MINOR DISSERTATION TOPIC:

'ENFORCEABILITY OF DIGITAL COPYRIGHT ON THE DARKNET'

Submitted in partial fulfilment of the requirements for the degree

MASTER OF LAWS (Intellectual Property Law)

In the

FACULTY OF LAW

at the

UNIVERSITY OF CAPE TOWN

by

MOSES WANJUKIA MATHINI

STUDENT NUMBER: **MTHMOS024**

SUPERVISOR**: Dr. LEE-ANN TONG**

WORD COUNT: 20,916

Date of Submission**: 06 DECEMBER 2017**

TABLE OF CONTENTS:

Contents

DEDICATION:

I dedicate this dissertation to you and everyone who reads it thereafter after. With the hope that it may be a foundation of better thoughts and illuminating conversations in the jurisprudence of technology law. Go further than the limitations of my mind in this space.

DECLARATION REGARDING PLAGIARISM

I, ***Moses Wanjukia Mathini***, know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own. I have used the footnoting convention for citation and referencing. Each contribution to, and quotation in, this dissertation from the work(s) of other people has been duly attributed, and has been cited and referenced. This dissertation is my own work. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

DECLARATION

Research dissertation presented for the approval of Senate in fulfilment of part of the requirements for the degree of Masters of Law in Intellectual Property Law and a minor dissertation. The other part of the requirement for this qualification is the completion of a programme of courses. I hereby declare that I have read and understood the regulations governing the submission of LLM dissertations, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation conforms to those regulations. I authorize the University of Cape Town to reproduce for the purpose of research the whole or any portion of the contents in any manner whatsoever.

……..

Moses Wanjukia Mathini

Date: 06th December 2017

ABBREVIATIONS & ACRONYMS

COSNU:	Capable of Substantial Non-infringing Uses
CBIs:	Copyright-Based Industries
CAK:	Communications Authority of Kenya
DNS Leak:	Domain Name System Leak
DMCA:	Digital Millennium Copyright Act
DEA:	Digital Economy Act
DNS:	Domain Name System
DRM:	Digital Rights Management System
ECD:	The European E-Commerce Directive
EU:	European Union
EULA	End-User License Agreement
ECT Act:	Electronic Communications and Transactions Act
IP:	Intellectual Property
ISP:	Internet Service Provider
IP address:	Internet Protocol address
KECOBO:	Kenya Copyright Board
OSS:	Open Source Software
OPEN:	Online Protection and Enforcement of Digital Trade Act
OECD:	Organization of Economic Communication and Development
PIPA:	Protection of Intellectual Property Act
P2P network:	Peer to Peer network
SOPA:	Stop Online Piracy Act
SPA:	Software Publishers association
TPM:	Technological Protection measures
US:	United States of America
VPN:	Virtual Private Network
WCT:	WIPO Copyright Treaty
WIPO:	World Intellectual Property Organization

ABSTRACT:

This dissertation seeks to comparatively analyse different emerging jurisprudence of pioneering jurisdictions on the operability of enforcing digital copyright in light of the growing use of the Darknet. It addresses the legal lacuna in the existing copyright laws with regards to enforcement against the illegal distribution of infringing copies of online digital content. It also seeks to illustrate how the concept of digital copyright protection has been compromised by the inoperability of enforcement laws on illegal distribution via the Darknet. It thereby advocates for a 'digital use' exemption and or free access as a recommendation.

Although the advancement of technology created new and advanced forms of distribution or availing copyrighted works to the public, these new advanced channels of distribution have been compromised by rogue online clandestine file sharing networks.

Digital copyright protection laws have been advanced so as to respond to illegal online file sharing, however, they have had limited impact due to the vast, flexible and unregulated nature of the internet which transcends the territorial nature of any single state's copyright laws. Currently, online file sharing is effected through peer to peer networks due to their operational convenience.

This dissertation suggests that the need to control distribution, legally or technological, is driven by the urge to enable digital copyright owners to benefit financially from their works and get a return on their investment. Technologically, this has been effected through the adoption of Digital Rights Management (DRMs) measures that control access to these works through the use of paywalls on commercial websites that require online consumers to pay/ subscribe first before they gain access to the copyrighted works. (eg Netflix, Showmax, itunes e.t.c)

However, since absolute control over one's digital works, online, is impossible, the success of these access-control mechanisms remains debatable and remain vulnerable to technologically sophisticated users who could easily circumvent them and make the protected works available to millions of other users in Darknets. This, in effect, creates a parallel and free market for digital content.

Darknets have grown as the new preferred channel of distribution due to their unique features which have rendered any judicial or legislative threat of sanctions, merely

academic and detached from practical application. The Darknet essentially provides for user privacy, in anonymity, and security from monitoring and detection. These two primary features have exacerbated online piracy as various Darknets ISPs have now developed more user-friendly Darknet versions for the average mainstream user. This dissertation will highlight how the digital creative industry faces an existential threat with the growing use of Darknets.

Darknets have created a virtual environment where illegal digital content distribution continues with impunity, since the burden of the enforceability of copyright rests squarely on the individual copyright holder and the pursuit of liability only begins upon detection of any such infringement of copyright. In effect, copyright owners, most often than not, lack the technological expertise to monitor and detect and thereby cannot enforce their copyright.

As such, this dissertation postulates that the legal/ technological effort to maintain any form of monopoly over digital content online is an unattainable objective. As a solution, to end both online piracy and safeguarding the financial interests of copyright owners, a change in the approach to digital copyright is needed. This will be achieved through creating a 'digital use' exemption and or free access.

Rather than copyright owners trying to control access, they should provide free access and profit on alternative revenue business models. Free access to digital content will do away with the need of online users to pirate and also save copyright owners the effort and resource to keep monitoring the virtual world for infringement. It will also counter-react to the Darknet's parallel market since users will have free access to digital content from the official distribution websites. This dissertation will interrogate the viability of this option.

CHAPTER ONE:

1.1. INTRODUCTION

1.1.1. Background

The ingenuity and evolution of technology has led to the advancement of more sophisticated modes of content distribution so as to cater for the growing insatiable consumer demand for entertainment. As a result, the mode of delivery of musical and cinematographic works has evolved immensely, from limited-capacity, live performance theater halls, to being distributed through recorded mediums such as compact discs (CDs) and now; online 'content-on-demand' platforms that have amplified the potential viewership to a global audience, at the convenience of the user.[1]

In the digital age, increased access to computers and the internet has led, not only to the change in the nature and form of the distribution of copyrighted works, but also, a change in the commercial business models around them.[2] The evolution of these models and modes of content delivery have been consistently designed in order to secure copyright owners' return of investment by controlling content distribution channels and at the same time secure as many viewership as possible.[3]

However, this advancement in the mode of distribution has diminished the capacity of copyright owners to maintain their, once absolute, monopoly over their works. Currently, unauthorized online distribution of digital works, poses a critical existential threat to the digital content industry through the circulation and reproduction of online, digital and infringing copies, on a mass scale. Online digital media content, could arguably be said to have been targeted through their unauthorised communication or availing to the public, due to their high demand.

It is on this premise that the substance of this dissertation challenges the concept of digital copyright protection and avers that technology has eliminated the ability of

---

[1] Deloitte, 'Digital Media: Rise of On-demand Content' < www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-rise-of-on-demand-content.pdf> accessed on 9 October 2017.

[2] M Jaconi in Business Insider, 'The 'On-Demand Economy' is Revolutionizing Consumer Behavior-Here's How' 13 July 2014 < http://www.businessinsider.com/the-on-demand-economy-2014-7 > accessed on 9 October 2017; Jayant Bhargava and Alice Klat, 'Content democratization: How the Internet is Fueling the growth of creative economies' 5 January 2017 < https://www.strategyand.pwc.com/reports/content-democratization > accessed on 9 October 2017.

[3] ibid

digital copyright owners to maintain an economic monopoly over their digital works. As such, it will thereby be advocating for a 'digital exemption use' through open/ free access to digital content as opposed to restrictive business models that only end up competing with parallel 'black markets' operating through advanced clandestine distribution networks collectively known as, 'the Darknet'.

This dissertation will interrogate the commercial relevance of digital copyright protection in light of online infringers who benefit with impunity from anonymity and security from monitoring and detection, in the Darknet. As such, it will illustrate how any judicial or legislative threat of criminal sanctions, thereof, has been detached from practical applicability in the context of South Africa, Kenya, the United States of America (USA) and the European Union (EU).

The fact that the average copyright owner has been left with the responsibility of monitoring and detecting online copyright infringement, has only exacerbated online digital piracy and challenged the essence of copyright in this digital era. The commercial objective of copyright has been described in different theories such as; the fairness theory and the personality theory , as to create a monopoly for the copyright owners to get an opportunity to profit from their work.[4]

The fairness theory states that, the law ought to give authors what they deserve by rewarding their hard work through giving them control of the fruits of their labour.[5] Copyright holders, therefore, should hold the exclusive right to control the distribution and or reproduction of their works, in any manner or form. The personality theory propounds that the authors' emotional bond with their creation should be protected. This includes the right to determine when the work is to be published and collect a fee thereof.[6]

Other commonly referred theories for copyright are; natural rights theory, the incentive theory and the welfare theory.[7] The rights theory postulates that a person who labours on resources that are unowned or held in common has a natural property

---

[4] J Meindertsma, '*Theories of Copyright'* (9 May 2014) < https://library.osu.edu/blogs/copyright/2014/05/09/theories-of-copyright/> accessed on 2 June 2017

[5] ibid

[6] J Meindertsma, (n 4)

[7] S Papadopoulos, S Snail (eds), '*Cyberlaw@SAIII; The Law of The Internet in South Africa'* (Van schaik, Pretoria, 3, 2012) 1; Balangesh, S 'Foreseeability and Copyright Incentives' (2009) 122 *Harvard Law Review* 1569 at 1577.

right to the fruits of their efforts and the state should respect and enforce that natural rights.[8] On the other hand, the incentive theory avers that if authors are incentivised by being rewarded for their works, they will create more.[9] The welfare theory favours the argument that incentives should be balanced so as to make works available for the benefit of the public and advocates for the expiration of exclusive rights.[10] It therefore emphasized on the collective good as opposed to individual interests.

