not prevent the granting of injunctive relief against ISP’s;\footnote{111}

provide for a take-down procedure;\footnote{112}

do not impose a general obligation on ISP’s to monitor for unlawful content or activities.\footnote{113}

The DMCA is the first of the three statutory instruments to have been promulgated and it is submitted that it can be considered as the progenitor legislation upon which it appears that the EU Directive and the ECTA are based. However, there are differences between the limitation of liability provisions of the DMCA and those of the other statutory instruments, such as:\footnote{114}

The DMCA only provides for the limitation of ISP liability arising from third party copyright infringement. This is an important distinction as the EU Directive and the

\footnote{106} 17 USC § 512(l); s79(d) of Act 25 of 2002; H Rep No 105-551 11; Smith \textit{Internet Law} 365; Weinstein 2008 \textit{Cardozo Art and Entertainment LJ} 598.


\footnote{109} Recital 42 of Directive 2000/31/EC; Roos “Freedom of expression” in \textit{ICT Law} 429. In relation to the DMCA, this is an observation made based on the content of the provisions of 17 USC § 512.


\footnote{111} 17 USC § 512(j); S Rept No 105-190 20; recital 45, art 12(3), art 13(3), art 14(3) of Directive 2000/31/EC; ss73(3), 74(2), 75(3), s79(c) of Act 25 of 2002; Pistorius “Copyright law and IT” \textit{ICT Law} 284; Smith \textit{Internet Law} 365; Hocking 2009 \textit{The Computer & Internet Lawyer} 13; Weinstein 2008 \textit{Cardozo Art and Entertainment LJ} 597; Van Eecke & Ooms 2007 \textit{JIL} 4.

\footnote{112} 17 USC § 512(c)(3); recital 40, art 16 of Directive 2000/31/EC; s77 of Act 25 of 2002.

\footnote{113} 17 USC § 512(m)(1); art 15 of Directive 2000/31/EC; s78 of Act 25 of 2002.

\footnote{114} Besides these differences, specific differences exist between the DMCA and the Directive, such as: the DMCA at 17 USC § 512(c)(3) provides for the elements of notification for the notice and take-down procedure, while recital 40 and art 16 of Directive 2000/31/EC provides that each member state must determine the elements and the procedure themselves; unlike the DMCA at 17 USC § 512(c)(3)(A), the Directive does not provide for the appointment of a third party to accept take-down notices; and the Directive does not provide protection to information location tools.
ECTA provide far wider protection for ISP’s by limiting an ISP’s civil and criminal liability arising from third party content;\textsuperscript{715}

- The DMCA provides for a counter-notification procedure. The purpose of this procedure is to provide an opportunity to the affected third party, whose content the ISP has removed, to notify the ISP to place the content back;\textsuperscript{716}

- The DMCA provides protection to non-profit educational institutions;\textsuperscript{717}

- The DMCA provides procedures where ISP’s are to disclose information concerning the author of the unlawful content to private persons. The EU Directive and the ECTA only provide for procedures to disclose such information to the state.\textsuperscript{718}

The ECTA appears to be extensively based on the EU Directive.\textsuperscript{719} However, there are also similarities between the ECTA and the DMCA,\textsuperscript{720} as both provide for:

- threshold requirements for ISP’s to comply with to utilise the defences;\textsuperscript{721}
- limited liability for information locations tools;\textsuperscript{722}
- the appointing of an agent to receive take-down notices;\textsuperscript{723}


\textsuperscript{716} 17 USC § 512(g).

\textsuperscript{717} 17 USC § 512(c). This section provides that under certain circumstances a non-profit educational institution will not be vicariously liable for the copyright infringements of its employees, whether they are staff or students.

\textsuperscript{718} 17 USC § 512(h); art 15(2) of Directive 2000/31/EC; s78(2) of Act 25 of 2002. Visser 2003 \textit{JBL} 44.

\textsuperscript{719} Roos “Freedom of expression” in \textit{ICT Law} 429; Pistorius \textit{LEAD: Cyberlaw} 70.

\textsuperscript{720} Pistorius \textit{LEAD: Cyberlaw} 70.

\textsuperscript{721} 17 USC § 512(i); s72 of Act 25 of 2002; Pistorius “Copyright law and IT” in \textit{ICT Law} 280; Weinstein \textit{Cardozo Art and Entertainment LJ} 2008 597; Brown 2008 \textit{Berk Tech LJ} 444. In terms of 17 USC § 512(i)(1)(A), the ISP must adopt, implement and inform the recipient of its services of the ISP’s policy of termination, in appropriate circumstances, of the recipients services should such recipient be a repeat infringer. Further, in terms of 17 USC § S512(i)(1)(B), the ISP must accommodate and not interfere with standard technical measures. The ECTA does differ in that its threshold requirements are more stringent and extensive than the DMCA. See Chapter 4 for a more detailed discussion of the ECTA’s threshold requirements.

\textsuperscript{722} 17 USC § 512(d); s76 of Act 25 of 2002.

\textsuperscript{723} 17 USC § 512(c)(2); s77(1) of Act 25 of 2002. In terms of the s75(2) of Act 25 of 2002, an ISP that performs the function of a host must appoint an agent to receive notices to avail itself of the host defence. However, the ECTA does differ from the DMCA in relation to its other defences in that the appointing of an agent is
• certain formal requirements for a take-down notice;\textsuperscript{724}
• a party to be liable for damages for a wrongful take-down,\textsuperscript{725}
• an exclusion of an ISP’s liability for the wrongful take-down of content in response to a notification.\textsuperscript{726}

3 The safe havens contained in the ECTA

With the similarities between the three different statutory instruments identified, it is appropriate to examine each of the safe havens provided for by the ECTA.\textsuperscript{727} Each section will begin with a brief description of the function in question, followed by a more detailed discussion of the relevant section in the ECTA and conclude with identifying any key similarities or differences with the appropriate provision of the foreign statutory instrument to which it is most closely related.

3.1 Mere Conduit

Mere conduits are a passive conduit for content, similar to telephone networks.\textsuperscript{728} The ECTA provides that a mere conduit is an ISP which provides access to or operates facilities for information systems or transmits, routes or stores data messages via an information system under its control.\textsuperscript{729} This function must be performed in an automatic and

\textsuperscript{724} The Directive provides for a take-down procedure. The elements or formal requirements of notification have been left to member states to develop. Recital 40 of Directive 2000/31/EC; art 16 of Directive 2000/31/EC; First Report on the application of Directive 2000/31/EC 14; Valcke & Dommering “Directive 2000/31/EC” in European Media Law 1104; Van Eecke & Ooms 2007 JIL 4. The wording of the provisions contained in the DMCA and the ECTA for the take-down notice procedure is similar. Further, both statutory instruments provide certain formal requirements for a take-down notice for the ISP that performs the functions of a cache (17 USC § 512(b)(2)(E); s74(1)(e) of Act 25 of 2002) and host (17 USC § 512(c)(3); s75(1)(c) of Act 25 of 2002). The ECTA differs as it does not provide for the take-down notice for information location tools, however the DMCA does at 17 USC § 512(d)(3).

\textsuperscript{725} 17 USC § 512(f); s77(2) of Act 25 of 2002.

\textsuperscript{726} Should that party knowingly lodge a take-down notice which misrepresents the facts. 17 USC § 512(g); s77(3) of Act 25 of 2002.

\textsuperscript{727} In the ECTA the third party content is referred to either as ‘data’ (defined at s1 of the ECTA as electronic representations of information in any form) or ‘data messages’ (defined as data generated, sent, received or stored by electronic means, including voice and a stored record). The EU Directive refers to a third parties content as ‘information’ which is not defined in the Directive, however the EU Commission stated that this term should be understood in a ‘broad sense’. Proposal for a European Parliament and Council Directive 27. Section 512 of the DMCA refers to third party content as ‘material’, this terms is not defined. However, the term ‘content’ will be used in the following discussion.

\textsuperscript{728} Smith Internet Law 371; Roos “Freedom of expression” in ICT Law 425, 430. Another analogy for mere conduits is the postal service which cannot be held liable for the content of a letter it delivers. Lodder “EU Directive” in Guide to EU Law 87. However, Smith contends that web based e-mail services which store information cannot be classified as mere conduits, a contention supported by Roos. Smith Internet Law 374; Roos “Freedom of expression” in ICT Law 425.

\textsuperscript{729} S73 of Act 25 of 2002.
technical manner, therefore the ISP should not: initiate the transmission;\(^{730}\) select the addressee;\(^{731}\) select the content;\(^{732}\) nor should it modify the content contained in the transmission.\(^{733}\) Further, the automatic, intermediate and transient storage of content must take place for the sole purpose of the transmission of the content.\(^{734}\) The storage must be in a manner that makes it accessible only to the intended recipients and it must be for a period no longer than is reasonably necessary for transmission.\(^{735}\) Should the mere conduit comply with these requirements it will not be liable for third party unlawful content.\(^{736}\)

ISP’s performing this function will “not be liable”,\(^{737}\) thereby indicating that this defence limits both civil and criminal liability.\(^{738}\) Lack of knowledge of unlawfulness is not a requirement of this defence. This suggests that knowledge of unlawfulness will not result in the loss of this safe harbour.\(^{739}\)

### 3.1.1 Comparison with the EU Directive

Both the EU Directive and the ECTA limit the civil and criminal liability for ISP’s which perform this function in accordance with the requirements provided.\(^{740}\) The ECTA’s

---


\(^{732}\) S73(1)(c) of Act 25 of 2002.

\(^{733}\) S73(1)(d). This provision is very similar to that of art 12(1)(c) of Directive 2000/31/EC. In terms of recital 43 of Directive 2000/31/EC, manipulations of a technical nature do not qualify as modifying information. This has been suggested as including installing virus scanners and firewalls. Valcke & Dommering “Directive 2000/31/EC” in European Media Law 1101.

\(^{734}\) S73(2)(1) of Act 25 of 2002. Roos notes that this appears to be aimed at preventing unlawful interception of the transmitted data. Roos “Freedom of expression” in ICT Law 430. The EU Commission, in relation to the similar provision contained in art 12(2) of Directive 2000/31/EC, explained certain terms. The term ‘automatic’ refers to the storage of the content that occurs as a result of the ‘ordinary operation of the technology’. The term ‘intermediate’ indicates that the storage of content is made during its transmission. The term “transient” indicates that the storage is for a limited time period. Proposal for a European Parliament and Council Directive 28. Valcke & Dommering “Directive 2000/31/EC” in European Media Law 1101: the “automatic, intermediate and transient storage of information” means the function is performed by machines not humans, during the course of the transmission of the content and storage is for a very short period of time for the purpose of transmission. See Chapter 2 for a discussion on the functioning of the Internet.

\(^{735}\) S73(2)(1)(b)-(c) of Act 25 of 2002, respectively.

\(^{736}\) S73(1).

\(^{737}\) Ibid.

\(^{738}\) Ibid.


provisions are very similar to those of the EU Directive. However, unlike the ECTA, the EU Directive does not require ISP’s which perform the function of the automatic, intermediate and transient storage of content to prevent unlawful access to the content transmitted.\textsuperscript{741}

3 2 Caching

Caching is the automatic, intermediate and temporary storage of content.\textsuperscript{742} Caching allows for efficient and prompt access to content as the user does not have to request the data from its source.\textsuperscript{743} The automatic, intermediate and transient storage of content referred to under the mere conduit function, is for a very short period of time and is for the purpose of carrying out the act of communication. Caching differs as it is the storage of content for a longer period and for the purpose of efficient communication.\textsuperscript{744}

The ECTA provides that an ISP that transmits content is not liable for the automatic, intermediate and temporary storage of that content where the purpose of that storage is to make the onward transmission of that content more efficient for other recipients of the ISP’s service.\textsuperscript{745} However, the ISP must not modify the content.\textsuperscript{746} Further, the ISP must not interfere with the lawful use of technology, which is widely recognised and used by the industry, to obtain information on the use of the content.\textsuperscript{747} The ISP must comply with the conditions of access to the content, and the industry standard rules regarding the updating of

\textsuperscript{745} S74 of Act 25 of 2002. This process is more generally known as “caching” data. Roos “Freedom of expression” in ICT Law 430.
\textsuperscript{746} S74(1)(a) of Act 25 of 2002.
\textsuperscript{747} S74(1)(d). An example of technology that is used to obtain information on the use of data is statistical programs that track the traffic on web pages. The ISP must ensure that the cached page does not result in less traffic being recorded on the source web page. Valcke & Dommering “Directive 2000/31/EC” in European Media Law 1102; Smith Internet Law 384; Lodder “EU Directive” in Guide to EU Law 88; Roos “Freedom of expression” in ICT Law 426.
the data. Finally, the ISP must remove or disable access to the data upon the receipt of a take-down notice that complies with section 77.

This provision is similar to the mere conduit safe harbour as it limits both civil and criminal liability. Furthermore an ISP will not lose the protection of this safe harbour where it has knowledge of unlawfulness. It will only lose the protection if it fails to remove content upon receipt of a take-down notice in the prescribed form.

3.2.1 Comparison with the EU Directive

Both the EU Directive and the ECTA limit the criminal and civil liability of ISP’s which perform this function in accordance with the requirements provided. There is a degree of similarity between the provisions of both statutory instruments. However, the ECTA provides more certainty than the EU Directive in relation to the removal of infringing content. The EU Directive provides that the cached content must be removed expeditiously by the ISP when it obtains ‘actual knowledge’ that the source content has been removed or disabled. Therefore, the EU Directive imposes a duty of care on ISP’s and where an ISP fails to act expeditiously it exposes itself to the risk of losing the protection of the Directive. However, what constitutes ‘actual knowledge’ or ‘expeditiously’ is not clear. In comparison, the ECTA provides that the content must be removed upon receipt of a take-down notice as opposed to obtaining actual knowledge, thus providing ISP’s with more certainty.

---

748 S74(1)(b)-(c) of Act 25 of 2002. Examples of conditions of access to data are: if a service is only accessible upon subscription, the cached page cannot be available for free; or the revenue from advertising banners must be paid to the rightful recipient and not the ISP caching the page. Valcke & Dommering “Directive 2000/31/EC” in European Media Law 1101-1102; Lodder “EU Directive” in Guide to EU Law 88; Roos “Freedom of expression” in ICT Law 426. The sale of products online provides an example of the necessity for the regular updating of data in accordance to the industry standards and rules. If a cache of a page selling a product is not regularly updated, a user may purchase the goods at an outdated price. Valcke & Dommering “Directive 2000/31/EC” in European Media Law 1101-1102; Lodder “EU Directive” in Guide to EU Law 88.