Collectively, these theories have informed copyright law legislation and created exclusive rights for copyright owners. These restricted acts have been considered as the boundaries which determine copyright owners' monopoly during the subsistence of copyright.[11]

1.1.1.1. The nature of digital copyright and its mode of distribution:

The embodiment of digital works differ from their corresponding analogue versions since they are dematerialized and are not contained in tangible form susceptible to all the human senses. However, digital works are represented in material form as binary format (a predetermined sequence of ones and zeros) or digital data and signals which could later be downloaded and reproduced into permanent form by printing or storage on a disk drive.[12]

Dematerialization of the physical embodiment of these works has allowed for the convergence of copyright works into a single work and its subsequent immediate dissemination to millions of others. Digital works, by their nature, are not subject to degradation in quality with each generation of reproduction.[13] They are infinitely renewable, reusable and makes users become producers. Digitization creates a homogeneous medium for the storage and transmission or works.[14]

---

[8] J Hughes, "*The Philosophy of Intellectual Property*," (*Georgetown Law Journal*, 77, 1988) 287, at 299-330

[9] ibid

[10] O Afori, 'Human Rights and Copyright: The Introduction of Natural Law Considerations into American Copyright Law' (2004 14 *Fordham Intellectual Property, Media and Entertainment Law Journal)* 496 at 502.

[11] O Dean, A Dyer (eds), '*Introduction to Intellectual Property Law'* (Oxford University Press South Africa 2014) 33

[12] S Papadopoulos, S Snail (eds), '*Cyberlaw@SAIII; The Law of The Internet in South Africa'* (Van schaik, Pretoria, 3, 2012) 170

[13] A Christie, *'Reconceptualizing Copyright in the Digital Era'* (European Intellectual Property Review 1995, 522) 532; M Bide at al, '*Copyright Clearance and Digitization in UK Higher Education: Supporting Study for the JISC/ PA Clearance Mechanisms Working Party'* <http://www.ukoln.ac.uk/services/elib/papers/pa/clearance/ > accessed on 28 July 2017

[14] ibid

Although the South African and Kenyan Copyright Acts[15] do not have express provisions dealing with digital/ dematerialized works, it could be argued that their provisions do not discriminate as to the form of the works. Digital/ dematerialized forms of copyrighted works therefore are entitled to equal protection.

In South Africa and Kenya, in order for copyright to subsist in a work, it should have; originality, materiality of the work and the author of the work should be a qualified person.[16] The threshold of originality is not necessarily something new, but rather the level of independent skill, judgement and effort exerted, otherwise known as 'the sweat of the brow'. The material form of the works requires only that the work be written down, recorded, represented in digital form or signals or otherwise reduced in material form.[17]

However, exclusive distribution and economic rights thereof, among other rights in copyright works, do not exist indefinitely and are time-limited.[18] Upon the expiry of such term, the work is considered as part of the public domain and no longer subject to copyright restrictions.[19] The limitation of duration of copyright creates the urgency to protect the copyright owners' commercial interests while copyright protection still subsists.

As such, copyright acts as a negative right designed to economically exclude others from benefiting or undermining the copyright owner's legal or financial interests during the subsistence of copyright. Such exclusive rights include; the right to reproduce the work in any manner or form, publication, public performance, broadcast, transmission in a diffusion service and adaptations of the works.[20] The cumulative effect of these exclusive rights remain the foundational structures of the copyright owners' monopoly in the digital economy.

---

[15] O Dean, A Dyer (eds), '*Introduction to Intellectual Property Law'* (Oxford University Press South Africa 2014) 437

[16] Copyright Act No 98 of 1978 (SA), S 2; Copyright Act Cap 130 Laws of Kenya, No 12 of 2001, S22(3)

[17] Copyright Act, (SA), S2(2); Copyright Act Cap 130 Laws of Kenya, No 12 of 2001, S22(3)(b)

[18] S Papadopoulos, S Snail (eds), '*Cyberlaw@SAIII; The Law of The Internet in South Africa'* (Van schaik, Pretoria, 3, 2012) 21

[19] ibid

[20] Copyright Act, (SA), S6, S7, S9

1.1.1.2. Significance of Digital Copyright to the Creative Industry and the Digital Economy:

Copyrighted works are commodities, in an intangible form, distributed, for value, in a controlled fashion, in exercise of an author's substantive rights, to supply an existing demand.[21] The creative industry has grown with the increase in internet access. It has been estimated that as of July 2016, about 3.41 billion people across the globe (46% of the world's population) was an online consumer.[22] Although digital content consumption had always been on the rise, the internet has changed how people consume such content.[23]

Video and musical content in traditional platforms such as satellite and cable TV have increased their viewership by adopting online platforms, and increased its breath of revenue streams.[24] The mode of consumption however has remained in either downloads or online streaming. The growth of the creative industry has also been attributed to digitization of content, high-speed communication infrastructure and significant decline in cost of data storage.[25]

However, unauthorised use could undermine incentives to invest in the creation and diffusion of such works, since rights holders will find it hard to recoup the costs of creation.[26] This interest is pursued through the use of subscription-based-systems, such as paywalls, on access-controlled online platforms. Any copyright system, needs to strike a balance between users' economic rights and public access to the works.

Substantively, both the Kenyan and South African Copyright Act criminalizes the distribution of infringing copies, during the subsistence of copyright in the work, for purposes of trade or for any other purpose, to such an extent that it prejudices the copyright owners' exclusive right to the economic exploitation of their works.[27] This dissertation would show that copyright owners' economic rights can only be realized

---

[21] A Kalvi, '*The Impact of Copyright Industries on copyright Law'* <www.juridicainternational.eu/public/pdf/ji_2005_1_95.pdf> accessed on 9 October 2017

[22] J Bhargava and A Klat, '*Content democratization: How the Internet is Fueling the growth of creative economies*' 5 January 2017 < https://www.strategyand.pwc.com/reports/content-democratization > accessed on 9 October 2017

[23] ibid

[24] ibid

[25] OECD, '*Chapter 5: Copyright in the Digital Era: Country Studies*' <www.oecd.org/sti/ieconomy/Chapter5-KBC2-IP.pdf> accessed on 8 August 2017,

[26] ibid

[27] Copyright Act 98 of 1978 (SA) S27; Copyright Act Cap 130 No 12 of 2001 (Kenya) S35

once the ability to control their digital works' distribution and communication to the public, has been realized.

1.1.1.3. Right to Exclusive Economic Exploitation of Copyright:

The subsistence of copyright in digital content being undisputed, it is the practicality of maintaining an economic monopoly that is challenged in the digital dematerialized environment. The trade of physically-embodied copyright works differs from that of digital dematerialized works in the sense that, the latter works, 'offered for sale', are distributed online only through non-exclusive copyright licenses (End-User License Agreements (EULA)) granting limited exploitation rights, of a reproduction of the work, to a potential 'buyer' or licensee.[28]

Therefore, no contract of sale is concluded and the rights to the digital works are not analogous to the rights a of 'purchaser' of a physical form, of the work, since a digital dematerialized copy of a work cannot be resold.[29] In example, a purchaser of a cinematographic film embodied in a compact disc may resale his copy, however, this may not be possible for an intangible digital copy since it would only amount to generation of further copies of the digital work.

The 'purchaser' of a digital work therefore does not acquire any proprietary interest since ownership is not transferred by the license agreement. Further reproduction or adaptation of a digital work, is prohibited as the license only gives a licensee a non-transferable right to use the digital work as par the license granted.[30]

The answer to the question, whether digital works are subject to exhaustion of economic rights, is fundamental in determining whether an EULA should be qualified as a license or a sale.[31] It is in this respect that digital works differ from their physical versions with respect to the exhaustion of their economic rights.

1.1.1.4. Exhaustion of Economic rights:

Copyright works, in physical form, have long since, had limits on the extent the copyright owner can restrict or control how and where the product is distributed so as

---

[28] O Dean, A Dyer (eds), '*Introduction to Intellectual Property Law'* (Oxford University Press South Africa 2014) 437

[29] ibid 438

[30] ibid 439

[31] *Vernor v Autodesk Inc* 555 F. Supp. 2d 1164

to regulate parallel importation.[32] The doctrine of exhaustion of economic rights (also known as the 'first-sale doctrine') serves to limit the copyright owner's power in controlling the sale of copyright works beyond their initial authorized distribution. However, the direct application of this principle to digital copyright works has however proven challenging and the approach taken by the USA, EU and South Africa differ.[33] Kenya is yet to express any judicial inclination on this issue.

In the USA,[34] the doctrine was said to have originated from the sale of moveable property to prevent anti-competitive behavior through the restriction of further distribution. The first sale or distribution of a work, with the consent of the copyright owner, exhausts his exclusive distribution rights. The application of the doctrine extends to situations where the works have been given away.

Despite the doctrine's notoriety to moveable property, legal pundits have argued for its equal application to copyright works, as a form of property.[35]Courts have shared this opinion by holding that the scope of protection should only extend only so far as the benefits were intended to be granted.[36]This is because the essence of protection is to enable production of copyright for financial gain. Once a copyright owner has received compensation and passed ownership over the work to a purchaser, he has no right to control any subsequent disposal of it.