749 Take down notices are dealt with in s77 of Act 25 of 2002 and will be discussed further in Chapter 6.

750 Roos “Freedom of expression” in ICT Law 431. As it states that the ISP will “not be liable”.


753 Art 13(1)(e) of Directive 2000/31/EC.


### 3.3 Hosting

Hosting is the non-temporary and non-automatic storage of content at the request of a third party.\(^757\)

The ECTA provides that an ISP that stores content for a third party will not be liable for the damages arising from that content.\(^758\) It would appear that the protection only extends to civil liability.\(^759\) To qualify for this protection the ISP must:

- not have actual knowledge that the offending content or activities relating to it are infringing the rights of a third party;\(^760\) or
- be aware of facts or circumstances from which such an infringement is apparent; and\(^761\)
- upon receipt of a take-down notice that complies with section 77, the ISP must act expeditiously to remove or disable access to the offending content;\(^762\) and
- have appointed an agent to receive take-down notices and have provided sufficient contact details of its agent in locations accessible to the public.\(^763\)

This defence provides that ISP’s which perform this function will “not be liable for damages”.\(^764\) It therefore appears that this defence only limits civil liability.\(^765\) An ISP will lose this protection should it fail to remove the content upon receipt of a take-down notice in the prescribed form.\(^766\) It is submitted that this does not result in ISP’s benefiting from the protection of the safe harbour should they gain knowledge of the unlawful nature of the content. Should it be proved that an ISP obtained knowledge and only removed the content later upon receipt of the notice, it would not benefit from the protection of the safe harbour. Unlike the cache safe harbour, an ISP performing a function of a host must remove the content expeditiously. The term ‘expeditiously’ is not defined.\(^767\) However, the Guidelines

---


\(^758\) S75 of Act 25 of 2002.

\(^759\) Roos “Freedom of expression” in *ICT Law* 429, 431-433; Pistorius “Copyright law” in *ICT Law* 289.

\(^760\) S75(1)(a) of Act 25 of 2002.

\(^761\) S75(1)(b).

\(^762\) S75(1)(c).

\(^763\) The details that it should provide in terms of the ECTA are the agents name, address, phone number and email address. S75(2) of Act 25 of 2002.

\(^764\) S75(1) of Act 25 of 2002.

\(^765\) Roos “Freedom of expression” in *ICT Law* 432. However, see Van Zyl 2008 *THRHR* 233 as Van Zyl states that s75(3) gives an indication that the criminal liability of hosts can be limited.

\(^766\) Roos “Freedom of expression” in *ICT Law* 432.

\(^767\) See Chapter 6 for the potential problems that arise as a result of a lack of definition for this term.
remove any uncertainty that may arise by this failure, as it provides that an IRB’s take-down procedure is applicable to all its members. Therefore ISP’s must merely ensure that they comply with their IRB’s take-down procedure which has been approved by the minister, to comply with any time requirements contained in the safe harbours.

3.3.1 Comparison with the EU Directive

Both statutory instruments limit certain types of liability for hosts that comply with particular requirements. There are differences between their provisions relating to hosting:

- **Extent of protection from liability**
  
  The EU Directive provides for immunity from both criminal and civil liability, which is part of a global trend. The ECTA merely provides that ISP’s are not liable for damages, thus limiting ISP liability to civil claims only.

- **Appointing of an agent to receive take-down notices**
  
  In terms of the ECTA, for an ISP to utilise the host defence, it must appoint an agent to receive take-down notices. Further, the ISP must provide the agent’s contact details. The EU Directive does not have such a provision.

- **Removal and disabling of content**
  
  The EU Directive places a greater duty of care on ISP’s performing the host function than the duty placed on ISP’s performing the cache function. The EU Directive places an ISP that performs the host function in a difficult position. To benefit from

---

766 This term is not defined in the EU Directive or the DMCA, and authors have stated that this leads to uncertainty as to the length of time that ISP’s have to consider whether or not to remove the content. Edwards “The fall” in Law and the Internet 66; Weinstein 2008 Cardozo Art and Entertainment LJ 603-604, 609.

767 GG 29474 17.

768 The Guidelines also provide that the take-down procedure must contain an acceptable turn around period, thus the minister would examine the time-periods for compliance purposes in relation to the IRB recognition process. GG 29474 17.


770 Reed Internet Law 134.

771 S75(1) of Act 25 of 2002.


774 Roos “Freedom of expression” in ICT Law 432.

limited liability it must remove the content expeditiously upon obtaining actual knowledge, or becoming aware, of the allegedly unlawful content.\textsuperscript{779} However, should the content be found to be lawful, the ISP is exposed to liability in terms of a potential breach of contract with the recipient of its services for the wrongful removal of content.\textsuperscript{780} Further, what constitutes ‘actual knowledge’ or becoming ‘aware’ of the unlawful content is not clear and could depend on the nature of the content and the associated law.\textsuperscript{781} An example of this quandary can be found in the UK law of defamation.\textsuperscript{782} As a result of these difficulties and uncertainties, it appears that ISP’s in the EU are electing to remove or disable access to data upon receipt of a take-down notice without any investigation.\textsuperscript{783} This is despite the Directive providing that the removal or disabling of access to content must observe the principle of freedom of expression.\textsuperscript{784}

The ECTA does not place host ISP’s in the same difficult and uncertain position that the Directive does.\textsuperscript{785} In terms of the ECTA, ISP’s are not liable for the wrongful take down of content as a result of a take-down notice.\textsuperscript{786} The party who knowingly lodged a take-down notice that misrepresents facts will be liable for the costs of the wrongful take-down.\textsuperscript{787} ISP’s that perform the host function need only remove the content upon the receipt of a take-down notice provided that is in the prescribed format.\textsuperscript{788}

### 3.4 Information location tools

\textsuperscript{779} Art 14(1)-(2) of Directive 2000/31/EC. Lack of actual knowledge of unlawfulness is required to limit criminal liability and lack of awareness of facts or circumstances from which unlawful activity is apparent for limitation of civil liability. There is therefore a difference in the levels of knowledge required.\textsuperscript{780} Valcke & Dommering “Directive 2000/31/EC” in European Media Law 1103; Lodder “EU Directive” in Guide to EU Law 89; Roos “Freedom of expression” in ICT Law 427-428, 432; Edwards “The fall” in Law and the Internet 74.

\textsuperscript{781} It has been noted that the ‘knowledge-triggered liability system’ may have negative effects on information location tools as even the mere scanning of web pages may constitute knowledge. It has been argued further that advanced technology such as semantic analysis, concept-mapping, and natural language searches will make it impossible for information location tools to deny having knowledge. This could potentially hinder the continued growth of the Internet and the use of advanced technology. Ziniti 2008 Berk Tech LJ 602.


\textsuperscript{785} Roos “Freedom of expression” in ICT Law 432.

\textsuperscript{786} S77(3) of Act 25 of 2002.

\textsuperscript{787} S77(2).

\textsuperscript{788} S75(1)(c).
ISP’s that perform this function assist users in locating content online.\textsuperscript{789}

ISP’s performing this function will not be liable for damages incurred as a result of the actions of a third party,\textsuperscript{790} under circumstances where it:

- does not have actual knowledge of the offending content or that it is infringing the rights of a third party;\textsuperscript{791}
- is not aware of facts or circumstances from which such an infringement is apparent;\textsuperscript{792}
- does not receive direct financial benefit from the infringing content or activity;\textsuperscript{793} and
- removes or disables access to the content within a reasonable time of being informed that the content infringes the rights of another person.\textsuperscript{794}

This defence only limits the civil liability of ISP’s performing this function.\textsuperscript{795} It differs from the other defences provided for in the ECTA. ISP’s performing this function have more time to remove the content than is provided in the other functions.\textsuperscript{796} However, this defence does not provide the same certainty as the other defences, as it is not clear what constitutes being adequately ‘informed’. It is not clear why the legislature has opted not to extend this certainty to ISP’s that perform this function.

3 4 1 Comparison with the Digital Millennium Copyright Act

The Directive does not make provision for ISP’s which perform the function of information location tools.\textsuperscript{797} There however appears to be a degree of similarity between the provisions

\textsuperscript{789} See 5 5 on page 19 in Chapter 2 for a discussion on information location tools.
\textsuperscript{790} S76 of Act 25 of 2002. In terms s76, information location tools are ISP’s that refer or link Internet users to a web page through the use of information location tools, including a directory, index, reference, pointer, or hyperlink.
\textsuperscript{791} S76(a) of Act 25 of 2002.
\textsuperscript{792} S76(b).
\textsuperscript{793} S76(c). Roos suggests that, potentially, persons who receive revenue for linking web pages do not benefit from the immunity. Roos “Freedom of expression” in ICT Law 433.
\textsuperscript{794} S76(d) of Act 25 of 2002.
\textsuperscript{795} Roos “Freedom of expression” in ICT Law 433. This reason for this interpretation is the same as for the host function.
\textsuperscript{796} Although, the difference between expeditious and reasonable time are largely irrelevant in light of the Guidelines as discussed underneath the host function supra.
of the ECTA and DMCA. However, the DMCA differs from the ECTA as it extends the notice and take down procedure to ISP’s that perform this function. It is not clear why the RSA legislature elected not to extend this procedure to this function.

4 Criticism of the defences

ISP’s can play an important role in the creation of a safe, secure and effective online environment through assisting in the reduction of unlawful online content and activities. These defences can be criticised as they potentially encourage ISP’s not to monitor or filter at all for unlawful content to obtain protection. This would allow online unlawful content and activities to continue unabated.

Another criticism is the different manner that information location tools are dealt with.

5 No general obligation to monitor

The ECTA provides that there is no duty upon ISP’s to monitor the content they transmit or store, or to actively search for facts or circumstances indicating unlawful content or activities. However, this does not mean that the courts cannot impose specific obligations to monitor on ISP’s. The ECTA provides that executive authorities may establish procedures for ISP’s to inform the appropriate authorities of any illegal activities perpetrated by a recipient of the ISP’s services or content provided by the recipient. It also provides that procedures may be established whereby ISP’s furnish information enabling the identification of the recipient to the appropriate authorities upon request. This section can therefore be utilised by authorities to reduce any negative effect that the defences may have.

5 1 Comparison with the EU Directive and the Digital Millennium Copyright Act


798 17 USC § 512(d)(3).

799 GG 29474 9. The creation of a safe internet is also an objective of the ECTA, s2(1)(j) of Act 25 of 2002.

800 Self Regulation of Digital Media 8; Tambini et al Codifying Cyberspace 8.

801 S78(1)(a)-(b) of Act 25 of 2002.

802 Ss 73(3), 74(2) and 75(3) are similar to arts 12(3), 13(2) and 14(3) of Directive 2000/31/EC. These provide that those particular safe harbours do not prevent a court ordering the termination or prevention of unlawful activity in terms of any other law. This has been interpreted as allowing for specific obligations to be imposed by the courts. Valcke & Dommering “Directive 2000/31/EC” in European Media Law 1103.

803 Art 15(2) of Directive 2000/31/EC; s78(2) of Act 25 of 2002. The ECTA provides the power to establish such procedures to the minister.

804 See 2 supra.
All three statutory instruments bar the imposition of a general obligation to monitor on ISP’s.\(^805\) The provisions of the Directive and ECTA are very similar and despite barring the imposition of a general obligation to monitor on ISP’s, do provide for specific obligations to be imposed by the courts on ISP’s and for the authorities to establish certain reporting procedures.\(^806\)

In the DMCA, the ‘no obligation to monitor’ provision appears under the title of ‘Protection of Privacy’.\(^807\) It is submitted that it therefore appears that one of the considerations for this provision in the USA was to protect user’s privacy from ISP’s. In comparison, it appears that the purpose of this provision in the EU and the RSA was to address certain practical considerations. Firstly, it would be impossible for an ISP to monitor all of their content for any unlawful content or activity that may exist.\(^808\) Secondly, it would result in the ISP no longer performing the functions in a technical, automatic and passive manner. This would result in ISP’s being unable to rely on the protection provided by the statutory instrument.\(^809\)

### 6 ECTA’s savings section

The ECTA provides that the provisions of Chapter XI do not affect any obligations:

---

\(^{805}\) 17 USC § 512(m)(1); art 15 of Directive 2000/31/EC; s78 of Act 25 of 2002.

\(^{806}\) Recitals 47-48 of Directive 2000/31/EC; ss 73(3), 74(2), 75(3), 78(2) and 79 of Act 25 of 2002; Proposal for a European Parliament and Council Directive 30; Valcke & Dommering “Directive 2000/31/EC” in *European Media Law* 1103; Roos “Freedom of expression” in *ICT Law* 428; Lodder “EU Directive” in *Guide to EU Law* 90; Walden “Directive 2000/31/EC” in *Concise European IT Law* 254; Akdeniz Internet Child Pornography 236; Van Eecke & Ooms 2007 JIL 4. Examples of specific obligations to monitor exist in intellectual property case law from certain EU member states (such as Belgium, Germany and Denmark) where permanent injunctions to monitor or prevent certain content being transmitted have been imposed on ISP’s in terms of that states national law. Van Eecke & Ooms 2007 JIL 4-8. An example is the Belgian case, *SABAM v SA Scarlet* District Court of Brussels No 04/8975/A Decision of 29 June 2007, published in CAELJ Translation Series #001 (Mady, Bourrouilhou, & Hughes, trans.), 25 *Cardozo Arts & Entertainment LJ* 2008 (25) 1279, where the court ordered that the ISP concerned install filtering technology to prevent the downloading of illicit content. The court found that this does not amount to general monitoring as it is a technical instrument allowed by recital 40 of Directive 2000/31/EC. Further, it would not prevent the ISP from benefiting from the mere conduit defence as the filtering technology amounted to a technical and automatic function and therefore the ISP was not selecting or modifying the data. *SABAM 2008 Cardozo Arts & Entertainment LJ* 1288-1289. It is interesting to note how very different this view is to the USA *Stratton’s* case. It has been argued that injunctions imposed by the courts, such as in the *SABAM* case, increase ISP liability and are against the principle of no general monitoring as ISP’s are forced to permanently monitor their content for unlawful content, in this regard see Van Eecke & Ooms 2007 JIL 4-8. This was followed by members of Ireland’s music industry instituting legal action against Ireland’s biggest ISP, Eircom, seeking an injunction that was in the same terms as the *SABAM* case, i.e. that the ISP must use filtering technology. McIntyre *SCL.com* (03-04-2008). However, the matter was settled out of court in January 2009. Horten “Eircom filtering case settles out of court” iptegrity.com (29-01-2009) http://www.iptegrity.com/index.php?option=com_content&task=view&id=236 &Itemid =9 (accessed 19-10-2009).

\(^{807}\) 17 USC § 512(m).


• in terms of an agreement;\textsuperscript{810}
• in terms of a licensing or other regulatory regime established for ISP’s in terms of any other legislation;\textsuperscript{811}
• imposed by law or by a court to remove, block or deny access to content.\textsuperscript{812}

Further, it does not affect any right to limited liability based on common law or the constitution.\textsuperscript{813} Should any of the abovementioned obligations amount to an obligation to monitor, it must not be phrased too widely as this would be contrary to section 78.

7 Extent of ISP liability with the application of the ECTA

7 1 General
The ECTA removes the uncertainty that exists as to the extent of ISP liability by replacing the determination of their liability with a determination of whether they may utilise the safe harbours. It appears that the criminal and civil liability of ISP’s performing the mere conduit or cache functions is limited by the ECTA. However, it should be noted that there is disagreement between the authors as to whether the ECTA does limit the criminal liability of mere conduits and caches.\textsuperscript{814} This matter is yet to be settled by our courts.\textsuperscript{815} The ECTA only limits the civil liability of ISP’s that perform the host or an information location tool functions. The exact effect of the ECTA on ISP liability is yet to be decided by our courts.\textsuperscript{816} Suggestions as to the extent of ISP liability for the particular types of unlawful content will be provided infra.