Exhaustion of economic rights could occur either nationally, regionally or internationally depending on a state's jurisdiction and laws. In South Africa, an interpretation of section 23(2) of the Copyright Act[37] was considered in the case of *Twentieth Century Fox Film corporation v Anthony Black films (Pty) Ltd*[38]. The court held that economic rights of a copyright owner would survive the first sale and it would constitute copyright infringement if a person, without the South African

---

[32] M Owen, '*Exhaustion of rights and digital content'* (November 2013) < https://www.taylorwessing.com/download/article_exhaustion_of_rights.html> accessed on 4 June 2017
[33] S Karjiker, '*The First-Sale Doctrine: Parallel Importation and Beyond'* (2015 Stellenbosch LR 633) < http://blogs.sun.ac.za/iplaw/files/2016/04/The-first-sale-doctrine-Parallel-importation-and-beyond.pdf> accessed on 4 June 2017
[34] *Kirtsaeng v John Wiley & Sons Inc* 2013, 133 S Ct 1351
[35] S Karjiker, '*The First-Sale Doctrine: Parallel Importation and Beyond'* (2015 Stellenbosch LR 633) < http://blogs.sun.ac.za/iplaw/files/2016/04/The-first-sale-doctrine-Parallel-importation-and-beyond.pdf> accessed on 4 June 2017
[36] *Bobbs-Merrill Co v Straus & Another* 1908, 210 US 339
[37] Copyright Act (SA)
[38] 1982 (3) SA 582

copyright owner's permission, either imports an infringing article into South Africa, sells or distributes into South Africa.

In the case of digital works, where a work is downloaded from a foreign location other, than where the reproduction right in the work is held, by a person other than the host of the downloaded reproduction, it would be parallel importation or dealing with grey goods.[39] This parallel trade may decrease the incentive to innovate and diminish copyright holders' capacity to recoup their investment due to the creation of parallel free markets.[40] The above described scenario only emphasizes the need for digital copyright holders to control their exclusive right for reproduction and distribution.

1.1.1.5. Right to reproduction, distribution and communication to the public:

Consumers of digital works are referred to as 'end-users' since the license agreement, granting them a limited right to use, does not grant them a right to dispose of the digital works.[41] Reproduction of digital works under the license is made subject to the condition that possession and use of the works, remains with the end-user.[42]

Although there is no express statutory guidance on what happens upon the termination of the license, it has been suggested that, all digital works, in the possession of the end-user, become unauthorized reproductions or infringing copies of the original.[43] However, mere possession such infringing copies does not constitute actionable infringement of copyright in the work.[44] Since digital copyright laws criminalize the distribution of such infringing copies.

Reproduction in digital works could occur through uploading, downloading of a digital file into a computer's memory or the permanent or transient storage of digital works.[45]However, it is no longer possible to distinguish the digital copying of a work from its distribution nor is it be possible to identify an infringing digital copy from its

---

[39] M Owen, '*Exhaustion of rights and digital content'* (November 2013) < https://www.taylorwessing.com/download/article_exhaustion_of_rights.html> accessed on 4 June 2017

[40] P Cimentarov, *'The Exhaustion of Copyright in the Digital Environment: Are The Rules Suitable to Deal with digitally Transmitted Goods? A comparative Approach between the USA and the EU' (*2010, Ghent University) <https://lib.ugent.be/fulltxt/RUG01/001/786/979/RUG01-001786979_2012_0001_AC.pdf > accessed on 23 October 2017

[41] O Dean, A Dyer (eds), '*Introduction to Intellectual Property Law'* (Oxford University Press South Africa 2014) 439

[42] ibid

[43] ibid

[44] ibid

[45] Art 9 Berne convention; Statement adopted by the WIPO Diplomatic Conference on Certain Copyright and Neighouring Rights Questions (20 December 1996).

quality.[46] To prevent infringement through distribution of digital works, copyright owners have resorted to Digital Rights Management Systems (DRMs).

'DRM' is a collective term refer to technological measures applied to online digital works in order to control their lawful exploitation and prevent or restrict further reproduction or use.[47] DRMs are a form of *ex post facto* copyright enforcement measures that try address the risk of unauthorized reproduction and or distribution of digital works and ensure compliance with the licenses granted. DRMs would include access control or rights control measures such as; content encryption, watermarking and authorization verification measures among others.[48]

Despite the innovative contribution DRMs have made in the fight against unauthorized online file sharing, their effectiveness remain debatable since online piracy still endures unabated. Their continued use by copyright owners has also been challenged due to their inadvertent overreaching technological scope which negatively impacts on end-users' right to fair use of the works.

As a result, the circulation of infringing digital copies online, poses a critical existential threat to the digital content industry on a global scale. It is estimated that billions of dollars of due revenue are lost due to their circulation. This has come to be made possible by Darknets, as intermediaries, which create an enabling environment for piracy and operate from a virtual environment with a global reach into any jurisdiction and without the need of physical presence.

These technological advancements have led to the development of more sophisticated online file sharing platforms/ networks which challenge the ability of the existing copyright enforcement legislations to keep up. Any significant development of the existing legal jurisprudence has been motivated only after judicial intervention.[49] As a result, many legislative interventions have been deprived of any practical capability of enforcement in the digital environment.[50]

---

[46] S Papadopoulos, S Snail (eds), '*Cyberlaw@SAIII; The Law of The Internet in South Africa'* (Van schaik, Pretoria, 3, 2012) 168

[47] O Dean, A Dyer (eds), (n 52) 441

[48] Q Liu, 'Digital Rights Management for Content Distribution' (University of Wollongong School of Information Technology and Computer Science, 2003) < https://dl.acm.org/citation.cfm?id=827994> accessed on 9 October 2017

[49] *A&N Records Inc & Ors v Napster Inc Ors* 2001 239 F 3d 1004 (9th Cir); *Metro-Goldwyn-Mayer Studios Inc & Ors v Grockster Ltd & ors* 2005 545 US 913

[50] Stop Online Piracy Act (USA); Protection of Intellectual Property Act (USA)

The proposed legislations still face glaring jurisdictional limitations since copyright law is territorial whereas the internet remains vastly unregulated and unencumbered by nationality.[51] This, coupled with the existing disparity in states' domestic copyright laws on copyright infringement liability, presents a challenge for the operability of enforcement.[52]Copyright enforcement laws face relevance and practicality challenges on the Darknet since the crackdown on conventional torrent sites has only increased the notoriety of more secured networks, known as the 'Darknet', to copyright infringers.[53] This dissertation seeks to address these shortfalls.

The significance of enforceability in the legislative process cannot be considered as a separate discussion from the threat of sanctions. Emerging jurisprudence on copyright enforcement, after detection, should also provide for measures for detection since existing laws have elaborate sanctions, but are arguably devoid of practical operation. In the event detection remains the central point of failure, consideration should be given on whether a 'digital-use' exemption would solve the problem of online piracy irrespective of the channel of distribution.

This dissertation seeks to address the plight of the copyright holder in their pursuit of the means to enforce their copyright in their online digital works in light of the growing access and use of the Darknet as a digital content distribution channel. It will suggest that this has been defeated or obscured by the need for individual copyright holders to personally enforce their rights in the absence of any online monitoring capabilities. This is due to the fact that the burden of detection of the infringement rests squarely on the individual copyright holder and the pursuit of liability only begins upon the copyright holder being aware of any such infringement.

In light of the above, it could be suggested that, in practice, the concept of digital copyright is a mirage since the continuing advancement of technology only seems to deprive the law any chance of enforcement operability. Despite significant precedents conjured through litigation, to a large extent, on a closer look, these victories are more

---

[51] ibid

[52] H Klopper, T Pistorius, LA Tong et al '*Law of Intellectual Property in South Africa'* (2011 Lexis Nexis) 145; HADOPI of France proposing the 'three strikes' rule

[53] L Edwards, '*Role and Responsibility of the Internet Intermediaries*' 28 May 2010 < http://www.wipo.int/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf> accessed on 9 October 2017.

pyrrhic. This dissertation will highlight how the recent legislative developments to hold 'enabling intermediaries' contributory liable for infringement, have been rendered obsolete by the mutation of online file sharing networks into Darknets.

Online piracy is further limited by the fact that there is no one universal governing law and internet regulation only exists in states' domestic legislation. The lack of a competent legal infrastructure to inform on enforcement practices, coupled with the complacency of developing countries in recognizing and responding to the threat online piracy, gives online pirates the opportunity to take advantage of these 'enabling' jurisdictions by providing safe havens for the unauthorised distribution of infringing copies of digital content.

1.2. RESEARCH FOCUS AND SCOPE

This dissertation comparatively analyses the effectiveness, relevance and practical operability of the USA's Digital Millennium Copyright Act[54], The EU Copyright Directive,[55] South Africa's and Kenya's Copyright Acts[56] as 'yard sticks' in curbing, specifically, the unauthorised distribution of copyright works in digital form. It will thereby advocate for open access or free access to digital content online and a shift in the conventional revenue streams from 'subscription based' to 'ad-based' systems.

1.3. RESEARCH QUESTIONS

a) What is the scope and effectiveness of the existing piracy laws in curbing online piracy on the Darknet?

b) What are the limitations of the existing legal framework entrusted to combat unauthorised/ illegal distribution of copyrighted digital content?

c) What is the future of digital copyright distribution, in light of the growing access and use of the Darknet as an intermediary for online piracy?

1.4. RESEARCH OBJECTIVES

[54] 1998 USA

[55] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society (Information Society Directive or the InfoSoc Directive)

[56] Kenya Copyright Act No 12 of 2001, Cap 130 LOK; South Africa Copyright Act No 98 of 1978

a) To find out whether the development of the digital copyright laws, in 'fore-front' jurisdictions', has made any impact in curbing unauthorised online file sharing or whether it has only increased demand for the Darknet as an alternative superior distribution channel.

b) To interrogate whether or to what extent existing online piracy laws face enforceability challenges on the Darknet.

c) To show how ISPs' 'internet policing' through online monitoring of web traffic on behalf of IP rights' holders, infringes on users' right to privacy.

d) To find out whether the pursuit of the enforcement of an economic monopoly over digital works is an effort in futility and whether copyright holders could pursue other alternatives revenue streams.

1.5. HYPOTHESIS

a) Digital content distribution has been effected through access-control paywall TPMs that enable content creators restrict access and maintain an economic monopoly thereof.

b) These TPMs remain susceptible to circumvention, and as such, absolute distribution and economic monopolies are compromised in the long run.

c) Online infringers have been motivated to use Darknets, as a preferred superior distribution network, in order to escape liability for copyright infringement.

d) The internet remains vastly unregulated as there is no universal law that governs it. Any such existing framework only exists through pieces of domestic legislations that are limited by their territorial jurisdiction.

e) Any form of state regulation through ISPs has been met with resistance from privacy activists since they require ISPs to monitor each online user's web traffic hence violating the users' right to privacy.

f) The general obligation of detection and monitoring infringement, having been left to content creators, has compromised digital copyright enforcement due to the lack of technological capacity to monitor activities in the Darknet.

g) Digital copyright holders could still get a return on investment and attain commercial success by adopting an open/ free access, online and ad-based business model as opposed to a 'subscription-based' model with restricted access to digital content.

1.6. METHODOLOGY

The thesis has used legislation from the USA, EU, South Africa and Kenya for primary sources. It has referred to provisions of International Legal instruments of the EU and WIPO as well. It has relied on academic articles and other relevant literature obtained from journals, reports and internet sources.

1.7. CHAPTER BREAKDOWN

1.7.1. CHAPTER ONE:

This is an introductory chapter into the dissertation topic. It establishes the nature of digital copyright and its mode of distribution or conveyance to the public. It highlights the copyright holders' exclusive right of economic exploitation as dependent on their ability to control the distribution or conveyance of their works to the public. It avers that absolute control of access to online digital content is an unattainable objective and susceptible to circumvention and further distribution in the Darknet. It thereby proposes open/ free access business model as opposed to a 'subscription-based' model with restricted access to digital content.

1.7.2. CHAPTER TWO:

This chapter focuses on the nature and impact of the illegal distribution of online digital content in the Darknet and the relevance and inadequacy of current legislative frameworks in curbing the same.

1.7.3. CHAPTER THREE:

This chapter highlights the evolution of the different modes of copyright enforcement in response to development in technology advancements. It seeks to interrogate and evaluate the effectiveness of the various law enforcement practices currently being implemented in the US, EU, Kenya and South Africa, and assess their relevance to the Darknet.

1.7.4. CHAPTER FOUR:

This chapter interrogates Darknet intermediaries under various developed immunity regimes recognized in USA, the EU, South Africa and Kenya and whether they could be held liable as enablers for copyright infringement. It will focus on the 'TOR

Browser' as a case study and analyse whether it could be deemed as capable of non-infringing use despite its notoriety as a Darknet intermediary.

1.7.5. CHAPTER FIVE:

This chapter will advocate for 'digital exemption use' as a solution to copyright owners' present dilemma in their inability to monitor and detect illegal online content distribution of their works in the Darknet. It will motivate this recommendation by encouraging open/ free access, online and ad-based business model as opposed to a 'subscription-based' model with restricted access to digital content. Copyright owners will be alleviated from the burden of trying to monitor and control the internet and would also get a return of investment from the digital traffic in their website.

CHAPTER TWO:

2.1. PARALLEL DIGITAL CONTENT DISTRIBUTION IN THE DARKNET

2.1.1. The Evolution of Parallel Free Markets into Darknets:

It can be assumed that only those copyrighted works which are offered for value, in access-controlled sites, are the ones that are subject to online piracy since other digital content is available for free. Also, in light of the homogenous nature of all digital works and the similarity of their business revenue models, they are all subject to the same form of parallel distribution and therefore can be referred to, collectively and without discrimination, in this dissertation.

It is on this premise that legitimate online digital content distribution enterprises try and enforce their exclusive distribution rights since otherwise they would have to compete with the free parallel distribution of their works occurring in illegal distribution networks.

The South African Copyright Act distinguishes copyright infringement into direct (primary) infringement and indirect (secondary) infringement. Direct infringement is whereby, 'any person, other than the copyright owner and without the licence of the copyright owner, does or causes any other person to do, any act, which the copyright owner has the exclusive right to do or to authorize'.[57]Such acts, include reproduction of the copyright work.

Indirect infringement occurs where a person *knowingly* deals with infringing articles by either;

> [I]mporting into the republic for purposes other than for his private and domestic use; sells, lets or by way of trade offers or exposes for sale or hire, distributes for the purpose of trade, or for any other purpose, to such an extent that the owner of the copyright in question is prejudicially affected; or acquires an article relating to a computer program in the Republic.[58]

[57] Copyright Act, (SA), S23(1)
[58] Ibid S23(2)

Similar substantive provisions exist in the US' DMCA and Kenya's[59] Copyright Act. In the digital environment, any form of 'resale' or giving away of digital content would constitute an infringement since it would be merely creating and giving of a copy. This will amount to reproduction of the copyrighted work since reproduction would entail, the making of copies of protected works in any manner or form.[60] Indirect infringement would occur where a person deals with the infringing articles by distributing them online.

Digital dematerialized content eligible for copyright should enjoy the same standard of protection offered to their physically embodied versions.[61] However, the internet provides an efficient, simple and readily available means of infringing copyrighted works in digital form.[62] Consequently, billions of dollars of due revenue are lost due to the creation of virtual parallel free markets on an exponential global scale. Digital content development, distribution infrastructure technology and entertainment companies have been adversely affected and their business models severely challenged by illegal parallel distribution in the Darknet.[63] Both established and emerging legitimate businesses remain threatened since consumers have become competing publishers and distributors, of their content, for free.[64]

Digital content distribution differs greatly from the distribution of physically embodied copies of copyrighted works since their distribution is not confined to physical means.[65] This has been exacerbated by the fact that it takes only one uploaded file on the internet to serve as a template for perfectly identical and unlimited reproductions for subsequent downloaders. Each subsequent downloader could then, in turn, further distribute the work by uploading onto other networks creating infinite reproductions thereof.

It is therefore necessary to understand how digital content distribution has evolved overtime and inadvertently creating parallel fee markets which challenge copyright

---

[59] Copyright Act, Cap 130 Laws of Kenya, S 35
[60] O Dean, A Dyer (eds), '*Introduction to Intellectual Property Law'* (Oxford University Press South Africa 2014) 34
[61] ibid
[62] ibid
[63] D Choi, A Perez, 'Online Piracy, Innovation and Legitimate Business models' April 2007 < http://www.sciencedirect.com/science/article/pii/S0166497206001040> accessed on 9 August 2017
[64] <www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf> accessed on 10 August 2017
[65] Ibid 417

enforcement by their network topologies. Online file sharing is primarily done through Peer to Peer (P2P) networks. P2P networks allow for the direct distribution of information among users without the need for a central storage.[66] In these networks, a user's computer acts as both a client computer and a server thereby enabling the direct communication with other computers hence the classification as a distributed network.[67] The digital content is stored on the respective users' computers reducing the intermediary's online platform to a mere connecting bridge between the computers.[68]

This has differed from conventional file sharing systems which required the use of websites which provided for an indirect file sharing system.[69]Computers connected to the internet used to communicate to each other using standard protocol guidelines. Internet Protocol (IP) addresses that identify each computer on the internet could then be converted into recognizable names for the transmission of data. Files and other digital content were stored on central servers.[70]

Availability of content in P2P networks depends on contemporaneous files on the network users' computers. Online intermediaries provide only the software application used to establish the network connection. The software application retrieves the IP addresses of other available users and creates a direct connection with other users looking for similar files.[71]

Basic P2P network designs facilitate the input of new content into the network, the distribution of copies of the content to other users and a search mechanism that enables other users to find desired content stored in the network.[72] They are

---

[66] J Wood, '*The Darknet: A Digital Copyright Revolution*'(2010) < http://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1330&context=jolt> accessed on 9 October 2017

[67] S Androutsellis- Theotokis & D Spinellis, *A Survey of Peer to-peer Content Distribution Technologies, 36 ACM Computing Surveys 335, 335-36 (2004)*

[68] A Jacover, *I Want My MP3! Creating a Legal and Practical Scheme to combat Copyright Infringement on Peer-to-peer Internet Applications,* 90 Geo. L.J. 2207, 2208 (2002)

[69] Ibid 4

[70] J Wood, '*The Darknet: A Digital Copyright Revolution*' (2010) < http://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1330&context=jolt> accessed on 9 October 2017

[71] ibid 5

[72] Peter Biddle et al, '*The Darknet and the future of content distribution'* 2 (2002) < http://msl1.mit.edu/ESD10/docs/Darknet5.pdf> accessed on 29 June 2017

economically efficient since users donate their own computer as storage space and distribution networks which are scalable.[73]

Due to P2P network's convenience for digital file sharing, unauthorised file sharing has grown on an unprecedented scale provoking a concerted response from the digital content industry. The insatiable demand for digital content makes its distribution inevitable since consumers, who are also suppliers, provide a ready market and have full control on what content to share.[74]

The first generation of P2P networks/ intermediaries such as the defunct 'Napster', provided a centralized index of all the files stored and available for download. This provided convenience in the efficiency in which users could search for files. It was on this basis that Napster was found contributory and vicariously liable for infringement of copyright.[75]

The second generation of P2P intermediary eliminated the dependence of a centralised index and instead had each user maintain an index of only those files stored on their computer. Users would then trace a desired filed by sending out requests to other users of the P2P software until it received a positive response. The P2P software negotiates the files' download between the computer with the file ('seeder') and the one that made the request ('leecher').[76]

This model was adopted by intermediaries such as 'Gnutella', 'KaZaA' and 'Grokster'. The third generation, a slight variation of the second generation, used a number of user computers called 'supernodes' to act as servers which hosted sub-indexes of the files and thereby improving on the networks efficiency.