7 2 Defamation

\textsuperscript{810} S79(a) of Act 25 of 2002.
\textsuperscript{811} S79(b).
\textsuperscript{812} S79(c).
\textsuperscript{813} S79(d).
\textsuperscript{814} Nel “Freedom of expression” in Cyberlaw 206, states that the ECTA only limits the civil liability of all the different functions. This is due to an interpretation of the savings clause as excluding immunity from criminal liability. Roos “Freedom of expression” in ICT Law 431 interprets the ECTA as providing mere conduits and caches with immunity from criminal liability. See Van Zyl 2008 THRH 234 where Van Zyl argues that s78 bars any obligation of monitoring for unlawful content, thus placing the ECTA in conflict with the obligation created by the FPA. Van Zyl argues that this can be avoided if Chapter XI is considered to only limit civil liability.
\textsuperscript{815} Roos “Freedom of expression” in ICT Law 432.
\textsuperscript{816} Nel 2008 Responsa Meridiana 124. In relation to defamation. However, there do not appear to be decided cases in relation to hate speech or obscene and indecent content either.
The ECTA extends protection to all ISP’s performing the functions contained therein from liability for third party defamatory content. The extent of this protection is however not the same. It would appear that an ISP performing either the mere conduit or a cache functions and is aware of the defamatory nature of the content would not be liable. However, it is difficult to conceive of a practical situation where ISP’s that perform such an automatic and technical function would gain such knowledge. An ISP performing a cache function would only lose the protection of the safe harbour should it fail to remove the content upon receipt of a take-down notice that complies with section 77 of the ECTA. ISP’s performing the host function are provided with certainty as they are only required to remove the content upon receipt of a take-down notice. However, should it be proven that they obtained knowledge of the defamatory nature of the content before receiving the take-down notice they would loose the protection of the safe harbour. The ECTA does not extend the same certainty to information location tools, as it is not clear what constitutes being adequately ‘informed’ of the defamatory statement.

7.3 Hate Speech

It was established in Chapter Three that an ISP requires knowledge of the unlawful nature of the content to commit the offence of distributing hate speech in terms of the FPA. 817 ISP’s that perform the function of either a mere conduit or a cache may be protected by the ECTA from criminal liability arising from third party hate speech regardless of knowledge. 818 ISP’s that perform the functions of either a host or an information location tool will not be protected by the ECTA from criminal liability. However, as the offence requires knowledge, ISP’s are not faced with a real threat should they perform their functions in an automatic, passive and technical manner.

It was suggested that in respect of the Equality Act ISP’s have a duty to monitor the content they transmit for hate speech. 819 As the Equality Act contains a supremacy clause, all ISP’s, regardless of the function they perform, are required to perform this duty. 820 This duty would cover any ‘loopholes’ available to mere conduits and caches in respect of the offences provided in the FPA.

817 S26(1) of Act 65 of 1996. See 4.3 on pages 70-77 in Chapter 3 for a discussion on ISP liability for obscene and indecent material.
818 Though note see n814 supra for authors different opinions.
819 See 3.3.2 on page 59 in Chapter 3 for a discussion on this point.
820 s5(2) of Act 4 of 2000.
7 4 Obscenity and indecency

In terms of the FPA, ISP’s that perform the function of a host or information location tool may be liable for the offence of distributing unclassified films. Although these offences require knowledge ISP’s may still be liable based purely on the performance of its basic functions. This is contrary to the principle in Chapter XI of the ECTA. Clarity is therefore needed as to the extent of ISP responsibility for the distribution and classification of films. Clarity is also required as to whether all film and multi-media content available on the Internet to the public is required to be classified.

ISP’s that perform the function of a mere conduit or a cache may not be liable for any offences committed by third parties in relation to child pornography, regardless of knowledge. However, this ‘loophole’ is closed by the fact that IAP’s are required to take all reasonable steps to ensure that their networks are not utilised for child pornography. They also have the duty to report its existence to the authorities. This obligation is not in conflict with the ECTA. Clarity is required as to the exact nature of these reasonable steps, especially in the light of the fact that the definition of ISP in the FPA is wide enough to include entities ranging from Internet cafes to large corporations. ISP’s performing the function of a host or information location tool are not protected by the ECTA and face liability for offences committed by third parties, should they have knowledge thereof.

8 Are ISP’s overprotected?

Due to the importance of ISP’s, it is necessary to provide them with protection where they would have been found liable for the performance of their basic functions. However, is it possible that they may be over protected? The author is of the opinion that they are not as the defences provided by the ECTA are based on the performance of basic functions that imply that the ISP neither has knowledge nor control over the third party content. Where an ISP has

---

821 See 4 3 4 on page 74 in Chapter 3 for a discussion on this point.
822 Example: Hosting mirrored international websites that contain film. See 4 3 4 on page 74 in Chapter 3.
823 See 4 3 4 on pages 74-75 in Chapter 3 for discussion on this point.
825 S27A(1)(b) of Act 65 of 1996. See Van Zyl 2008 THRHR 234 where Van Zyl argues that s78 bars any obligation of monitoring for unlawful content, thus placing the ECTA in conflict with the obligation created by the FPA. Van Zyl argues that this can be avoided if Chapter XI is considered to only limit civil liability.
826 S27A(2)(a) of Act 65 of 1996.
827 S27A(2)(b). As this amounts to a specific procedure to inform authorities of illegal activities, this is not in conflict with the ECTA as it allows for such procedures in terms of s78(2).
knowledge of unlawful content, there appears to be action that can be taken against it. This is not the position with ISP’s in the USA, where they receive broad immunity despite having knowledge of unlawful content.\textsuperscript{828} The author is of the opinion that ISP’s may still face unreasonable risks in relation to hate speech and obscene and indecent content in RSA.\textsuperscript{829}

It was argued in Chapter Four that the threshold requirements are unnecessary due to the manner in which the safe harbours are structured.\textsuperscript{829} However, it was stated in Chapter Two that the wide definition of an ISP may result in entities not considered by the legislature receiving protection.\textsuperscript{830} It should be obvious from the discussion supra that the safe harbours are based on the performance of particular functions in a technical, automatic and passive manner. If an ISP has knowledge of unlawful content, it can still be found liable. The widening of the application of the defences will therefore not result in a ‘CDA-like’ situation, where ISP’s are provided with immunity despite knowledge of the unlawful nature of the content.\textsuperscript{831} As the aim of the legislation is to provide ISP’s with protection from liability for the performance of their basic functions, the author considers it irrelevant what type of ISP receives protection. The operation of the safe harbours will limit the protection of the ECTA to those ISP’s that perform their functions automatically.

It should be obvious that the defences in themselves do not provide protection for Internet users. Further, it can be argued that these defences merely encourage ISP’s not to monitor or filter at all for unlawful content regardless of whether specific duties are imposed on ISP’s. This would allow for the proliferation of online unlawful content and activities to the detriment of the users of the Internet. This raises the question whether the approach adopted by RSA provides a balance between regulating ISP liability and protecting users from online unlawful content? To provide this balance another element is required, which it is submitted exists in the form of the notice and take-down procedure. This procedure will be discussed in the following chapter.

\section*{9 Recommendations}

\textsuperscript{828} See 2 1 8 on pages 38-39 in Chapter 3.
\textsuperscript{829} See 6 on page 96 in Chapter 4.
\textsuperscript{830} See 7 4 on pages 25-26 in Chapter 2 for reasons why it is necessary to have a wide legal definition.
\textsuperscript{831} See 2 1 8 on pages 38-39 in Chapter 3 for these negative effects.
The potentially onerous burdens imposed by the Equality Act and the FPA and the effects these may have on ISP’s have been raised in Chapter Three. It appears that the application of the ECTA may not resolve these issues and certain recommendations are made in this regard.

As regards the Equality Act, it is recommended that government establish the exact extent of ISP responsibility for any monitoring requirements that may exist. It is suggested that these duties should take into account the functions ISP’s perform, with mere conduits being imposed with a lesser duty to monitor than hosts. Together with the other recommendations made in Chapter Three in relation to the FPA, it is recommended that duties be placed on the correct parties in relation to monitoring for child pornography. To assist in placing the correct duties on the appropriate entities, attempts should be made to harmonise the FPA with the functions outlined in the ECTA, and specifically, that mere conduits should have a lesser duty to monitor than hosts. These steps need to be taken to harmonise the legislation to prevent a conflict with the objectives of the ECTA, as pointed out in Chapter Three.

10 Conclusion

Due to the importance of ISP’s it is appropriate to provide them with reasonable protection. It is apparent that the ECTA is a hybrid of both the DMCA and the EU Directive, and it has to a certain extent improved on the defences contained in these two statutory instruments. The defences are based on the basic functions that ISP’s perform. Despite certain exceptions, the ECTA’s defences provide ISP’s with simplicity and a greater degree of certainty as to the extent of their liability for particular types of unlawful third party content. ISP’s do not appear to be over protected as they face liability where they have knowledge of unlawful content. There would therefore not be any negative effects to widening the safe harbours to include ISP’s that do not comply with the threshold requirements. Concerns raised elsewhere in this dissertation in relation to hate speech and obscene and indecent content still appear to remain even with the application of the ECTA. Steps need to be taken by government to clarify certain issues for the benefit of ISP’s and prevent any conflict with the objectives of the ECTA.

---

832 ISPA argues the problem of child pornography will not be solved by bringing IAP’s under the jurisdiction of the act as IAP’s do not produce, distribute or offer child pornography. Massel & Molosiwa ISPA Submissions 4. The FPA seeks to regulate content, therefore responsibilities should be placed on content providers and not IAP’s. ISPA Amendment Bill Presentation 10.
CHAPTER SIX: NOTICE AND TAKE-DOWN PROCEDURE

1 Introduction
The notice and take-down procedures require an ISP, which performs specific functions, to remove or disable access to unlawful content or activities that exists on its networks upon receipt of a notification by a complainant. Failure to comply with a legitimate take-down notice will result in the ISP losing the protection of the safe harbour. This procedure is an essential element to the safe harbour legislation examined as its purpose is to provide a balance between providing ISP’s limited immunity and protecting Internet users from unlawful content. The procedures provide for the quick and inexpensive removal of content by ISP’s without the complainant having to prove its unlawfulness in court. Relevant notice and take-down procedures that exist in the USA, EU and the RSA will be analysed.

2 Notice and take-down procedures
2.1 United States of America
For ISP’s performing certain functions to be able to benefit from the safe harbour provisions of the DMCA, they must comply with the notice and take-down procedure provided therein. The purpose of this procedure is for the ISP to share the burden of copyright enforcement with the copyright owner. The procedure promotes cooperation between ISP’s and copyright owners in the detection and managing of copyright infringements. However, the procedure does not require an ISP to ‘evaluate the merits of a dispute’.

833 See the discussion on each of the procedures contained in the DMCA, EU Directive and the ECTA infra.
834 The notice provides the ISP with knowledge or awareness of the unlawful content or activity. It’s liability will then be determined by the normal application of the law in question. H Rep No 105-551 11; House of Representatives Digital Millennium Copyright Act of 1998 H Rep No 105-551 Part II (1998) 53-54; Smith Internet Law 372; Roos “Freedom of expression” in ICT Law 425, 429; Pistorius “Copyright law and IT” in ICT Law 280; Weinstein 2008 Cardozo Art and Entertainment LJ 598; Van Eecke & Ooms 2007 JIL 4.
The procedure applies to ISP’s performing the functions of a cache, host or information location tool. The DMCA’s procedure includes the following elements:

An ISP designating an agent to receive take-down notices

The DMCA provides that, an ISP must designate an agent for the above-mentioned purpose. The ISP must also provide the public and the Copyright Office with the agent’s contact information.

Take-down notice sent by the copyright owner

For the notification to be valid it must be in writing and include: the signature of the copyright owner or of a party authorised to act on their behalf; an identification of the copyrighted work claimed to have been infringed; identification of the alleged copyright infringing content and sufficient information to allow the ISP to locate it; the complainant’s contact information; a statement by the complainant that they believe, in good faith, that the content in question is not being used with the authority of the copyright owner, agent or the law; and a statement that guarantees the accuracy of the information contained in the notification, and under the penalty of

---

838 Pistorius “Copyright law and IT” in ICT Law 283; Romero 2006 Vniversitas 207; Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 626. However, there is an argument that this is an incorrect interpretation of the statute, as the take-down notice is merely a notification of a claim and not a notification of infringement. It therefore does not amount to sufficient notice for secondary copyright infringement. However, proponents of this argument admit that US case law has not necessarily followed this interpretation. See Yen “Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment” 2000 (88) Georgetown LJ 1833 1872-1880; Zarins “Notice Versus Knowledge Under the DMCA’s Safe Harbors” 2004 (92) Californian LR 261 286-289.

839 17 USC § 512(b)(2)(E). However, an ISP performing the function of a cache only has to comply with the procedure if: the content has already been removed from the originating web site or access to the content has been disabled; or a court has made an order to such an effect; and the user notifying the ISP performing the function of a cache must include a statement that advises the ISP that either of the above has occurred.

840 17 USC § 512(c)(3).
841 17 USC § 512(d)(3).
842 17 USC § 512(c)(2).
843 In terms of 17 USC § 512(c)(2), the ISP must make the information available to the public ‘through its service’, including in an accessible location on its website. The information required is the agents’: name, address, phone number, e-mail address and any other contact information which the Registrar of Copyrights may deem appropriate.

844 17 USC § S512(c)(3)(A).
845 The signature can be physical or electronic. 17 USC § S512(c)(3)(A)(i).
846 The DMCA provides further that if there is the infringement of multiple copyrighted works at a particular site, a list of all such works must be submitted in the notification. 17 USC § S512(c)(3)(A)(ii).
847 17 USC § S512(c)(3)(A)(ii).
848 The DMCA provides examples of such information being an address, telephone number and, if available, an e-mail address. 17 USC § S512(c)(3)(A)(iv).
perjury, that the complainant has the necessary authority to act on the behalf of the copyright owner.\footnote{17 USC § S512(c)(3)(A)(vi).}

Should the notice fail to contain the above-mentioned information, it cannot be considered in a determination of whether the ISP has adequate knowledge of the infringing content or activity.\footnote{17 USC § S512(c)(3)(B)(i).} There is an exception to this provision: if a complainant’s notice is defective the ISP must assist the complainant in making the notice compliant. Certain information must however be contained in the notice for a complainant to rely on this exception.\footnote{17 USC § S512(c)(3)(B)(ii).} In the event of the ISP failing to assist, the defective notice may be used in determining whether the ISP has adequate knowledge.\footnote{17 USC § S512(g)(1).}

Counter-notification by the party who is alleged to have infringed the copyright.

An ISP will not be liable for the wrongful removal or disabling of access to content which is made in good faith. It must however comply with certain requirements in order to avail itself of this protection.\footnote{17 USC § S512(g)(2)(A).} Firstly, the ISP must take reasonable steps to notify the third party that it has removed or disabled access to the content.\footnote{17 USC § S512(g)(2)(B)(i).} Secondly, the ISP must promptly provide the complainant with the third party’s counter notification upon receipt thereof.\footnote{17 USC § S512(g)(2)(B)(ii).} Upon the provision of such notice, the ISP must inform the complainant that it will replace or cease disabling access to the content in ten business days.\footnote{17 USC § S512(g)(3).} Finally, the ISP may not replace or cease disabling access to the content in less than ten or more than fourteen business days following the counter notification. The ISP may not take any action should its designated agent

\footnote{17 USC § S512(g)(2)(B).}
receive notice from the complainant of the institution of legal action against the third party.\textsuperscript{858} The counter notification is only applicable to ISP’s that perform the function of a host.\textsuperscript{859}

The DMCA provides for the minimization of fraudulent notifications and counter notifications, by providing that a person who makes such misrepresentations will be liable for damages incurred by the other parties involved.\textsuperscript{860}

\section{European Union}

A formal notice and take-down procedure was deliberately not prescribed by the EU Directive, leaving this aspect to self regulation at national level by member states.\textsuperscript{861} The EU Directive however does provide a basis for the development of such procedures,\textsuperscript{862} specifically in relation to ISP’s that perform the function of a host.\textsuperscript{863} The EU Directive provides that these procedures: could be developed through voluntary agreement by all parties;\textsuperscript{864} should be reliable and provide for the rapid removal of illegal content;\textsuperscript{865} and must take into account the freedom of expression.\textsuperscript{866} The EU Directive therefore does not affect the possibility of member states establishing specific requirements that must be fulfilled prior to removal or disabling of content by ISP’s.\textsuperscript{867} It appears however that member states have left this to self regulation by ISP’s.\textsuperscript{868}

\textsuperscript{858} 17 USC § 512(g)(2)(C).
\textsuperscript{859} 17 USC § 512(g)(2).
\textsuperscript{860} These damages include costs and attorneys fees incurred by the alleged infringing third party, copyright owner (or authorised licensee) or the ISP. 17 USC § 512(f); Pistorius “Copyright law and IT” in ICT Law 283.
\textsuperscript{862} Recital 40 of Directive 2000/31/EC. The cache and host safe harbours both provide that ISP’s must not have knowledge of the unlawful content, the mere conduit safe harbour does not. Art 12(1) of Directive 2000/31/EC provides that the ISP must act in a technical, automatic and passive manner. It therefore follows that any notice and take-down procedure could only be applicable to ISP’s that perform a cache or host function.
\textsuperscript{863} Recital 46, art 14(3) of Directive 2000/31/EC.
\textsuperscript{865} Recital 40 of Directive 2000/31/EC.
\textsuperscript{866} Recital 46, art 14(3) of Directive 2000/31/EC.
\textsuperscript{867} Recital 46 of Directive 2000/31/EC. However, only Finland and Iceland have done so. First Report on the application of Directive 2000/31/EC 14. The UK EC Regulations do not provide a specific procedure, but do provide an indication as to what information should be contained in the notice, such as: the complainant’s full name and address; details as to the location of the content; and details of the unlawful nature of the activity or information in question. Reg 22 of SI 2002/2013.
\textsuperscript{868} First Report on the application of Directive 2000/31/EC 14. In its first report on the EU Directive, the Commission found that while there was not an EU wide consensus as to the exact nature of the procedure,
2.3 South Africa

2.3.1 ECTA

ISP’s that perform the function of a cache or a host, and wish to benefit from limited liability, must remove or disable access to unlawful content or activities upon receipt of a take-down notice that complies with section 77 of the ECTA. The procedure does not require ISP’s to evaluate the merits of the dispute. The procedure consists of the following elements:

- ISP designating an agent to receive take-down notices
  An ISP that performs the function of a host must fulfill this requirement to benefit from limited liability. It is not a requirement for an ISP performing a cache function. When an ISP appoints an agent it must provide the agent’s contact information through its services and websites, in locations accessible to the public.

- Take-down notice sent by complainant
  For the notification to be valid, it must be in writing and addressed by the complainant to the ISP or its agent. The notification must include: the complainant’s full names and address; the complainant’s written or electronic signature; an identification of the allegedly infringed right; an identification of the unlawful content or activity; the remedial action required to be taken by the ISP in respect of the complaint; the complainant’s telephonic and electronic contact details, if any; a statement that the complainant is acting in good faith; a statement by the complainant that the information contained in the take-down notification is, to his knowledge, true and correct.

agreement had been reached as to the essential elements of such a procedure. It therefore concluded that there was no need for any changes to the Directive in this respect. First Report on the application of Directive 2000/31/EC 15.

869 Ss74(1)(e) and 75(1)(c) of Act 25 of 2002 respectively.
871 S75(2) of Act 25 of 2002.
872 The details that should be provided are the agent’s name, telephone number, address and e-mail address. S75(2) of Act 25 of 2002
873 S77(1)(a).
874 S77(1)(b).
875 S77(1)(c).
876 S77(1)(d). It is interesting to note that this particular sub-section of the ECTA does not refer to ‘data’ or ‘data message’, but to ‘material’ which is the term used in the DMCA.
878 S77(1)(f).
879 S77(1)(g).
880 S77(1)(h).
The ECTA provides that any person who lodges a complaint while knowingly misrepresenting the facts is liable for damages for the wrongful take-down.\textsuperscript{881} Further, that ISP’s, in such a case, are not liable for the wrongful take-down of the content.\textsuperscript{882}

2 3 2 Guidelines for the recognition of an industry representative body

The Guidelines\textsuperscript{883} are relevant to this discussion as IRB’s are required to establish a take-down procedure that is applicable to all its members.\textsuperscript{884} These form part of the minimum requirements for the recognition of an IRB by the minister. The procedure must be in accordance with section 77 and other relevant sections of the ECTA. It must be published on the IRB’s website and its members must provide a link to the procedure on their own websites. Finally, the Guidelines provide that the procedure must contain an acceptable turn around period in dealing with complaints.\textsuperscript{885}

3 Comparisons between the notice and take-down procedures

The EU Directive does not provide the same degree of certainty to ISP’s as compared to the DMCA and ECTA.\textsuperscript{886} The EU Directive places the burden of assessing the merits of a complaint on ISP’s.\textsuperscript{887} However, it fails to provide a statutory prescribed notice and take-down procedure to enable the ISP to perform this function properly. There is a potential negative effect on the freedom of speech, which will be discussed \textit{infra}. The failure to provide a notice and take-down procedure has been criticized,\textsuperscript{888} and the industry in the UK has requested that a procedure, underpinned by statute, be established.\textsuperscript{889} Further, unlike the DMCA and the ECTA, the Directive does not provide ISP’s with any protection against making a wrongful take-down in good faith in response to a notification.\textsuperscript{890}

\begin{thebibliography}{9}
\bibitem{881} S77(2).
\bibitem{882} S77(3).
\bibitem{883} GN 1283 GG 29474.
\bibitem{884} 17.
\bibitem{885} 17.
\bibitem{886} Van Eecke \& Ooms 2007 JIL 5; Albert et al \textit{How 'Liberty' Disappeared} 9.
\bibitem{887} In terms of the Directive, the ISP must remove the content upon gaining knowledge of unlawfulness. This requires a determination by the ISP as to whether the content is unlawful. See Chapter 5.
\bibitem{888} Van Eecke \& Ooms 2007 JIL 5; Albert et al \textit{How 'Liberty' Disappeared} 11.
\bibitem{889} \textit{Defamation and the Internet} 19. The UK government however believes that the procedures established by ISP’s are adequate. Should the procedures be inadequate, the government believes it would be more appropriate for the industry to attempt to resolve the issue themselves. United Kingdom Department of Trade and Industry \textit{A guide for business to the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013)} (2002) http://www.berr.gov.uk/files/file14635.pdf 28-29 (accessed on 7-10-2009).
\end{thebibliography}
The procedure contained in the DMCA and the ECTA is similar as it appears that both statutory instruments do not require an ISP to assess the merits of the dispute.\textsuperscript{891} The ISP may however elect to assess the merits in order to decide whether to comply with a notice or not. If it elects not to comply with the notice, it will lose the protection of the relevant safe harbour.\textsuperscript{892} Despite certain similarities, there are differences between the DMCA and the ECTA, for example:

- The ECTA’s procedure is applicable to fewer ISP’s than is the case with the DMCA. The ECTA only applies to ISP’s performing the function of a cache or a host,\textsuperscript{893} whereas the DMCA’s procedure applies to caches, hosts and information location tools;\textsuperscript{894}

- The ECTA does not make provision for ISP’s to provide assistance to complainants who do not comply with the notice requirements. The DMCA provides for ISP’s to assist complainants, but only where they have provided certain information;\textsuperscript{895}

- The ECTA does not provide protection to ISP’s from being deemed to have acquired knowledge or awareness of unlawful content from the receipt of a notice that does not comply with the statutory requirements. The DMCA provides that a notice that does not comply with the statutory requirements cannot be used to determine whether an ISP acquired knowledge or awareness of unlawful content;\textsuperscript{896}

- The ECTA does not make provision for a counter notification procedure, while the DMCA does. The ECTA provides that ISP’s can remove content without notification or reasons for the removal of content to the affected third party. It therefore does not protect the freedom of speech to the extent that the DMCA does. The potential negative effect on the freedom of expression will be discussed \textit{infra};

\begin{itemize}
\item Pistorius “Copyright law and IT” in \textit{ICT Law} 283 289.
\item Its liability will then be determined by the normal application of the law in question. H Rep No 105-551 11; H Rep No 105-551 Part II 53-54; Smith \textit{Internet Law} 372; Roos “Freedom of expression” in \textit{ICT Law} 425, 429; Pistorious “Copyright law and IT” in \textit{ICT Law} 280; Weinstein 2008 \textit{Cardozo Art and Entertainment LJ} 598; Van Eecke & Ooms 2007 \textit{JIL} 4. See Chapter 5 for a discussion on the operation of safe harbours and the role of knowledge and notices.
\item Ss74(1)(e) and 75(1)(c) of Act 25 of 2002.
\item 17 USC § S512(b)(2)(E), (d)(3) and (c)(3) respectively.
\item 17 USC § S512(c)(3)(B)(ii).
\item 17 USC § S512(c)(3)(B)(i). In other words, if a complainant furnishes a notice that is rejected by the ISP because it does not comply with the statutory requirements, that party cannot institute legal action against the ISP on the basis that the ISP has now gained knowledge or has become aware of facts that indicate unlawful activity through the receipt of the notice.
\end{itemize}
The DMCA provides that ISP’s act in good faith in the wrongful removal of content in response to a take-down notice. The ECTA does not contain such a provision.

4 The Internet Service Providers Association

To obtain recognition from the minister, IRB’s must establish a take-down procedure that is applicable to all its members. As ISPA is currently the only IRB to be recognized by the minister, it is relevant to examine the notice and take-down procedure that it has established in response to the ECTA and the Guidelines.

ISPA provides the public with a description of its notice and take-down procedure and information as to the requirements for a valid notice. It further provides an online form for the public to use to request a take-down notice. It is possible that the complainant may have to go further than the nine step notice and take-down procedure to have unlawful content removed. Should the ISP fail to remove the content at the conclusion of the procedure, the complainant is requested to indicate whether he wishes to lodge a Code of Conduct complaint. The relevant provisions of both procedures will be discussed, followed by statistics and information relating to the application of these procedures in practice.

4.1 ISPA’s notice and take-down procedure

Upon receipt of a take-down notice from a complainant, ISPA must whether the target of the complaint is an ISPA member. If it is, it must then be ascertained whether the information required in section 77 of the ECTA is contained in the notice. Should information be missing, ISPA notifies the complainant. Should all the required information be present, a number of “sanity checks” are then performed.

---

897 17 USC § 512(g)(1).
898 GG 29474 17.
902 ISPA “Take-down notification” para 9.
903 Para 3.
904 Para 4.
• Is the content in fact hosted on the ISP’s network?
• Has the content which is subject of the complaint been taken down previously due to an earlier request or for another reason?
• Is it technically feasible for the ISP to perform the requested remedial action?

If the complaint fails any of the sanity checks, ISPA staff will notify the complainant and the ISP that the complaint has been rejected and furnish reasons for such rejection. However, should the complaint pass these checks, it is forwarded to the ISP and the complainant is notified. ISPA then undertakes three separate checks at prescribed intervals to ascertain whether the content has been removed. The complainant is notified if the content is removed. However, should the ISP fail to remove the content, provision is made for ISPA to notify the ISP of its failure to do so. Should the ISP’s fail to remove the content after three such notifications, ISPA must establish what the ISP’s response is. The complainant is informed of this response and asked whether he wishes to lodge a Code of Conduct complaint against the ISP. The basis of the Code of Conduct complaint is that the ISP is allegedly in breach of clause 25 of ISPA’s Code of Conduct for failing to remove the content.

4 2 ISPA’s Code of Conduct complaints procedure
Should a complainant elect to lodge a complaint in terms of ISPA’s code of conduct, a copy of the complaint is forwarded to the ISP. The ISP is granted further time to remedy the complaint. Should the ISP not respond, an attempt is made by ISPA to inform the ISP that the matter remains unresolved. Should the complaint not be resolved to the satisfaction of all the parties involved, the complaint is forwarded to an adjudicator for review. The complainant and the ISP are both notified of this step.

---

906 Para 4-5. The target turn-around time for these first steps is three working days.
907 ISPA “Take-down notification” para 6-7.
908 Para 8.
909 Para 9. The target turn-around time for the performance of these notification functions is four working days.
911 ISPA “Code of Conduct complaint and disciplinary procedure” para 5.
912 The ISP is granted 5 further days, and may be granted another 5 days after being notified that the matter remains unresolved. The second 5 day period is at the discretion of the Code of Conduct Compliance officer. ISPA “Code of Conduct complaint and disciplinary procedure” para 6.
913 Ibid.
The adjudicators are independent experts who are skilled in evaluating complaints in a reasonable and fair manner. There are certain considerations that the adjudicator must take into account when deciding on the merits of the matter. Should the complainant have lodged a complaint or instituted action with any other regulatory body or court, the adjudicator may decide to hear, dismiss or suspend the hearing of the complaint. The adjudicator can request the parties to submit further information relevant to the dispute within a specified timeframe. Should a party fail to do so, the adjudicator must proceed without it.

The Code of Conduct Complaints Procedure provides guidance as to the type of decision the adjudicator can make, for example: that the complaint is not valid or that the content should be taken-down. A copy of the adjudicator’s decision and the reasons must be forwarded to the complainant, the ISP and ISPA’s Management Committee.

Either party may appeal against the decision. The appeal must be lodged with ISPA’s Management Committee, who may reject the appeal or refer it to an appeals panel. A copy of this decision and the reasons are forwarded to the ISP and the complainant. Should it be referred to the appeals panel, the procedure is the same as was followed by the adjudicator in the initial decision. The appeal panel consists of three adjudicators, with the majority decision considered the final decision of the panel.