A fourth generation popularly known as the 'BitTorrent' approach emerged with a different network topology. Its users would be able to download a file, not just from one identified source, but from several sources having the same file.[77] The desired

---

[73] N Elkin-Koren, '*Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic' (*9 NYUJ, Legis & Pub, Poly 15, 22, 2006)

[74] J Wood, (n 86) 9

[75] *A&N Records Inc & Ors v Napster Inc Ors* 2001 239 F 3d 1004 (9th Cir)

[76] L Edwards and C Waelde , *'Online Intermediaries and Liability for Copyright Infringement* ' 8 < https://www.google.co.za/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjO1pfnwuPWAhWXHsAKHZCKAXIQFggmMAA&url=https%3A%2F%2Fwww.era.lib.ed.ac.uk%2Fbitstream%2Fhandle%2F1842%2F2305%2Fwipo-onlineintermediaries.pdf%3Fsequence%3D1%26isAllowed%3Dy&usg=AOvVaw0NtRZXEY5BhAKnvliYzUI6> accessed on 9 October 2010

[77] J Wood, (n 86) 5

file would be split into parts, each of which could be transferred and downloaded independently.[78] This improved the speed of transfer of files by distributing the burden of a single source, to several other sources.

In effect, this made it difficult to identify any one file's source as having been derived from a particular computer/ user and thereby complicating the attribution of liability for infringement.[79] After downloading the file, users have an option of leaving the file available for others to download from them, as a source ('seeding'). This has substantially affected the effectiveness of anti-piracy response measures such as domain take down or access blocking since users would still be able to gain access to the files without the website.[80]

Successive generations of P2P networks have mutated into open source protocols which essentially enable anyone to recreate the same software application and become its operator. This frustrates any potential suite since anyone could become an operator and the program could be replicated and implemented to keep the network functioning.[81]The growing illegalization of the peer to peer file sharing networks has however, resorted many torrent networks to seek refuge in the Darknet.[82]

2.1.2. The Rise of the Darknet:

The Darknet could be defined as an overlay network, ranging from, small file sharing networks to elaborate exclusive cyber clubs, accessed only by specific software, configurations, or authorizations, mainly using non-standard communication protocols usually in the form of peer to peer platforms and accessed through clandestine networks such as 'The Onion Router (Tor) project'[83] and 'I2P'[84].[85]

The etymology of term 'Darknet' is attributed to the influential paper titled *The Darknet and the Future of Content distribution.* It has also gained notoriety as virtual safe havens clear of legal restrictions imposed by the entertainment industry.[86] It also

---

[78] ibid
[79] L Edwards, (n 92) 9
[80] ibid
[81] J Wood, (n 86) 14
[82] ibid
[83] The Tor Browser Bundle, 'What is Tor Browser' < https://www.torproject.org/projects/torbrowser.html.en> accessed on 20 April 2017
[84] I2P, 'What does I2P do for you?' < http://getit2p.net > accessed on 20 April 2017
[85] J Wood, (n 86) 14
[86] JD Lasica, '*Darknet: Hollywood's War Against the Digital Generation'* 264 (John Wiley & Sons Inc 2005)

offers a secure, private and anonymous environment and promotes itself to consumers by directing online users to the Deep Web via social media, websites, mobile apps, page searches, page search ads and phishing or spam emails.[87]

Due to its level of technological sophistication, the Darknet has also gained notoriety for the commercialization of counterfeit drugs, stolen goods, assassins for hire, child pornography, arms trafficking, animal cruelty and human medical experimentation and the sale or distribution of proprietary information and files of copyrighted works.[88]

The rise of the Darknet's usage has been attributed to the development of stringent copyright liability laws and data management tools which in effect force consumers into the Darknet.[89]Consequently, it has been argued that monopoly of copyright is no longer practical in the digital realm due to the inability to enforce copyright over online digital works.[90]

2.1.3. Illegal Parallel-Distribution of Digital Content on the Darknet:

Despite successive generations of P2P networks managing to shift control away from ISPs, they failed to secure the anonymity of their users and risk of prosecution.[91] In effect, server endpoints could be determined, revealing users' IP addresses and thereby making it possible to track, identify and prosecute individual infringers.[92] The threat of liability created a demand for distributed networks that offered anonymity, privacy and increased security. These improved networks are what constitutes the Darknet today.[93]

The evolution of these online intermediaries has greatly been influenced by the desire of self-preservation from the threat of legal liability.[94]Consequently, enforcement of digital copyright has been considered impaired since the detection or identification of

---

[87] The deep web, Darknets, bitcoin and brand protection < http://www.worldtrademarksview.com/intelligence/online-brand-enforcement/2016/chapters//the-deep-web-darkness-bitcoin-and-brand-protection-2 > accessed on 1 April 2017

[88] M Chertoff and T Simon, '*The impact of the dark web on internet governance and Cyber security'* (CIGI 2015) < chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf > accessed on 17 April 2017

[89] ibid

[90] J Wood (n 86), 16

[91] ibid

[92] ibid

[93] ibid

[94] L Edwards, (n 92) 9

the direct infringers and their infringing activity has been frustrated by the encryption and anonymity features the Darknet provides. This renders any legislated sanctions unimplementable since identification of infringers is vital for any viable enforcement of copyrights through law suits and criminal sanctions thereof.[95]

Anonymity-aiding-devices such as Virtual Private networks (VPNs) or Darknets such as the 'Tor Router', deprive copyright holders, knowledge of any ongoing infringement since they hide infringers IP addresses making their identification nearly impossible and their infringing activity, virtually untraceable.[96]

Normally, users who desire to connect to the internet, first connect to their ISP who then would connect them to any websites they would like to visit. This allows ISPs to monitor online users web traffic and trace it back to a user's IP address and identify him/ her.

The 'TOR Browser' redirects users' internet traffic, disguising where their computer, phone or other device is when it makes contact with websites. It also encrypts information sent across the internet, making it unreadable to anyone who intercepts your traffic including ISPs.[97]It creates the impression that the user is accessing the internet from the IP address of the VPN service provider.[98] It has gained notoriety for evading censorship by ISP and governments and facilitates secure P2P downloading.[99]

This presents a challenge in the fight against online piracy since the burden of detection of the infringement rests squarely on the individual copyright holder and the pursuit of liability only begins upon the copyright holder being aware of any such infringement.[100]

---

[95] J Wood (n 86), 24

[96] Longworth '*The Possibilities for a legal framework for cyberspace-including a New Zealand Perspective'* in Fuentes-Camacho (ed) Law of Cyberspace Series volume 1: The international Dimensions of Cyber Space Law (2000) 9 9; Powers The internet Legal Guide: Everything you need to know when doing business online (2002) 1-3; Nel '*Freedom of expression and the internet'* in Buys (ed) Cyberlaw @SA II: The Law of the interne in South Africa 2 ed (2004) 197.

[97] L Hautala, '*A VPN can Protect your online Privacy but there is a Catch' 29* March 2017 <https://www.cnet.com/news/vpn-protect-online-privacy-its-complicated/> accessed on 02 August 2017

[98] ibid

[99] D Crawford, '*VPNs for Beginners- What you Need to Know'* 20 January 2016 <https://www.bestvpn.com/vpns-beginners-need-know/> accessed on 2 August 2017

[100] ECD Art 15

Detection, itself, requires a certain level of monitoring of web traffic in real time, a task of which, ISPs have described as near impossible.[101] Monitoring of Web traffic has also faced opposition by privacy advocates who consider any form of cyber surveillance as a violation of users' right to privacy.[102] The above described situation, leaves most digital copyright holders vulnerable and ill-equipped to curb the unauthorized distribution of their digital content.

Online piracy, through the illegal distribution of digital content, remains a vibrant virtual business model since their online platforms, such as torrent sites, are designed to financially benefit through online ad-based revenue business models that grant free access as opposed to the mainstream conventional websites that control access through paywalls. The ad-based revenue model is dependent on only users' web traffic, on a per-view or per-click basis for every unique user. Therefore, one need not download from a pirate site so to financially support it, loading onto the web page is sufficient.[103]

In the advent of open source protocols establishing such networks, Darknets have been used to establish safe havens for illegal file sharing which act as closed off virtual spaces free from the restrictions imposed by copyright legislations.[104] Earlier versions of Darknet applications were only operable to technologically sophisticated users, however, more commercially viable and user-friendly versions are being made available in the mainstream market for the average user.[105]

Illegal distribution of digital content, on conventional P2P networks and the Darknet has made many digital copyright owners to consider adopting distribution rights control measures otherwise known as Digital Rights Management systems (DRMs) or Technology Protection Measures (TPMs). An analysis of the circumvention of these TPMs is necessary since it is only upon acquiring access to digital content that infringers are then capable of illegally distributing them via the Darknet.

---

[101] E Duah, '*Internet Service Providers' Monitoring Obligations'* (2013) < chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://journals.muni.cz/mujlt/article/download/2605/2169> accessed on 9 October 2017

[102] ibid

[103] ibid

[104] J Wood, (n 86) 17

[105] ibid 20

2.1.4. Circumvention of TPMs as a precursor to illegal distribution in the Darknet:

Access to online digital content can be obtained legitimately through licences or illegally, through the circumvention of TPMs. Although, in both instances, copyright infringement occurs upon further distribution of the article, it is necessary to interrogate how the user came into the possession of the content, since its only upon access to the digital content, that subsequent distribution becomes possible.