---

914 The adjudicator must warrant that he is free of any conflict of interest. ISPA “Adjudicators and appeal panel” http://www.ispa.org.za/code/adjudication_panel.shtml para 1-2 (accessed on 18-07-2009) subsequently ISPA “Adjudicators and appeal panel”. The adjudicators are usually information communication technology lawyers and, at this stage, are appointed in an ad hoc manner as the need arises. Brooks “Question 14” in Re: Questions relating to ISPA’s take down procedure (26-10-2009) E-Mail to N.D. O’Brien (copy on file with author), subsequently Brooks Re: ISPA’s take down procedure.

915 The adjudicator should take into account: the complaint; the ISP’s response to the complaint; the code of conduct; any other complaints made by the complainant; and any other complaints made against the ISP. ISPA “Code of Conduct complaint and disciplinary procedure” para 7.

916 Para 8.

917 Para 9.

918 Other decisions the procedure empowers the adjudicator to make are: The ISP must undertake appropriate remedial action; the ISP should be issued with a reprimand, warning or a fine; the ISP should be suspended from ISPA subject to conditions determined by the adjudicator; the ISP’s membership should be revoked; ISPA should publish a report containing the identity of the ISP, the details of the breach of the Code of Conduct, and any action taken regarding the breach; ISPA should report unlawful conduct or content to the relevant law enforcement authority. Further, should an ISP have failed to have provided requested information to the adjudicator, he may take this failure into account in making his decision. ISPA “Code of Conduct complaint and disciplinary procedure” para 10. Note that these decisions are for any breach of the code of conduct and are not tailored specifically for the take-down process, unless where specified.

919 ISPA “Code of Conduct complaint and disciplinary procedure” para 11. The target turn-around time from the appointment of adjudicator to the resolution of the dispute is three calendar weeks.

920 ISPA “Code of Conduct complaint and disciplinary procedure” para 12. Within ten working days of the distribution of the adjudicator’s decision.


922 Para 14.
43 ISPA’s notice and take-down procedure in practice

In terms of the Guidelines, ISPA must provide the minister with statistics of the number of take-down notices received. These statistics prove useful in providing some insight to the ISPA’s procedure in practice. During 2008, ISPA received 44 take-down notices thirteen were rejected, ten because the target ISP not not an ISPA member. The other 31 notices were accepted:

The content was removed by the ISP or it’s client in 22 of these matters;

Five were resolved through negotiation between the complainant, the ISP and/or it’s client;

In three of the matters, the target ISP’s refused to remove the content;

One notice was withdrawn by the complainant, who subsequently lodged an amended notice.

Only one of these notices led to a complaint being lodged in terms of ISPA’s complaints procedure. ISPA keeps records of all complaints and subsequent steps taken thereafter and does not have a recorded case of a fraudulently submitted complaint. At the time of writing, the 2009 figures had not yet been analysed but it was indicated that the number of complaints had increased. ISPA claims that it is able to meet its target times approximately 90% of the time. The primary reason for any delays is caused by ISP’s who are unfamiliar with the procedure. Another reason is that ISPA has only one compliance officer. It is therefore possible that a notice will not always be dealt with in the target times when ISPA experiences a high volume of complaints or take-down notices. According to ISPA most notices are resolved within 24 to 48 hours. The cost of compliance is high, with the duty becoming more onerous as the number of notices increases.

ISPA must ensure that the notice complies with section 77 of the ECTA. It is not necessary to investigate the validity or legitimacy of the claim made in the notice. The ISPA procedure does not provide the third party with an opportunity to object to a take-down notice. However, in practice, ISP’s contact the third parties who may then raise objections to

---

923 ISPA “Adjudicators and appeal panel” para 3.
924 GG 29474 30.
927 ISPA’s Code of Conduct Report 3.
928 Brooks “Question 17” and “Question 3” in Re: ISPA’s take down procedure.
929 Brooks “Question 22” in Re: ISPA’s take down procedure.
930 Brooks “Questions 11-13” in Re: ISPA’s take down procedure.
931 Brooks “Question 8” in Re: ISPA’s take down procedure.
the notice with their ISP. The ISP must then make an informed decision as to how to respond to ISPA. However, anecdotal evidence provided by ISPA suggests that clients of its members who receive a take-down notice panic and remove the content themselves. There are also instances where the content has been removed by the ISP itself as a result of a failure by the client to respond to the ISP. Depending on the nature of the notice, entire websites or particular pages have been removed. The persons receiving the notices do not necessarily have legal training. The larger ISP’s, however, generally employ someone with some degree of training.

It is interesting to note that ISPA believes that the ECTA has the potential of having a chilling effect on free speech. This belief appears to be based on the ease that any person may lodge a take-down notice. Although there is the belief that the procedure should be improved, no suggestions have yet been formulated.

5 Concerns related to the notice and take-down procedures
The notice and take-down procedure is an important element in Internet content regulation. Internet technology allows unlawful content to be made available quickly to a worldwide audience. Notice and take-down procedures therefore offer a quick and cost effective solution to complainants to limit damages suffered as a result of such unlawful content. However, number of concerns have been raised regarding this procedure. These concerns will be discussed infra, followed by a consideration of their relevance to RSA and recommendations as to possible improvements.

5.1 Appropriateness of expanding the procedure to all forms of unlawful content
It has been questioned whether a procedure that was originally established to deal with copyright infringements is suitable to be extended to all types of unlawful content. In theory, the DMCA take-down notice is simple to prepare and has narrow application to a

932 Brooks “Question 19” in Re: ISPA’s take down procedure.
933 Brooks “Question 6” in Re: ISPA’s take down procedure.
934 Brooks “Questions 10” in Re: ISPA’s take down procedure.
935 Brooks “Questions 7” in Re: ISPA’s take down procedure. Small ISP’s generally do not have qualified persons to deal with notices, however they receive fewer notices than larger ISP’s who have a member staff with some degree of training.
936 Brooks “Questions 20-21 and 23” Re: ISPA’s take down procedure.
938 Tambini et al Codifying Cyberspace 122; Ziniti 2008 Berk Tech LJ 605; Self Regulation of Digital Media 45.
particular area of law. Its narrow application means that an ISP is not faced with any difficult interpretations of the law should it elect to evaluate the merits of the dispute and it is not required to make any complicated judgment calls. However, a study of a collection of DMCA notices found that a third of the take-down notices were majorly flawed in that either there was no legal basis for the claim or there was substantial non-compliance with the take-down procedure, thus rendering the notice unusable. The study found that content was removed when it should not have. The research therefore found substantial errors in the application of this procedure to a narrow field of law. This should cast doubt on the expansion of the use of this procedure to cover all types of unlawful content. Such expansion requires an ISP to have legal knowledge covering the full legal spectrum and the ability to apply that knowledge correctly to a particular set of facts. It is therefore questionable whether ISP’s will have the capacity, or inclination for fear of liability, to identify which notices are legally baseless and correctly identify content as unlawful. This raises concerns over the negative effect that the procedure has on the freedom of speech.

5.2 The negative effect of notice and take-down procedures on the freedom of expression

The regulation of Internet content amounts to a freedom of speech issue, the regulation of which is usually considered to be a public function. However, the public policy of the jurisdictions’ examined promote and favour regulation of the Internet by ISP’s over

---

939 Ziniti 2008 Berk Tech LJ 605; Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 621, 640-641. However, it has been argued that this is not entirely true as courts can struggle to interpret copyright law and apply it to the facts of a particular case. This therefore casts doubt over an ISP’s ability to do so. Ziniti 2008 Berk Tech LJ 605; Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 640-641; Zarins 2004 Californian LR 278-281.

940 Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 666. The study examined approximately 876 take-down notices gathered by the Chilling Effects project from the period of March 2002 until August 2005. The Chilling Effects project is a consortium of law school clinics in the USA. The project collects take-down notices and cease and desist letters relating to intellectual property and other online speech. The documents are then published online at www.chillingeffects.org. Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 641.

941 Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 666.

942 Ziniti 2008 Berk Tech LJ 605; Arehart 2007 The Yale LJ Pocket Part 44.


944 Tambini et al Codifying Cyberspace 272 275. Depending on the nature of the speech and the manner it is communicated, societies are in certain instances comfortable with state regulation of speech and in other instances they are not. For instance, certain societies become concerned when political speech is limited or monitored by the state, whereas they are comfortable with the monitoring and limitation of certain types of entertainment by the state. Tambini et al Codifying Cyberspace 272.
Due to the sheer volume of online content, the greater degree of control and choice that users have over the content they elect to view, it is not practical to have a central regulatory system. As a result, the system settled on for the regulation of Internet content is the notice and take-down procedures. However, there is concern regarding the effect that these procedures have on the freedom of expression, as they do not provide an incentive to protect the freedom of expression.

It is argued that self regulation amounts to the privatization of censorship as the public function of limiting the freedom of speech is placed in private hands. Self regulation allows ISP’s to determine the scope of their legal obligations. This discretion can endanger the freedom of speech, as users are not provided with the same protection that may exist where this freedom is limited by public authorities. ISP’s will not necessarily face the same legal constraints or scrutiny that is imposed by the courts or society on public authorities who regulate speech. There is concern that ISP’s will favour their own commercial interests over an individual’s freedom speech, electing to remove content to avoid financial loss. They may also elect to sacrifice the principle of freedom of speech all together in order to gain access to a new market.

---

945 See 5 on page 93 in Chapter 4.
946 Tambini et al Codifying Cyberspace 271; Moore & Clayton The impact and incentives 199; Alhert et al How ‘Liberty’ Disappeared 2.
948 Kreimer 2006 University of Penn LR 31; Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 637-638.
949 Tambini et al Codifying Cyberspace 275; Kreimer 2006 University of Penn LR 27-28; Alhert et al How ‘Liberty’ Disappeared 14; Self Regulation of Digital Media 45.
951 This financial loss may occur in at least two different ways: increased operating costs due to having to determine which content is legal or not; and high damages awards as a result of costly lawsuits. In comparison, the value of keeping one client over the potential financial loss is marginal. Ziniti 2008 Berk Tech LJ 606; Brown 2008 Berk Tech LJ 456; Kreimer 2006 University of Penn LR 28-30; Arehart 2007 The Yale LJ Pocket Part 45; Alhert et al How ‘Liberty’ Disappeared 7-8; Self Regulation of Digital Media 8.
952 For example: Google and Skype agreed to censor their networks for the purposes of gaining large market shares in China. China is known for its draconian censorship of communication mediums. Kreimer 2006 University of Penn LR 18. There may be pressure exerted on ISP’s to sacrifice the freedom of speech in order to avoid criminal sanction. This occurred in Pennsylvania where the effect of new legislation was that, due to commercial and technical practicalities, ISP’s disabled access to approximately 1.19 million innocent websites. The legislation was found to be unconstitutional. Center for Democracy & Technology v Pappert 337 F Supp 2d 606 (ED Pa 2004). See n541 on page 76 for a further discussion.
It is also not clear whether ISP’s have the skills, resources, ability or inclination to properly establish the lawfulness of the content subject to a take-down notification. Courts can struggle to identify and balance all the competing rights in a particular matter. It follows that ISP’s would struggle more so as this is not their function. There is concern that notice and take-down procedures are not properly administered and little regard given to the principle of freedom of expression. These procedures can therefore result in the unfair removal of legal content without due process, right of appeal, right of review or transparency. This leaves little recourse for the third party whose legal content has been removed. Research has indicated that a penalty for perjury may not be enough to prevent the submission of wrongful take-down notices to ISP’s.

The procedures outlined supra allow online content to be removed without a court order and without the third party receiving any notice prior to the removal of his content. Complainants of unlawful offline content would invariably have to make use of the court system to obtain the satisfaction they seek, whereas they only need to make an allegation in relation to online content to have it removed. This amounts to a very strong remedy to remove speech off the Internet. The system is open to abuse by parties wishing to silence criticism and their competition, with few remedies available for an innocent third party. Specific concerns relating to the use of the DMCA in silencing of critics and the relative ease of removing content in the EU is discussed infra.

---


956 Tambini et al Codifying Cyberspace 122; Arehart 2007 The Yale LJ Pocket Part 45; Kreimer 2006 University of Penn LR 28, 65; Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 636-637; Alhert et al How ‘Liberty’ Disappeared 14; Self Regulation of Digital Media 45. Researchers have found that there is a lack of detailed information on the amount of take-down notices, websites removed as a result thereof, and the procedures used by ISP’s to determine the legality of content as it is not part of public record. Alhert et al How ‘Liberty’ Disappeared 2; Nas The Multatuli Project 7; Tambini et al Codifying Cyberspace 122; Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 623.

957 Nas The Multatuli Project 7; Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 666.


5 2 1 Negative effect of on the freedom of expression: Digital Millennium Copyright Act

It would appear that the DMCA does contain some protection for the third party’s freedom of expression through its counter notification procedure. However this procedure does not provide an adequate balance between the competing interests of all the parties to the dispute. The counter notification procedure is only enacted after the content has been removed, with the content only replaced ten to fourteen days after its removal, if it is able to be replaced at all. This is a substantial period of time for a person to be silenced.\textsuperscript{960} Should the content be replaced, it can still be removed a second time without a court order.\textsuperscript{961} The third party is silenced again until the completion of the court proceedings. This has created the perception that in terms of the DMCA, a third party is guilty until proven innocent.\textsuperscript{962} It is clear that the DMCA’s counter notification procedure is not a quick and efficient remedy for the third party. It is therefore not as effective at protecting the interests and rights of the third party as the notice and take-down procedure is for the copyright holder.\textsuperscript{963}

These flaws are significant as it appears that the take-down procedure is being abused by corporations to silence their critics and their competition.\textsuperscript{964} Approximately 55\% of the section 512(d)\textsuperscript{965} take-down notices submitted to Google, were from corporations requesting the removal of links to their rivals products.\textsuperscript{966} Of these, 22.5\% of the notices were deemed questionable.\textsuperscript{967} However the study did not find much evidence of counter notices or of ISP’s putting content back.\textsuperscript{968}

\textsuperscript{960} Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 637. An example is the case where the Church of Scientology attempted to use take-down notices to silence its critics. It filed 4000 take-down notices on YouTube, which responded by removing the content. However, the content was replaced again when the affected third parties filed counter notices. The effect was that for a period of 10 days, critics of Scientology were unjustifiably silenced on YouTube. Anderson “Scientology fights critics with 4000 DMCA takedown notices” Arstechnica.com (08-09-2008) http://arstechnica.com/old/content/2008/09/ scientology-fights-critics-with-4000-dmca-takedown-notices.ars (accessed 22-11-2009).

\textsuperscript{961} See 2 1 supra for a discussion on the operation of the DMCA’s take-down procedure,


\textsuperscript{964} Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 687; Romero 2006 Vniversitas 209-210; Long 2005 The John Marshall J of Computer & Info L 543. For example: Online Policy Group v Diebold Inc 337 F Supp 2d 1195 1203 (ND Cal 2004), the defendant had used DMCA notices to suppress content that disclosed embarrassing flaws in their electronic voting machines, to which most ISP’s responded by removing the content despite it not being a copyright issue. However, see n959 supra for an example of that it is not only corporations that use take-down notices to silence critics.