Most online copyright-based business models rely on the internet for content delivery, and has been driven primarily by the improved portability and demand for digital content.[106] The demand for digital content from download and or streaming platforms, inspired the development of subscription-based revenue business models (total paywalls). This is where access to content is restricted until payment, to where access is unrestricted and is generated through alternative means such as ad-based models and for, so as to generate revenue.[107]

The law came to the aid of copyright owners who adopt such types of TPMs in their works by criminalizing the circumvention of TPMs. However, it is debatable on whether this should extend to the prohibition of circumvention devices or just punish the conduct of the infringer. Different approaches have been adopted by USA, EU, Kenya and South Africa.

In the USA, section 1201 of the Digital Millennium Copyright Act (DMCA)[108] penalizes the circumvention of TPMs that control access to copyright works. It also prohibits the manufacture, dissemination or offer of ***devices*** or ***services*** that circumvent access control or devices that circumvent a TPM that effectively protects a ***right*** of the author.[109]

Culpable circumvention of a technological measure has been elaborated to include; descrambling a scrambled work, decryption of an encrypted work, or otherwise to avoid, bypass, remove deactivate, or impair a TPM.[110]

---

[106] OECD, '*Chapter 5: Copyright in the Digital Era: Country Studies*' <www.oecd.org/sti/ieconomy/Chapter5-KBC2-IP.pdf> accessed on 8 August 2017
[107] Ibid 19
[108] Digital Millennium Copyright Act (DMCA) (17 U.S.C.) USA
[109] ibid
[110] Ibid section 1201(a)(3)

The Act,[111] criminalises the importation, offering to the public, trafficking of any technology, product, service, device or component that is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to, or effectively protects a right of a copyright owner, in protected work and has a limited commercially significant purpose or use other than to circumvent such TPMs; or is marketed as such.

The Directive 2001/29/EC of the European Union Parliament and the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society (the Information Society Directive), obligates member states to protect against circumvention of effective TPMs which the person concerned carries out in the actual or constructive knowledge of pursuing that objective.[112]

Similarly, article 7 of the EU Computer Programs Directive obliges member states to provide appropriate remedies against any person committing 'any act of putting into circulation, or the possession for commercial purposes of any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may be applied to protect a computer program'. However, if the device has multiple uses other than for unauthorized circumvention, it is not prohibited.[113]

Similarly, South Africa's, section 86 of the Electronic Communications and Transactions Act[114] (ECT Act) and section 35(3) of the Kenyan Copyright Act,[115] have substantively similar provisions with the exception that the ECT Act expressly includes computer programs designed primarily to overcome security measures for the protection of data.

The resort to DRMs as a pre-infringement enforcement tool to control online digital content distribution has been criticised as futile against Darknets, and likened, in analogy, as a rearrangement of deck chairs on a sinking ship.[116] Circumvention of

[111] S1201 (a)(2), S1201 (b)(2) DMCA
[112] Art 6.1 Directive 2001/29/EC of the European Union Parliament and the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society (the Information Society Directive)
[113] M Conroy, '*A Comparative Study of Technical Protection'* 2009< http://uir.unisa.ac.za/bitstream/handle/10500/2217/thesis.pdf;sequence=1> accessed on 9 August 2017
[114] No 25 of 2002, SA
[115] Cap 130, 2001
[116] J Wood, (n 86) 23

TPMs in physically-embodied copyrighted works, would have required each user to circumvent. However, in the digital environment, not every user needs to circumvent a TPM as it would only take just the first sophisticated user to do it, and thereafter make the copy available for the rest in the Darknets.[117]

Fred von Lohmann in *'Measuring the Digital Millennium Copyright Act Against The Darknet: Implications for the Regulation of Technological Protection Measures'*[118] notes that after the legislation of the DMCA, it has yet been evaluated whether it has delivered on its pre-legislative intent or if it has destabilized the balance between copyright owners and the public interest.[119] He argues that the Act has extensive unintended consequences and infringes on free speech, competition and innovation. Proponents of DMCA argued that copyright owners were not willing to make their works available online without TPMs, in light of the risk posed by digital piracy. The Act's pre-legislative intent was to encourage the use of TPMs such as Digital Rights management (DRMs) technologies by creating sanctions against those who created circumvention tools available to consumers.

The same criticism could be extended to the anti-circumvention provisions of the Kenya Copyright Act which does not provide for lawful circumvention of TPMs.[120] This omission impinges on users' right to make backup copies of digital works or transfer the copies to their other devices for private use as part of fair use.[121]

Anti-circumvention provisions were not intended to prevent the average consumer from evading them and keep circumvention tools out of the mainstream market.[122] This has been criticised as an objective targeted to only the technically

---

[117] Symposium, *At the Crossroads of law & Technology: fifth Annual conference, Alternative Methods for Protecting Digital content*, 25 Loy. L.A ENT. L. REV. 63, 67 (2004)
[118] F von Lohmann, *'Measuring the Digital Millennium Copyright Act Against The Darknet: Implications for the Regulation of Technological Protection Measures (*Loyola of Los Angeles Entertainment Law Review, 2004) <http://ditigalcommons.lmu.edu/elr/vol24/iss4/4> accessed on 27 May 2017
[119] Ibid 636
[120] Copyright Act Kenya S 35(3)(a)
[121] ibid S 26(1) (a)
[122] F von Lohmann, *'Measuring the Digital Millennium Copyright Act Against The Darknet: Implications for the Regulation of Technological Protection Measures (*Loyola of Los Angeles Entertainment Law Review, 2004) <http://ditigalcommons.lmu.edu/elr/vol24/iss4/4> accessed on 27 May 2017

unsophisticated users and presumes their continued ignorance in the advancement of user friendly circumvention tools.[123]

Another reason in support, was to create a technological 'speed bump' that although, not impervious to technically sophisticated users, it would be enough to subdue the average user to only make authorised uses of the works.[124] However, this has, in effect, only created scarcity of supply and thereby fuelling consumer demand and resorting users to get works from unauthorized sources.

It has been argued that by the time of DMCA's legislation, it was already surpassed by technological advancements and their widespread availability.[125]The drafters failed to anticipate developments in the digital distribution technologies that today challenge the operability of the enforcement of TPMs on digital copyrighted works. According to *'The Darknet and the Future of Content Distribution',* it makes three assumptions, namely; 'that any widely-distributed object will be available to at least a fraction of users for copying, users will copy the object if possible and interesting to do it and users are interconnected through high-bandwidth channels.'[126]

The Darknet qualifies on the first assumption by virtue of the fact that, no TPM is yet to be invented that is invulnerable to technologically sophisticated users. Any TPM is rendered redundant once it is compromised by any sophisticated user, and thereby made available to other users who have the desire and capability to mass distribute it. As long as the average user has access to sufficiently effective Darknets, they would not need to access circumvention tools and thereby defeating the objective of any TPM legal regime.

The recognition of small world networks through networks that fall under the 'safe habour' regimes to some extent facilitate the distribution of copyrighted material since they are only required to attempt to self-regulate through notice and take down requests and not obliged to seek out infringing activities.[127]

---

[123] ibid
[124] ibid
[125] Ibid 640
[126] P Biddle, P England, M Peinado & B William, *The Darknet and the Future of Content Distribution,* Microsoft Corporation <http://msl1.mit.edu/ESD10/docs/Darknet5.pdf > accessed on 25 May 2017
[127] ibid

Scientific surveys estimate that the continued exponential growth in use of the Darknet will result into the Darknet becoming a preferred alternative and substantial competitor to legal commerce in digital content distribution.[128] Darknet files will come off as free alternatives, of equal quality, to those offered in the mainstream sites that are encumbered with paywall TPMs. It could therefore be argued that, circumventing a rights' or access control TPM and subsequently uploading the protected item, amounts to a communication to the public.

2.1.5. Infringement through Communication to the Public via Darknets:

Copyright in literary, artistic, cinematographic (audio-visual) works and musical works reserves copyright owners, the exclusive right to communicate the whole or a substantial part of their works, to the public.[129] Recently, the European court of Justice (CJEU) in the case of *Stichting Brein v Ziggo and XS4ALL,*[130] ruled that operators of online platforms cannot escape liability since they play an essential role in making such protected works available to the public.[131]

Therein, the Court had been referred, a preliminary reference, from a Netherlands National Court, to consider whether sharing platforms, such as Pirate Bay, could be deemed as 'communicating to the public' under the EU Copyright Directive. The court ruled that, any act which a user, with full knowledge of the relevant facts, provides access to protected works, is liable for communicating the works to the public. Uploaded works in such P2P networks were being made available to users in such a way that they could be accessed from wherever and whenever users choose.

The Court held that an 'act of communication' and the communication of a protected work to a 'public' are interdependent. In determining the existence of an act of communication, it will depend on whether the user has played an indispensable role through a deliberate intervention, with full knowledge of the consequences of their action in giving access to other persons who would not otherwise have been able to enjoy it. Although individual users are responsible for uploading of digital works on

---

[128] P Briddle et al, (n 23) 14

[129] Art 3(1) EU Directive 2001/29; S26 Copyright Act, Cap 130 Laws of Kenya; S6(c), 8(1)(b), 9(e) Copyright Act 98 of 1978 SA

[130] C-610/15 14 June 2017

[131] C Angelopoulos, '*CJEU Decision on Ziggo: The Pirate Bay Communicates Works to the Public'* 30 June 2017 (CIPIL, University of Cambridge) < http://copyrightblog.kluweriplaw.com/2017/06/30/cjeu-decision-ziggo-pirate-bay-communicates-works-public/> accessed on 14 August 2017

the network, the management of the online platform amounted to an intervention in providing access to protected works in full knowledge of the consequences.