\textsuperscript{965} These are take-down notices for information location tools.

\textsuperscript{966} Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 651.

\textsuperscript{967} Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 684.

\textsuperscript{968} Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 680. There is also evidence to suggest that a number of take-down notices have nothing to do with copyright infringement at all and relate to another area of law. Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 687. An interesting development, is that the music industry is sending 17 USC § 5512(a) notices to ISP’s, despite no provision being made for take-down notices to be submitted to ISP’s performing the function of a mere conduit. This is the music
It would be difficult to apply the counter notification procedure to an information location tool as the third party does not have a service relationship with the ISP performing that function. It is therefore only applicable to ISP’s that perform the function of host. However, a link to content can still be removed purely on the basis of an allegation. This makes content more difficult to find and can effectively silence the third party, especially if the ISP is a large and popular information location tool such as Google. There is concern that corporations make use of the DMCA to remove their competition from an information location tool to increase their own ranking on the search results. The effect on free speech is not limited to the USA as the study shows that 34% of take-down notices submitted to Google were targeting foreign content.

5.2.2 Negative effect on the freedom of speech: EU Directive

An EU commissioned report found that there is a need for ‘legislative underpinning’ for take-down procedures to be effective. EU member states however have left this challenge to the Internet industry to regulate. It appears that ISP’s are removing content without any consideration as to the validity of the complaint or whether the content is in fact unlawful. Evidence of this was found in two separate experiments conducted in the EU to ascertain the effectiveness of ISP notice and take-down procedures and to identify whether it is easy to abuse these procedures. In both the Mystery Shopper and Multatuli Project experiments,

industries attempt to fight copyright infringement that occurs on peer to peer networks where the ISP acts as a mere conduit and has no control of the content that resides on the users computer. It appears that the music industry is attempting to force ISP’s to utilise their policies for repeat infringers as established in terms of 17 USC § S512(i)(1)(A) as a requirement of ISP eligibility for protection under the DMCA. There is evidence that ISP’s have threatened to cut a third party’s Internet access based on a single complaint. The problem is that the music industry is capable of misidentifying alleged infringers. Further, it raises a real freedom of speech issue in that if the third party’s account is cancelled, it results in him being unable to express himself in any manner at all online.

Research was undertaken on take-down notices collected by the Chilling Effects consortium, of which 736 out of the 876 notices collected were submitted to Google. Out of the 736 notices, approximately two thirds of the notices were submitted to Google in terms of its function as an information location tool. The report was part of the RightsWatch programme, funded by the European Commission, attempted to standardise the EU’s notice and take-down procedure. However, it failed to achieve this due to a lack of consensus between the stakeholders. The report was published in 2000.

970 Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 628; 17 USC § S512(g)(2).
972 Alhert et al How ‘Liberty’ Disappeared 17; Nas The Multatuli Project 1.
fake complaints about alleged copyright infringing content were submitted to certain ISP’s.\textsuperscript{978} The majority of ISP’s responded by removing the content within hours of the complaint without any attempts at further investigation.

A preliminary scoping report by the British Law Commission on defamation and the Internet,\textsuperscript{979} found that ISP’s invariably removed content upon receipt of a letter from solicitors representing a well resourced company.\textsuperscript{980} ISP’s often elected to remove the entire site and not the particular page with the offending content.\textsuperscript{981} The report stated that the feared result is that ISP’s are removing content that may be in the public interest,\textsuperscript{982} thus interfering with the freedom of expression.\textsuperscript{983}

The experiments and the report demonstrate the threat to freedom of speech that exists in the EU. It may be possible that the threat is even greater in the EU than it is in the USA.\textsuperscript{984} This is due to the EU Directives’ lack of specific requirements for a notice and take-down procedure, failure to provide for a counter notification procedure, and lack of transparency and accountability.\textsuperscript{985} The EU Directive leaves room for abuse and creates a situation where ISP’s remove content without due consideration to the merits of the notification.\textsuperscript{986} The EU Directive has removed an impartial judicial system with established rules and replaced it with an entity that is not neutral as its commercial interests are affected by its decision. It could further contravene principles of due process and places powers that are separated at state

\textsuperscript{978} Both experiments had a similar structure. The researchers created a website, which they had hosted by major ISP’s. The website contained legal content from a notable author, originally published in the 19\textsuperscript{th} Century. It was clearly stated that the content belongs to the public domain. The researchers then sent an e-mail from an anonymous Hotmail account, pretending to belong to a fictitious society and complaining that their copyright had been infringed. The experiments were therefore structured so it would be easily ascertainable that the complaint was not valid. The Mystery Shopper experiment tested a major USA and UK ISP. The USA ISP requested further information for DMCA purposes and the UK ISP removed the content in 24 hours of receipt of the complaint. The Multatuli Project experiment tested 10 major Dutch ISP’s. The result was that 70\% percent of the ISP’s removed the content within hours of the receipt of the content, with only one ISP seemingly looking at the website in question. See Alhert et al How ‘Liberty’ Disappeared and Nas The Multatuli Project.

\textsuperscript{979} See Defamation and the Internet.

\textsuperscript{980} 11.

\textsuperscript{981} 12.

\textsuperscript{982} 14.

\textsuperscript{983} 15. The report states that the effect will be even more detrimental on small, under-resourced organisations. Defamation and the Interne 15.

\textsuperscript{984} Alhert et al How ‘Liberty’ Disappeared 26-27.


\textsuperscript{986} Alhert et al How ‘Liberty’ Disappeared 27. This can be partly attributed to the provisions of the EU Directive that stipulate that content must be removed upon gaining actual knowledge of unlawfulness as opposed to receipt of a notice. See 3 3 1 on page 113-114 in Chapter 5 for a discussion on this aspect.
level into one entity as the ISP must: gather evidence themselves; make a judgment on the evidence that they gathered; and enforce their judgment.\textsuperscript{987}

5.3 Limitation on the third party’s right to defend himself

Closely linked to the issue of freedom of speech is the fact that the notice and take-down procedures do not make adequate provision for the third party to defend himself.\textsuperscript{988} It appears that the safe harbour legislation is created with two parties interests in mind: ISP’s and their interest in obtaining limited liability, which is achieved by encouraging them to be as ignorant as possible in relation to the content they transmit to be able to benefit from limited liability; and Internet users and their interest to have a mechanism of redress against unlawful content.\textsuperscript{989} The reality is that the third party’s interests are not adequately provided for.

It has been suggested that these procedures appear to be developed more in favour of preventing ISP liability than unlawful content.\textsuperscript{990} However, the complainant is furnished with more resources to enforce his rights than the third party has to defend his.\textsuperscript{991} The content is removed without judicial oversight and without the third party receiving notice prior to the removal of the content. These procedures place a third party in a weak position as his right to defend himself is circumvented.

5.4 Negative effect on the growth of the Internet

Supporters of a CDA-like immunity for ISP’s argue that the notice and take-down procedure has a negative effect on the growth of the Internet. It does not promote the creation and development of ISP’s with large networks carrying a wide variety and amount of content. By virtue of their size, large ISP’s are being exposed to greater potential liability, incurring a greater cost of compliance and carrying a heavier burden in dealing with a greater volume of take-down notices. It is argued that the notice and take-down procedure therefore forces ISP’s to restrict the size of their networks and the volume or nature of content they carry.\textsuperscript{992}

\textsuperscript{987} Alhert et al \textit{How 'Liberty' Disappeared} 27.
\textsuperscript{988} The DMCA is, to a limited degree, an exception to this due to its counter notification procedure. See 4 2 2.
\textsuperscript{989} Romero 2006 \textit{Universitas} 193; S Rept No 105-190 20; Brown 2008 \textit{Berk Tech LJ} 445.
\textsuperscript{990} Tambini et al \textit{Codifying Cyberspace} 124; \textit{Self Regulation of Digital Media} 45.
\textsuperscript{991} Romero 2006 \textit{Universitas} 212; Urban & Quilter 2006 \textit{Santa Clara Comp & High Tech LJ} 628, 636-637, 682.
\textsuperscript{992} Ziniti 2008 \textit{Berk Tech LJ} 604.
5.5 Lack of an adequate balance between ISP liability and protection of Internet users

The DMCA promotes a policy of co-operation between ISP’s and copyright owners.\textsuperscript{993} The burden of monitoring the Internet for copyright infringement is placed on the copyright owner as he is obviously the most capable of identifying content which is infringing his copyright.\textsuperscript{994} It is argued that the ISP’s burden of removing the content upon notification of a copyright infringement is relatively light.\textsuperscript{995} However, a reason for this light burden may be found in the belief that requiring ISP’s to monitor their networks for unlawful content is not practical due to sheer volume. Further, that such an obligation would result in a dramatic increase in the cost of Internet services.\textsuperscript{996} It is feared that the obligation could cripple the Internet and negatively affect the freedom of speech.\textsuperscript{997} However, it is argued that the Internet has changed significantly since the promulgation of the DMCA, calling into question the fairness of this arrangement.\textsuperscript{998} The DMCA is therefore no longer able to provide an adequate balance between ISP’s and copyright owners.\textsuperscript{999} These changes are:

- **Web 2.0**

  The biggest change to the Internet has been the rise of a phenomenon known as ‘Web 2.0’.\textsuperscript{1000} Web 2.0 websites are programmed by ISP’s, but the sites content, growth and development is predominantly due to the active participation of the sites users.\textsuperscript{1001} Well known examples of Web 2.0 websites are YouTube, MySpace and Facebook.\textsuperscript{1002} These sites generate income through advertising revenue,\textsuperscript{1003} which increases as more users view the site. It is argued that the Internet traffic increases substantially on web pages where there is unlawful content, thus these sites profit from unlawful content.\textsuperscript{1004} Due to the huge profits that these websites make, the relatively light...
burden placed on ISP’s by the DMCA no longer appears to be fair to copyright owners.\textsuperscript{1005} It is argued that the profits an ISP makes should be taken into account in determining who should bear the biggest burden of copyright enforcement.\textsuperscript{1006}

It is also argued that it is a fiction that ISP’s have no control over the content because these sites are predominately based on third party content.\textsuperscript{1007} The content exists and is uploaded into a space programmed and designed by the ISP’s. The latter can therefore control and determine the nature of the content on their sites.\textsuperscript{1008} It is further argued that the belief that placing an obligation on ISP’s to monitor for unlawful content is unreasonable, may now be outdated. So too the belief that such an obligation would place a great financial burden on ISP’s. This is due to the advancements made in filtering technology, the effect of which is that it may result in ISP’s being able to utilize such technology at a low cost.\textsuperscript{1009}

- Peer to peer networks

Another change to the Internet is the rise of peer to peer networks. A majority of copyright infringement appears to occur on these networks where ISP’s act only as mere conduits and never host any content. The content is transferred from one user’s PC to another users PC with it never being hosted, the only role the ISP plays is that of a mere conduit. It follows that copyright owners are not provided with protection in relation to this technology.\textsuperscript{1010}

There is a fear that the DMCA shields copyright infringement as it creates an incentive for ISP’s not to monitor for and prevent unlawful content where these changes to the Internet
determined to be profiting from the content, this would result in it loosing the protection of the host safe
harbour in terms of 17 USC § 512(c)(1)(B). See Brown 2008 Berk Tech LJ 464-468 for a discussion on
this aspect and the solution. The EU Directive and the ECTA do not contain such a provision.
453.
442.
441-442; Ziniti 2008 Berk Tech LJ 692.
Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 686-687; Edwards “The fall” in Law and the
Internet 78-79.
may require more active involvement. This can result in a negative effect on intellectual property development.\textsuperscript{1011}

6 Relevance of these concerns to South Africa

The ECTA allows content to be removed on the basis of a mere allegation without any notification to the third party either before or after removal. The ISP may elect not to remove the content. It will then however lose the protection of the safe harbour. The take-down procedure is not extended to information location tools.\textsuperscript{1012} This creates a situation similar to the EU which could result in information location tools responding to notices in a similar fashion as ISP’s in that jurisdiction. In general the ECTA does not provide: a counter notification procedure; rights of appeal or review; and transparency. The issue of transparency is however corrected to a degree by the Guidelines for the recognition of an IRB.\textsuperscript{1013} ISPA could improve transparency by publishing the relevant statistics related to take-down notices on its website.

ISPA’s procedure does correct some of the shortfalls of the ECTA and is transparent.\textsuperscript{1014} However the procedures being used by ISP’s to notify third parties of the take-down notice and for the removal of content are not. The ISPA procedure cannot escape certain realities created by the ECTA, viz, that the ISP bears the responsibility for making the decision to remove the content, that the third party is not provided the opportunity to defend himself and is reliant on the ISP to defend his interests. This should be of particular concern considering that half of the notices received in 2008 resulted in the content being removed, with only three instances where ISP’s refused to remove content. Further, only one complaint was referred to adjudication.\textsuperscript{1015} Therefore a large amount of the content complained of was removed by the ISP’s or their clients. The statistics do not indicate the nature of the complaints or their validity. It is therefore not clear whether ISP’s and their clients are

\textsuperscript{1011} Brown 2008 Santa Clara Comp & High Tech LJ 438; Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 637; Tambini et al Codifying Cyberspace 122; Self Regulation of Digital Media 8.
\textsuperscript{1012} S76 of Act 25 of 2002.
\textsuperscript{1013} One of the recommendations for the provision of greater transparency for such procedures is for ISP’s to publish summaries of complaints, numbers of adjudications and findings on their websites. Tambini et al Codifying Cyberspace 299; Alhert et al How ‘Liberty’ Disappeared 28. The Guidelines for the recognition of an IRB do provide this transparency to a limited degree. IRB’s must keep a record of the full process in dealing with all complaints received. GG 29474 28-29. Further, one of the IRB’s reporting duties is to advise the minister of take-down statistics in the annual report submitted by 28th February every year. GG 29474 29-30.
\textsuperscript{1014} The ISPA procedure provides: that its staff must notify complainants when their notices do not comply with requirements of s77 of Act 25 of 2002; for an appeal process; and full records are kept of all complaints with the number of which result in the removal of content. See 4 3 supra for a discussion on the ISPA notice and take procedure.
\textsuperscript{1015} See 4 3 supra for a detailed discussion on the statistics relating to take-down notices received by ISPA.
removing content for fear of liability in circumstances where the content is in fact lawful. It is possible that the ECTA take-down procedures may be too effective in providing relief to victims of Internet abuse and fail to provide an adequate balance between the rights of all Internet users. Due to the ECTA not providing protection to third parties, it would then appear that it does not provide an adequate balance between ISP accountability and the interests of all the users of the Internet.

In light of the above and the research conducted in the USA and the EU, there should be concern in RSA in relation to notice and take-down procedures, in particular: the capacity of ISP’s to correctly identify legally baseless notices and identify content as lawful; the privatisation of censorship; the negative effect on the freedom of speech; the centralisation of various powers into one entity; the capacity of ISP’s to remain neutral and not allow their commercial interests to affect their decision; the inadequate balance in favour of the complainant at the expense of the third party; the ease of removal of legal content without due process; the minimal provision to innocent third parties for remedies of abuse of the procedure by complainants; lack of transparency and accountability in the procedures; the lack of right to appeal or of review.

There is a further concern that does not appear to exist in the other jurisdictions examined. The ECTA does provide a degree of relief for the victims of Internet abuse. However the limited liability only applies to ISP’s that are members of a recognized IRB. It is doubtful whether an ISP that either does not have the resources or the inclination to join ISPA will have an adequate take-down procedure.\textsuperscript{1016} The result is that the ECTA does not extend equal protection to all Internet users. A complainant may have his take-down notice ignored by the ISP. Therefore some complainants may not be able to make use of the quick and cost effective procedure contained in the ECTA and be forced to institute lengthy and costly court proceedings.\textsuperscript{1017} Research conducted in the EU would suggest that ISP’s would remove the content as soon as possible without any due consideration to the merits of the claim. Therefore, not all third parties are offered the limited protection of the ISPA procedure.\textsuperscript{1018}

\textsuperscript{1016} There is also no benefit of limited liability to counteract the burden of having a take-down procedure.
\textsuperscript{1017} The statistics provided by ISPA showed that they rejected at least 10 take-down notices on the basis that the target ISP was not a member of ISPA. See 43 \textit{supra} for the statistics relating to take-down notices received by ISPA. That is therefore 10 complainants that have been denied the quick and cost efficient take-down procedure offered by the ECTA.
\textsuperscript{1018} As stated \textit{supra}, ISP’s are meant to notify the third party of the take-down notice, thus potentially offering them an opportunity to provide the ISP with information to defend their interests.
As the ISP would not be a member of a ‘watchdog’ entity such as ISPA, there is no place for Internet users and third parties to lodge complaints with.

In relation to the other concerns raised, there is no evidence to suggest that take-down procedures are resulting in a negative effect on Internet growth. At this stage, it would appear that filtering of content would be an answer to the problems created by Web 2.0 and peer to peer networking. However, despite the assertions of its proponents, there is a counter-argument that filtering and content blocking technology is still not feasible as it easily circumventable, too expensive and amounts to a significant burden on ISP’s.

7 Recommendations

Despite these issues, the take-down procedure should be favoured over the broad immunity provided by CDA. It is clear that the procedure needs to be revised to provide a greater balance between the interests of all three parties to the dispute. There following recommendations are made:

Amend the ECTA to allow for universal application of a take-down procedure

It is suggested that the RSA government consider the creation of a ‘hotline system’ similar to the system that exists in Europe. These systems operate by members of the public reporting content to the hotline they believe is illegal, such as child pornography. The complaint is then investigated and the relevant ISP or law enforcement officials are notified where necessary. The EU system currently only

---

1020 Esselaar What ISP’s can do 15-22. Ireland’s music industry sought an injunction to compel Eircom to use filtering technology. The estimated cost to deploy a particular filtering system in the EU was €6 per year. Eircom has approximately 560 000 broadband subscribers so the potential cost amounts to €3.3 million a year, without extra costs such redesigning its network to facilitate filtering. The matter was settled out of court. McIntyre SCL.com (03-04-2008). The Irish case was based on the Belgian case of SABAM v SA Scarlet, District Court of Brussels No 04/8975/A Decision of 29 June 2007. The ISP was ordered to install particular filtering software, but the trial court overturned its decision when the ISP managed to show the court that the software is technically unworkable. However, the court still requires the ISP to filter if an effective method can be found. The decision is being appealed. McIntyre “SABAM v. Scarlet: Belgian ISP released from obligation to filter network for illegal downloads” tjmcintyre.com (26-10-2008) http://www.tjmcintyre.com/2008/10/sabam-v-scarlet-belgian-isp-released.html (accessed 22-11-2009).
1021 See 2 1 8 on pages 38-39 in Chapter 3 for the negative effect of this policy.
1022 The hotline system formed part of the EU’s Safer Internet plan. EU Parliament and Council Decision No 276/1999/EC. For an example of a hotline, see http://www.iwf.org.uk for the UK’s Internet Watch Foundation (IWF).
1023 Tambini et al Codifying Cyberspace 123; Akdeniz Internet Child Pornography 253.
applies to certain categories of illegal content and would have to be expanded in RSA to include all unlawful content, such as defamatory content.\textsuperscript{1024}

This proposed body will be able to investigate content and advise ISP’s accordingly with no cost to the ISP or exposure to liability.\textsuperscript{1025} The body would not be in the same compromising position as ISP’s and its staff would be better trained.\textsuperscript{1026} A detailed discussion as to the body’s creation, structure and procedures falls outside the scope of this work.\textsuperscript{1027} However, it should have clearly defined and transparent procedures allowing for the balancing of rights and providing a quick resolution to complaints.\textsuperscript{1028} These procedures should apply to caches, hosts and information location tools. It should be further expanded to include ISP’s that are not members of a recognized IRB. This would require that the threshold requirements should no longer be applicable to obtaining access to the safe harbours. It has already been discussed that the widening of the application of the safe harbours should not result in any negative effects.\textsuperscript{1029} The creation of an independent body and the universal application of the take-down procedure would make it possible for all Internet users to have equal access to the same remedy.

- Further research and regular independent audits

Should the recommendations made supra not be considered favourably, it is stressed that further research is undertaken to determine whether there are any negative effects as a result of the current take-down procedure. It is also recommended that independent audits are undertaken to ascertain whether currently recognised IRB’s take-down procedures are subject to the same degree of abuse is occurring in the USA.

\textsuperscript{1024} For example: The IWF was originally created for the purpose of removal of child pornography and its mandate has been expanded to include racist material. Its focus is therefore on criminal content. Tambini et al \textit{Codifying Cyberspace} 296; IWF “Role and Remit” http://www.iwf.org.uk/public/page.35.htm (accessed 22-11-2009); \textit{Legal Instruments for Combating Racism} 155; Akdeniz \textit{Internet Child Pornography} 252-253.

\textsuperscript{1025} The creation of such a body is raised as a potential solution to the EU situation in Julià-Barceló & Koelman 2000 \textit{Comp L & Security Report} 237.

\textsuperscript{1026} Tambini et al \textit{Codifying Cyberspace} 123; Julià-Barceló & Koelman 2000 \textit{Comp L & Security Report} 236; Alhert et al \textit{How ‘Liberty’ Disappeared} 10. However, any legislation enacted would have to clearly provide that the investigation and decision is made by this entity and not ISP’s. This has not been made clear in terms of EU law with concern that it is creating confusion as to which entities bear the responsibility for making the decision to remove content. Tambini et al \textit{Codifying Cyberspace} 123.

\textsuperscript{1027} It is also recommended that the body contain sufficient representation of any recognised IRB’s due to their power and influence. They are a necessary asset and would be needed to lend their support to such a structure.

\textsuperscript{1028} Transparency would be an important issue for such a body. A criticism of the IWF is its lack of transparency. Edwards “Pornography” in \textit{Law and the Internet} 653.

\textsuperscript{1029} See 8 on page 121 in Chapter 5
and the EU. Through the recommended research and audit processes it will be possible to determine whether there is a need to amend the ECTA to counteract these abuses.

Grant information location tools a mere conduit protection
This function is largely automatic in nature and is essential to the functioning of the Internet in that they are the primary starting points for a majority of users in finding content. The negative effect on the freedom of expression would be great should these ISP’s be used as strategic targets to silence criticism and opponents. It is therefore recommended that the mere conduit safe harbour be extended to ISP’s performing that function.

Amend the ECTA to counter act the negative effects of peer to peer networks
In France, ‘graduated response’ or ‘three strikes’ legislation has been developed in relation to intellectual property law violations. This law provides that the government can issue ISP’s with a notice to terminate a users Internet access for a particular period of time. This notice can only be issued after the ISP has accumulated three warnings that a user has violated intellectual property law. The new law only allows for termination upon judicial review. This appears to be part of a gradual change in the EU from treating ISP’s as neutral intermediaries to being used actively to prevent certain types of unlawful content. It is recommended that government undertake research into the possibility and desirability of providing a similar solution in the ECTA, or any other appropriate statute. However, this is not a panacea that

1030 The recommendation of such an audit of the EU system is made in Tambini et al Codifying Cyberspace 298. See Tambini et al Codifying Cyberspace 303 for issues that should be included in such an audit.
1031 See 5 5 on page 19 in Chapter 2 for a discussion on the operation of information location tools.
1033 Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 690-691.
1034 This is a recommendation made in Urban & Quilter 2006 Santa Clara Comp & High Tech LJ 690-691 to counteract this effect on information location tools in the USA.
1036 A previous version of the bill had been struck down by the French Constitutional Court as it had not made provision for termination on judicial review. The British Department of Business Innovation and Skills has also proposed similar legislation. This is in contrast to Finland which has declared Internet access a legal right. Jackson “France Constitutional Court approves Internet piracy bill” Jurist (23-10-2009) http://jurist.law.pitt.edu/paperchase/2009/10/france-constitutional-court-approves.php (accessed 22-11-2009).
will cure all the ills of unlawful content, as defamation and hate speech often involve nuances of human speech which cannot be detected accurately by filtering options.\textsuperscript{1038}

8 Conclusion

The ECTA is similar to the other statutory instruments examined. The defences available encourage ISP’s to be as ignorant as possible of the content they transmit to be able to benefit from limited liability. The notice and take-down procedure is meant to provide a balance by providing a solution to complainants of unlawful content. A number of flaws in this procedure have been identified. It appears to only adequately preserve the interests of two parties to the dispute and does not protect the interests of third parties. The threshold requirements result in not all Internet users being afforded equal opportunity to utilise the same remedy. The take-down procedure raises doubts as to the neutrality and capabilities of ISP’s in performing the task required of them and the potential negative effects thereof, for example on the freedom of speech. The procedure provided by the Act does however appear to be effective in providing relief to victims of unlawful content. Although research does suggest that it is open to abuse, to the detriment of the third party. Due to these flaws it does not provide an adequate balance between ISP liability and the rights of all Internet users.

The notice and take-down procedure should be favoured over broad immunity. There appears however to be a need to amend the procedure. In terms of the ECTA’s take-down procedure, and as practiced by the ISPA, the ultimate responsibility for determining whether content is to be removed still lies with the ISP. The negative effects can never be removed completely until this power is moved to another entity. However, any amendment to the procedure must be able to provide the required balance between all the parties interests while still providing a quick and cost effective remedy to victims of online unlawful content.

\textsuperscript{1038} Edwards “The fall” in Law and the Internet 85.
CHAPTER 7: CONCLUSION AND RECOMMENDATIONS

1 Summary of findings
Through the performance of their basic functions, ISP’s face a risk of incurring civil and criminal liability from unlawful content posted by third parties. This risk was viewed by some jurisdictions to threaten the effectiveness of the Internet, prompting the promulgation of safe harbour legislation.

In Chapter Two a description of the role and characteristics of ISP’s in the functioning of the Internet was given. ISP’s perform a wide variety of different roles and are essential for the Internet’s operation and development. To provide sufficient protection to ISP’s, and to cover future technological developments, states developed wide definitions that encompass the wide variety of roles that ISP’s perform. This may have unintended consequences as entities may receive protection that the legislature did not intend.

In Chapter Three a survey was undertaken of the appropriate laws in the USA and the UK in order to provide suggestions as to the extent of ISP liability in RSA where they are not afforded the protection of Chapter XI of the ECTA. It was established that ISP’s that are not protected by the ECTA face uncertainty as to the extent of their liability for third party unlawful content. This can be attributed to difficulties in applying the law to the Internet and the fact that courts have at times struggled to fully understand the technology of the Internet. This results in the law not being properly applied. Examples of this appear in the USA and the RSA. Suggestions as to ISP liability for the following types of content were made:

- Defamatory content
  ISP liability should be determined by its relationship to the defamatory material in accordance with the common law. Difficulties may however arise in the application of the common law to the Internet. The result is not certain and may result in the ISP being erroneously found liable.

- Hate Speech
  In terms of the FPA, ISP’s can be found criminally liable for distributing third party hate speech. Knowledge is however required on the part of the ISP. It was suggested
that ISP’s have a duty in terms of the Equality Act to monitor the content they transmit for hate speech and for speech that unfairly discriminates against any person.

- Obscene and indecent content

ISP liability for third party obscene and indecent content is determined in accordance with the FPA. There are a number of offences that can be committed by ISP’s, but only if it has knowledge of the unlawful nature of the content it transmits or hosts. It is argued that there is uncertainty as to the exact extent of ISP’s duties for online content. IAP’s are required to register with the Films and Publications Board. IAP’s have the duty to take all reasonable steps to prevent their services being used for hosting or distributing child pornography. It is argued that there is uncertainty as to what constitutes reasonable steps. ISP’s are required to perform a number of duties upon becoming aware that their services are being used for child pornography.

In Chapter Four, the threshold requirements that ISP’s must comply with to be able to utilise the safe harbours in the ECTA were examined. The threshold requirements are based on membership to an IRB that has been recognised by the minister. The IRB is an integral element for ISP’s to obtain limited liability. IRB’s wishing to obtain recognition must comply the extensive set of requirements provided by the Guidelines. This is to fulfil the Departments duty to ensure that only responsible ISP’s benefit from Chapter XI of the ECTA. It was argued that this duty is misguided and contrary to the logic of the safe harbours which are based on the performance of ISP’s technical functions. The requirements are therefore an unnecessary barrier to limited liability that could possibly have a serious affect on the industry as a whole. The Guidelines are too broad and, after a comparison to the position in the EU, are not in accordance with international best practice. The Department has failed to meet certain objectives of the ECTA and the Guidelines. In practice recognition is difficult to obtain and is a costly process. It was argued that this indicates government’s failure to recognize the importance of the Internet industry. This failure could potentially stifle investment and development in the Internet, placing RSA in an unfavourable position to compete internationally.

In Chapter Five the safe harbours provided by the ECTA were examined. The safe harbours are a hybrid of similar provisions in the DMCA and the EU Directive. Due to the importance
of ISP’s in the flow of information and the development of the Internet it is appropriate to provide them with reasonable protection. The safe harbours in the ECTA are based on basic functions that ISP’s perform: mere conduit, caching, hosting and information location tool.

The ECTA limits the civil liability of ISP’s that perform the mere conduit or cache functions. There is however disagreement between authors as to whether the ECTA does limit the criminal liability of ISP’s performing those functions. This matter is yet to be settled by our courts. The ECTA only limits the civil liability of ISP’s that perform the host or information location tool functions. The safe harbours are justified as the functions that they are based upon must be performed in an automatic manner which implies that the ISP has neither knowledge nor control over the third party content. The ECTA extends protection to all ISP’s that comply with its requirements from liability for defamatory content. The ECTA does provide greater certainty to ISP’s. However certain exceptions exist as a result of legislation that does not take the technology of the Internet into account. The ECTA does not limit the application of duties identified in the Equality Act. All ISP’s, regardless of the function it performs, must execute the duty imposed. The ECTA does not assist ISP’s in resolving the uncertainty as to the extent of their duties in terms of the FPA. It also does not remove the duties imposed on IAP’s in relation to child pornography.