The Court also determined that a 'public' refers to a group of people of an indeterminate number that is of a certain, but not insignificant, size. It was irrelevant whether the audience were reached simultaneously but instead, the cumulative effect of making works available to a large number of people in succession is what should be considered. It is also necessary that the public be a 'new' to the extent that they were not contemplated by the copyright holder or that the later communication took place through different technical means from those which were authorized at the initial communication of the work to the public.

It is noteworthy to point out that, the South African Copyright Amendment Bill 2017, specifically provides that communication to the public to includes making it available on the internet as well.[132] From the forgoing, Darknet users create parallel markets through the circumvention of paywalls and subsequent distribution digital content online. It is at this point that the operability of detection and deterrence of this infringement, provokes interrogation.

[132] Clause 8 (1)(d) Copyright Amendment Bill SA 2017

CHAPTER THREE

3.1.OPERABILITY OF DIGITAL COPYRIGHT ENFORCEMENT IN THE DARKNET

3.1.1. The Role of Enforceability in Law

The diminished technological capacity of copyright owners to maintain any monopoly over their works through the control of the access and or distribution of their works has been amplified by the disconnection between legislative intent and effecting sanctions in regard to illegal content distribution in the Darknet. This has begged the question whether copyright over digital works can be enforced.

John L Austin's theory of law opines that 'enforceability' is a necessary condition for any rule of law to be distinguished from a mere expression of desire for compliance.[133] 'Law should be operable to the extent that there is a sufficiently high degree of conformity.'[134] Conformity is achieved, not only through the threat of sanctions in effort to coerce obedience, but by also depriving its subjects of the opportunity and capacity to break the law.[135] The objective of a system of enforcement is to ensure a high degree of conformity to the law, any less and it has failed despite its attributed value or moral beauty.[136]

However, the threshold of the degree of conformity is not as to determine the success of the system of law but rather the existence of it.[137] The application of this legal principle in light of technological developments in content distribution, tests the operability of digital copyright law in light of the Darknet's technological features.

Although copyright infringement laws have developed primarily in response to the ingenuity of online infringers' attempt to evade liability, the success of their enforcement initiatives have always been dependent on detection of infringement, at the distribution level. As such, the development of liability laws has inspired the innovation of successive generations of distribution networks that exist to provide anonymity and security from detection.

---

[133] F S McNeilly, '*The Enforceability of Law*' (Nous Vol 2 No 1 Feb 1968) < http://www.jstor.org/stable/2214413 > accessed on 23 April 2017

[134] ibid

[135] Ibid 44

[136] Ibid 48

[137] Ibid 49

Over time, in each successive litigation, copyright owners have moved from suing individual infringers to distribution networks, as intermediaries, deemed as active enablers. This has majorly been driven by then need to find the most cost effective and durable solution in ending illegal distribution of digital content online.[138] The application of these modes of enforcement is worth interrogating in light of the Darknet.

3.1.2. Operability of Suing Individual Distributors in the Darknet.

Enforcement of Copyright law begun by suing individual infringers for direct infringement in conventional distribution networks.[139] However, litigating against individual users in most countries has been a measure of last resort due to its impact on an organization's public relations. In South Africa, the *S v Norton* (*Four Corners Case)*[140] is the first and only conviction of an individual copyright infringer. Therein, the defendant had been accused of copyright infringement by uploading a copy of a local movie titled, 'Four corners', on 'Pirate Bay'. The Court sentenced him to a 3-year suspended sentence. However, this was only after the defendant himself had admitted to pirating the movie on social media.[141]

Threats of litigation as a scare tactic to individual infringers have not deterred their infringing activities but only created the need for online user anonymity. In 2008, the Recording Industry Association of America (RIAA) declared that it will no longer depend on suing individual infringers but rely on ISP cooperation.[142]

This change in law enforcements' tactics has been attributed to its susceptibility to error. There were reported cases where deceased people or senior citizens ignorant of technology have been set up as scape goats by scrupulous infringers.[143] Also, the

---

[138] L Edwards, *Role and Responsibility of Internet Intermediaries In the Field of Copyright and Related Rights*

[139] *A&M Records v Napster* 239 F d3 1004 (US), 2 October 2000

[140] Unreported (SA)

[141] IP Unit, University of Cape Town, 'Our Views Regarding the "Four Corners" Piracy Case Sentence' 23 April 2014< http://www.iplaw.uct.ac.za/news/our-views-regarding-%E2%80%9Cfour-corners%E2%80%9D-piracy-case-sentence> accessed on 9 August 2017

[142] Anderson N, 'No more lawsuits: ISPs to work with RIAA, cut off P2P users, <http://www.arstechnica.com/tech-policy/news/2008/12/no-more-lawsuits-isps-to-work-with-RIAA-cut-off-P2P-users.ars.> accessed on 9 October 2017

[143] Yu P, 'the Graduated Response', (2010), 62, 16-17 Florida Law Review, <http://www.papers.ssrn.com/sol3/papers.cfm?abstractid=1579782 > accessed on

prescribed punitive measures thereof for copyright infringement under many jurisdictions have been described as disproportionate and draconian.[144]

Further, imposing liability for copyright infringement only begins with detection of infringement.[145] However, since detection, even on conventional networks and websites, depends heavily on copyright owners conducting some form of online monitoring, it has been met with resistance from online privacy activist condemning any form of cyber surveillance.[146]

In Kenya, police officers or inspectors of the Kenya Copyright Board (KECOBO) have the power to investigate, arrest and prosecute copyright infringement offences.[147] However, these powers will only become operational upon receiving a complaint which thereby suggests that the burden of detection of the infringement rests on the copyright owner. As such, there has been no determined case on ISP liability for copyright infringement, to date, in Kenya.

The right to privacy, for online users, could be inferred from various international Conventions[148] and also the Bill of Rights of the Constitutions of; Kenya,[149] South Africa[150] and USA[151]. In the EU, states' legislations give effect to the EU Data Protection Directive which governs the collection of user data by ISPs. However, an interpretation by the ECJ on whether ISPs where obligated to disclose personal data to facilitate civil copyright infringement proceedings, held that there was neither an obligation to divulge not to withhold data under the Directive.[152]

Although, Darknets' encryption could theoretically be decrypted, practically, it has been discounted as uneconomical and a resourceful endeavour in trying to unlock

---

144 C Jooste, 'A diamond in the Rough- Technology and the Copyright Amendment Act' 19 August 2015 <http://www.blogs.sun.ac.za/iplaw/2015/08/19/a-diamond-in-the-rough-technology-and-the-copyright-amendment-act/ >accessed on 12 August 2017

145 A Jacover, *I Want My MP3! Creating a Legal and Practical Scheme to combat Copyright Infringement on Peer-to-peer Internet Applications*, 90 Geo. L.J. 2207, 2208 (2002) 25

146 L Bygrave, '*The Technologisation of Copyright: Implications for Privacy and Related Interest'* [2002] European Intellectual Property Review 51-57

147 Copyright Act Cap 130 Laws of Kenya, S40-43

148 Universal Declaration of human Rights (UDHR), Art 8 European Convention of Human Rights (ECHR), Art 12

149 Constitution of Kenya 2010 Art 31

150 Constitution of South Africa Art 14

151 Constitution of the US, Fourth Amendment

152 MUIR A'Online Copyright Enforcement by Internet Service Providers' (2013 Loughborough University, Journal of Information Science) 256-259<https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/10750/12/JIS-1880-Final.pdf> accessed on 11 August 2017

every Darknet network without probable cause. Complementary VPN services to Darknet services, provide users with near-perfect anonymity online.[153] The Tor Software is arguable the most popular anonymizing software available free to download.[154] The functionality of these Darknet services vary depending on; the internet's processing speed, level of privacy demanded, security, number of servers, foreign or domestic and the number of simultaneous connections the service provides among other factors.[155]

The level of sophistication in anonymity and security is relatively dependent on also the price, as such, users endure additional cost in order to attain a near perfect anonymity online. Further, VPNs do not make users anonymous *per se* but rather offer privacy, since the VPN service provider will always know who you are and can trace your digital footprints online.[156] The data is retained in logs by some VPN providers and could ultimately be used by law enforcement to identify suspected infringers.

VPN services models are built on the reputation of their privacy, therefore, any obligation to submit these data logs to law enforcement would render their business worthless. Also, even in the absence of the retention of logs, real-time monitoring and tracking of users is still possible. However, in cases where the VPN service uses shared IPs, that is, different users using the same IP address, the ISP would not be in position to identify a specific individual.

For the above reasons, it may be impractical and futile to try and identify individual infringers operating in the Darknet, before even considering suing them. The failure of copyright enforcement through suing individual infringers on conventional networks prompted the shift to suing P2P networks, as intermediaries.[157] As such, it is worth exploring the potential attachment of liability for Darknet Service Providers such as 'Tor', through this method.