The safe harbours do not provide ISP’s with too much protection as it was established that they face liability where they have knowledge of unlawful content. It was argued that there would not be any negative effects to granting all ISP’s the protection of the safe harbours.

In Chapter Six the notice and take-down procedure was analysed. The provision of limited liability is balanced with this procedure which provides relief to victims of unlawful content. This procedure was analysed and it appears to be effective in its ability in providing that relief. The concerns that have been raised in relation to this type of procedure as it exists in the USA and the EU were examined. Some of these concerns are relevant to RSA and it is suggested that certain flaws exist in the ECTA procedure. These are raised under 21 infra.

2 Conclusions drawn

In this dissertation the ECTA, FPA and Equality Act are referred to and certain provisions analysed. Conclusions can be made as to their strengths and weaknesses.
21 ECTA

Chapter XI of the ECTA does not affect the liability of the primary publisher, but does provide protection to ISP’s performing their basic functions as intermediaries for third party content. It removes the uncertainty that exists in relation to the extent and nature of ISP liability in RSA law, barring certain exceptions. The limitation of liability is justified on the basis that the nature of these basic functions imply that the ISP neither has knowledge nor control over the third party content. The notice and take-down procedure appears to provide effective relief for victims of unlawful content as they are provided with a quick and inexpensive method of removal of content by ISP’s without the victim having to prove its unlawfulness in court. ISP’s are protected from liability for the wrongful take down of content as a result of a take-down notice. The ECTA compares favourably to most of the safe harbour legislation examined. ISP’s are not over protected, unlike the position in the USA. ISP’s do not receive broad immunity from liability, and can be found liable where they had knowledge of the content and failed to act. The ECTA provides a better balance between the rights and interests of the ISP and victims of unlawful content than the CDA does. Further, the ECTA provides ISP’s with more certainty than the EU Directive. Despite these strengths, there are a number of criticisms that can be levelled at the ECTA:

- The requirement of membership of an recognised IRB to obtain limited liability is not in accordance with international best practice:
  The creation of this extra requirement amounts to an unreasonable barrier to limited liability.

- The ECTA does not offer the same benefits to information location tools:
  ISP’s that perform this function do not have the same degree of certainty that is provided in the other safe harbours as it does not utilise the notice and take-down procedure.

- The ECTA does not provide an adequate balance between ISP accountability and protection of the interests of the users of the Internet in South Africa:
  The ISP is encouraged to be as ignorant as possible in relation to the content it transmits to obtain limited immunity. This is balanced with the take-down procedure. It is established in Chapter Six that only the interests of the ISP and the complainant are promoted by the ECTA, at the expense of the rights and interests of the third party.
The notice and take-down procedure is not fair on the third party:
It is established in Chapter Six that third party content can be easily removed through the use of the notice and take-down procedure. However, it appears that it creates a situation where the third party is guilty until proven innocent as it does not provide the him: with an opportunity to object to having his content removed; to be informed of the removal of the content or the reasons thereof; for an appeal or review process. The complainant is granted a quick and inexpensive method of enforcing his rights, whereas the third party is forced to approach the courts to enforce his. The ISPA procedure does correct some of the shortfalls. It however cannot escape the underlying problem with the legislation, which is that ISP’s still have responsibility to remove content and that the third party is not granted adequate opportunity to defend himself.

The notice and take-down procedure can be easily abused and allows for an unreasonable limitation of the freedom of expression:
Research indicates that it is easy to silence competition online through take-down procedures as content is removed on the basis of a mere allegation that does not have to be proved in court. The procedure amounts to the privatisation of censorship and the centralisation of various powers underneath ISP’s. It is doubtful whether ISP’s have the capacity, or the inclination, to correctly identify legally baseless notices or establish the lawfulness of the content.

The ECTA does not extend equal protection to all users of the Internet:
The take-down procedure will in all likelihood only be utilised by ISP’s that are members of IRB’s. If the ISP is not a member of an IRB it could result in either the complainant’s request for removal of content being ignored or alternatively the automatic removal of content without any consideration of the merits of the request.
2.2 Promotion of Equality and Prevention of Unfair Discrimination Act
The Equality Act provides far more protection than legislation of a similar nature examined in other jurisdictions. It does not however take the Internet and its technology into account. It appears to place the unreasonable burden on ISP’s to monitor all content they disseminate for hate speech. As this duty does not appear to exist in the jurisdictions examined, it could stifle investment and development in the Internet should it be enforced.

2.3 Films and Publications Act
The FPA does not take the technology of the Internet fully into account, creates uncertainty, and places duties on the wrong entities. In particular it requires IAP’s to perform tasks that they are not capable of and imposes unnecessary burdens. It further requires IAP’s to undertake costly and potentially ineffective measures to combat child pornography. The Act therefore does not promote Internet development and could result in the objectives of the Act not being met, especially in relation to the protection of children.

3 Recommendations
Various provisions of the legislation examined appear not to stimulate investment, innovation and development of the Internet. They may hinder RSA international competiveness and potential for further economic development. Action is required to address these defects.

3.1 ECTA
It relation to the ECTA, the following recommendations are made:

- Grant mere conduit protection to information location tools
  Information location tools perform their functions in a largely automatic manner. They are very important as they are the primary starting points for Internet usage for a majority of Internet users. They may however be useful tools to silence opposition which would negatively effect the freedom of speech. It is therefore recommended that they are granted mere conduit protection.

- Legislation to limit the negative effects of peer to peer networks
  Investigations should be undertaken into the possibility and desirability of introducing ‘three strikes’ provisions into the ECTA, or other relevant legislation. A similar approach to French law could be adopted.
Restructure the threshold requirements
The ECTA should be amended to allow all ISP’s to utilise the safe harbours. This would result in the Guidelines becoming redundant. They could however be used as a model for future consumer protection regulations. The structure of the safe harbours will only allow ISP’s that perform their functions in an automatic, technical and passive manner to obtain limited liability. There would therefore not be any negative effects to widening the application of the safe harbours.

Restructure the notice and take-down procedure
The ECTA’s take-down procedure provides ISP’s with the power to decide whether to remove content or not upon receipt of a take-down notice. A number of negative effects of this procedure have been raised. It is recommended that an independent body, similar to the hotlines in the EU, is created to deal with notice and take-down requests. This body should be representative of all relevant interest groups and consist of staff trained in making the proper determinations as to the unlawfulness of content. The notice and take-down procedure used by this body must be transparent and afford third parties due process. The implementation would grant all users equal access to the same remedy.

Alternatively, the threshold requirements should be re-examined to be less of a burden to prospective IRB’s. It is also suggested that further research is performed to determine the extent of any negative effects that arise as a result of the current take-down procedure. Independent audits should be performed to ascertain whether currently recognised IRB’s take-down procedures are subject to any abuses. Through the recommended research and audit processes it will be possible to determine whether there is a need to amend the ECTA or IRB take-down procedures to counteract these negative effects.

3 2 Promotion of Equality and Prevention of Unfair Discrimination Act
In respect of the Equality Act it is recommended that government establish the exact extent of ISP responsibility for any monitoring requirements that may exist. It is suggested that these duties should take into account the functions ISP’s perform, for example: mere conduits should be imposed with a lesser duty to monitor for hate speech than hosts.
3 3 Films and Publications Act
The following are recommended in relation to the FPA:

- The term ‘Internet Service Provider’ should be changed to ‘Internet Access Provider’ (IAP) to avoid confusion;
- Clarity be provided by the Films and Publications Board as to the extent of ISP responsibility for the distribution and classification of films;
- To assist in placing the correct duties on the appropriate entities, attempts should be made to harmonise the FPA with the functions outlined in the ECTA;
- IAP’s should be excluded from the classification requirements for films;
- Automated mirrors for moderated international download sites should be excluded from the classification requirements for films;
- The reporting requirements for child pornography should better reflect information that IAP’s can provide;
- Multiple registration requirements for IAP’s that fall underneath the Electronic Communications Act and the FPA should be removed;
- Clarity needs to be provided as to whether multimedia content is a film or a publication;
- The Films and Publications Board should indicate what steps are considered reasonable for IAP’s to take to prevent their networks being utilised for child pornography.
- It should be further established exactly what the responsibilities of ISP’s are in relation to the classification requirements for online content and any associated registration requirements.

4 Concluding remarks
The promulgation of Chapter XI of the ECTA reduces the risks that ISP’s faced from civil and criminal liability. The approach provided should be favoured over the uncertain position that existed prior to the promulgation of the Act. It should also be favoured over the broad immunity that is afforded ISP’s in the USA. ISP’s can be held liable where they have knowledge of unlawful content. There are however flaws that exist that may be necessary to correct to truly provide certainty to ISP’s and provide adequate balance to the rights of all Internet users.
BIBLIOGRAPHY

BOOKS


Burns Y *Communications Law* (2001) Butterworth Publishers (Pty) Ltd: Durban


Siegel P *Communications Law in America* (2002) Allyn & Bacon: Boston


Snell N *Sams Teach Yourself the Internet in 24 Hours* (2002) Sams Publishing: Indianapolis


**JOURNAL ARTICLES**

Akdeniz Y “Case analysis: Laurence Godfrey v. Demon Internet Limited” 1999 (4) *Journal of Civil Liberties* 260

Arehart B “Regulating cyberbullies through notice-based liability” 2007 (117) *The Yale Law Journal Pocket Part* 41

Bonnici J & de Vey Mestdagh C “Right vision, wrong expectations: The European Union and self-regulation of harmful Internet content” 2005 (14) *Information and Communications Technology Law* 133

Brown B “Fortifying the safe harbours: Re-evaluating the DMCA in a Web 2.0 world” 2008 (23) *Berkley Technological Law Journal* 437


du Plessis G & Viljoen M “Registering domain names” 1998 (6) *Juta’s Business Law* 149

Ebersöhn G “Hyperlinking and deep-linking” 2003 (11) *Juta’s Business Law* 73

Engel “The role of the law in the governance of the Internet” 2006 *International Review of the Law, Computers, Technology* 201

Fee J “Obscenity and the World Wide Web” 2007 (6) *Brigham Young LR* 1691

Fifer S & Carter S “A tale of two safe harbours: The scope of ISP liability and the values of the Internet” 2004 (8) *Journal of Internet Law* 1

Frits E “Internet libel and the Communications Decency Act: How the courts erroneously interpreted Congressional intent with regard to liability of Internet Service Providers” 2004-2005 (93) *Kentucky Law Journal* 765
Hocking A “Selected liability issues: Social networks and blogs” 2009 (12) *The Computer & Internet Lawyer* 12


Kende M “Regulating Internet pornography aimed at children: A comparative Constitutional perspective on passing the camel through the needle’s eye” 2007 (6) *Brigham Young University Law Review* 1623


Leets L “Response to Internet Hate Sites: Is speech too free in Cyberspace?” 2001 (6) *Communications Law and Policy* 287 297

Long D “Electronic voting rights and the DMCA: Another blast from the digital pirates or a final wake up call for reforms?” 2005 (23) *The John Marshall Journal of Computer & Information Law* 533


Nair A “Internet Content Regulation: Is it a global community standard a fallacy or the only way out?” 2007 (21) *International Review of Law, Computers & Technology* 15

Nemes I “Regulating Hate Speech in Cyberspace: Issues of desirability and efficacy” 2002 (11) *Information and Communication Technology Law* 193


Nunziato D “Technology and pornography” 2007 (6) *Brigham Young University LR* 1538

Oppenheimer M “Is the prohibition on virtual child pornography an unjustifiable limitation on the Constitutional right to freedom of expression” 2007 *Responsa Meridiana* 197


Prins J & Schellekens M “Fighting untrustworthy Internet content: In search of regulatory scenarios” 2005 (10) *Information Polity* 129
Romero T “Internet service provider liability for online copyright infringement: The US approach” 2006 (112) Vniversitas 193


SABAM v SA Scarlet District Court of Brussels No 04/8975/A Decision of 29 June 2007, published in Cardozo Arts & Entertainment Law Journal Translation Series #001 (Mady, Bourrouilhou, & Hughes, trans.) Cardozo Arts & Entertainment Law Journal 2008 (25) 1279

Sutter G “Don’t shoot the messenger? The UK and online intermediary liability” 2003(17) International Review of Law, Computers & Technology 73


Urban J & Quilter L “Efficient process or “chilling effects”? Take down notices under section 512 of the Digital Millenium Copyright Act” 2006 (22) Santa Clara Computer & High Technology Law Journal 621

Van Eecke P & Ooms B “ISP liability and the E-Commerce Directive: A growing trend to greater responsibility for ISP’s” 2007 Journal of Internet Law 1

Van Zyl SP “Online defamation: Who is to blame?” 2006 (69) Tydskrif vir Hedendaagse Romeins-Hollandse Reg 139

Van Zyl SP “Sexual Offences and the Internet: Are we ready for 2010?” 2008 (71) Tydskrif vir Hedendaagse Romeins-Hollandse Reg 222

Visser C “A new online service provider liability regime” 2003 (11) JBL 40 40 Watney M “Regulation of Internet pornography in South Africa II” 2006 (69) Tydskrif vir Hedendaagse Romeins-Hollandse Reg 381


Williams KS “Controlling Internet Child Pornography and Protecting the Child” 2003 (12) Information & Communications Technology Law 3

Zarins E “Notice Versus Knowledge Under the DMCA’s Safe Harbors” 2004 (92) Californian Law Review 261

Ziniti C “The optimal liability system for online service providers: How Zeran v. America Online got it right and Web 2.0 proves it” 2008 (23) Berkely Technology Law Journal 583

CONVENTIONS, RECOMMENDATIONS AND DECISIONS

Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (Strasbourg 28 January 2003 ETS no 189)

Convention on Cybercrime (Budapest 23 November 2001 ETS no 185)

Council Recommendation 98/560/EC on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (Official Journal L270 of 7 October 1998)


INTERNATIONAL TREATIES AND COVENANTS

International Covenant on Civil and Political Rights (UN Res 2200A 1966)

International Covenant on the Elimination of All Forms of Racial Discrimination (UN Res 2106 1966)

Universal Declaration of Human Rights (UN Res 217 A 1948)
REPORTS


House of Representatives WIPO Copyright treaties implementation and on-line copyright infringement liability limitation H Rep No 105-551 Part 1 (1998)


Senate The Digital Millenium Copyright Act of 1998-Report S Rept No 105-190 (1998)

Swiss Institute of Comparative Law Legal Instruments for Combating Racism on the Internet (2009)

INTERNET SOURCES


**OTHER DOCUMENTS**


Brooks *Re: Questions relating to ISPA’s take down procedure* (26-10-2009) E-Mail to N.D. O’Brien (copy on file with author)


European Communities *Green Paper on Protection of Minors and Human Dignity in Audiovisual and Information Services* (COM (1996) 483 final)
GN 1954 Notice inviting comment on proposed Guidelines for recognition of Industry Representative Bodies in terms of Chapter XI of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002) GG26768

GN 588 Recognition of the Internet Service Provider’s Association as an industry representative body for internet service provider GG32252