---

[153] D Crawford, 'VPNS for Beginners-What You Need to Know' (20 January 2016) <https://www.bestvpn.com/vpns-beginners-need-know/> accessed on 12 August 2017
[154] D Omand, 'The Darknet: Policing The Internet's Underworld'(2015)< http://www.worldpolicy.org/journal/winter2015/dark-net> accessed on 21 August 2017
[155] ibid
[156] ibid
[157] L Edwards, (n 177) 36

3.1.3. Operability of Suing Darknet Parallel-Distribution Networks.

The change in copyright enforcement strategy to suing distribution networks, as enabling intermediaries, was a product of necessity and convenience. This was mainly due to the ability to identify the distribution network, its ISP and ability to effect Notice and Take-Down (NTD) procedures after the site was declared infringing. However, despite the successive generations of distribution networks providing more advantages over the previous ones, they lacked user-anonymity.[158] The networks permitted server end-points to be determined through the users' IP addresses. This exposed them to detection and legal action from their ISPs or the government agencies.[159] In response, various attempts were made to complicate and frustrate law enforcements' efforts, such as; the use of anonymizing routers, overseas routers, object fragmentation among others.[160]

Early forms of Darknet networks blossomed and thrived due to the protection from legal surveillance afforded by sharing amongst friends. This in effect, influenced interconnections between social networks, as each member of a social group of friends, shared it with other friends who partly overlapped with friends from other social groups. It was estimated that the average social person is separated from any other person in the world by a social chain of only about six people, this ratio decreases exponentially with the popularity of an individual. As such any file shared among friends still had the potential of mass distribution.[161]

Over time, more simplified and powerful search engines emerged and increased the search pool of material to a global view.[162] Centralised distribution networks gradually become only commercially and legally viable for legal commerce.

Paul Biddle et al, in '*The Darknet and the future of Content Distribution',*[163]noted that there has been an increase in the Darknet's aggregate bandwidth, reliability, usability, size of shared library and availability of search engines. Any digital content protection

158 P Biddle et al (n 98) 7
159 ibid
160 ibid
161 Ibid 4
162 ibid
163 Ibid 2

system will be overrun by digital experts who will in turn supply the content to Darknets for further distribution to millions of anonymous users.[164]

As a common basic infrastructure topology, the Darknets have; input facilities for new content, distribution networks, search mechanism and storage or caching mechanism to increase on efficiency.[165] Any additional unique features only serve the purpose of encryption and user convenience. Any fight against the Darknet has been motivated to deprive it of one or more of these fundamental structures. Conventional efforts, have usually targeted search engines and the distribution network, however, they have had little or negligible effect.

After Napster and its act-a-likes' network topology was found illegal, open protocols and fully distributed networks emerged that made each user capable of rewriting the protocol and thus created capacity for substantial non-infringing uses.[166] 'Napster', had relied on a centralized server and exercised a considerable amount of control over its users.[167]It was this single fact, that become a central point of failure for such network topologies since one law suit could shut down and eliminate an entire distribution network together with its act-a-likes.[168]

Subsequent, versions of P2P networks were created in response to threats of potential litigation. This was achieved by decentralizing P2P networks and diminishing or shifting control away from the service provider, making it more difficult for copyright holders to track illegal file sharing.[169] These advanced versions despite reducing chances of potential litigation, still left users with the risk of detection.

Through server end-points, decentralised networks left users' IP addresses vulnerable to identification. An estimated 15,000 individuals alleged of copyright infringement were consequently sued by the RIAA.[170] As a result, new consumer demands

---

[165] ibid
[166] Ibid 6
[167] *A&M Records v. Napster*, 239 F. 3d 1004 (9th Cir. 2001)
[168] MA Lemley & RA Reese, '*Reducing Digital Copyright without restricting innovation'*, 56 STAN. L. REV. 1345, 1382 (2004)
[169] JA Wood, '*The Darknet: A digital Copyright Revolution',* Richmond Journal of Law ^ technology, Vol XVI, 4, 16.
[170] Posting of RIAA Watcher to RIAA Watch < http://sharenomore.blogspot.com > accessed on 4 April 2017

required networks to provide user anonymity, privacy and increased security protocol, these versions were later coined 'the Darknet'.[171]

Despite over 35,000 lawsuits, having been reported as filed in 2005, against individual file sharers in the US alone and many more in other, law suits after *Grokster* have been widely considered as pyrrhic.[172]This has been made possible by the decentralized protocols of the BitTorrent generation since even if a client site is taken down, any meaningful law suit would be frustrated since legacy users of the system could continue sharing files in between each other.[173] Secondly, act-a-likes of BitTorrent are now open source protocols, meaning that new versions could be set up with very little effort.

In as much as the abovementioned precedents have been set out and accepted, in the US and European Courts, against conventional P2P networks, the war against illegal parallel distribution extends beyond any one jurisdiction. In effect, the digital content industry still finds itself fighting foreign web domains situated in almost every country in the world, where the domestic courts may not recognise the same liability theories thriving in the US, or face practical challenges to enforce any injunctions granted.[174]

Judgement debtors have had to use access-prevention measures such as domain-blocking or content filtering as some of the technical measures to control content from foreign jurisdictions.[175]However, the application of these method on Darknet websites and domains remains debatable. Access-blocking requires an IAP to block specific targeted content from being received or displayed by its consumers whereas, take down and removal of content entails measures by a website operator to remove or delete website contents.[176] The success of these methods, to a large extent, require ISP cooperation and technical ability in order to effect them. As such, enforcement against Darknets through ISP voluntary intervention is necessary.

---

[171] M Suvanto, '*Privacy in Peer-to-peer Networks',* 3 (2010) < http://www.tml.tkk.fi/publications/C/18/suvanto,pdf > accessed on 4 April 2017
[172] ibid
[173] L Edwards (n 177) 20
[174] ibid
[175] Swiss Institute of Comparative Law (SICL), '*A comparative Study on Blocking, Filtering and Take-Down of illegal Internet Content'* 20 December 2015, 5 < http://www.coe.int/freedomofexpression> accessed on 29 May 2017
[176] Ibid 5

3.1.4. Operability of ISPs' Intervention in the Darknet

This copyright enforcement efforts approach involves the use of ISPs to actively regulate the online behaviour of users and applying sanctions on any infringement of copyright thereof. ISPs intervention could be effected at two levels, on the distribution network using its service and towards identified individual infringers.

The Organization for Economic Co-operation and Development (OECD) identified four models of ISP cooperation; Notice and take down, notice and notice; notice and disconnection or graduated response; and filtering which would entail the blocking access to identified infringing websites or the examination of internet traffic in transit and accessing if its infringing (monitoring or 'deep packet inspection). These models have been lauded as a step forward in copyright enforcement.

On individual infringers, punitive measures, in the 'Graduated Response' could be executed through; slowing down of user's web traffic or denying individual users access to certain websites or disconnecting the user from access to the internet.[177] On distribution networks, ISPs could effect access-blocking, domain name seizures and content filtering.

The objective of the eradication of online piracy being defined, debate remains on whether such a responsibility should be placed on ISPs, whether it should be voluntary or mandatory through legislations and whether it is practical in the Darknet environment.

3.1.5. Challenges of enforcement technics used by ISPs for detection of online infringement:

Online access-blocking techniques currently being used include; Internet Protocol (IP) address blocking, Domain Name System (DNS) alteration, Uniform Resource Locator (URL) blocking and Packet inspection.[178] However, URL blocking is limited in scope of the content it could effectively block hence poses the risk of over-blocking.[179]

DNS blocking has been forwarded as the most economically viable despite having decreasing value in the long-term due to its incompatibility with the implementation of the DNS Security Extensions (DNSSEC).[180]This is because under the DNSSEC,

---

[177] L Edwards, (n 177) 26
[178] The Office of Communications (Ofcom), *'"Site Blocking", to Reduce Online Copyright Infringement; A review of sections 17 and 18 of the Digital Economy Act',* 27 May 2010
[179] ibid
[180] SICL, (n 217) 5

users would no longer be directed to alternative webpages and hence would be unable to tell the difference between a lawful court sanction blocking action and malicious activity on their DNS query.[181]

Deep Packet inspection (DPI) as a long-term solution, although effective, it is complicated, expensive and risks privacy, data protection and communications interceptions concerns.[182] The use of IP address blocking is limited in precision since it is common practice for multiple sites to share a single IP address. URL Blocking is limited in that infringement would simply migrate from web traffic to other means of distribution such as file transfer protocols (FTP).[183]

It has been noted that all the above methods of enforcement have limited value against Darknet websites such as Onion Sites on the Tor browser, since they ordinarily don't have any IP addresses.

Further, most countries, especially the Commonwealth Nations, lack targeted legislative frameworks on the issue of blocking, filtering and takedown of illegal online content and the conditions and procedures to effect them.[*184*]It was noted that most countries rely on a general legal framework and only intervene as a state, for the removal of online content without the need of a court order relate to child abuse material, terrorism and matters of national security.[185] This legal lacuna has created space for voluntary self-regulations by the private sector.

However, voluntary blocking poses the concerns on 'due process' as a fundamental right. In the absence of any legal basis in domestic laws for blocking access to websites, the authority or power to administer the blacklists remains problematic. Access-blocking has received criticism as being an ineffective approach with a significant risk to collateral damage in relation to the suppression of lawful expression and encouraging cross-jurisdictional disputes, whereby, one country may assert its jurisdiction over foreign websites through the Domain Name System (DNS).[186]

---

[181] ibid
[182] ibid
[183] ibid
[184] ibid
[185] Ibid 14
[186] Center for Democracy & Technology, *'The Perils of Using the Domain Name System to Address Unlawful Internet Content'* September 2011 <https://cdt.org/files/pdfs/Perils-DNS-blocking.pdf> accessed on 29 May 2017.

Domain-name seizure involves the ordering of the revocation of the website's domain name registration, and thereby preventing the use of that particular name whereas domain blocking involves the ordering of a Domain name look up service/ ISP not to respond to users' requests for a website or page associated with the blocked IP address.[187]

It has been criticised that, Domain-name seizure and blocking could be easily circumvented and thereby defeating its viability as and enforcement tool and also, neither seizing nor blocking access to a website domain name removes the site or its content from the internet. The site operator could simply; either register a new domain name for the site or distribute browser plug-ins to allow users to retrieve the operators' servers' IP addresses.

In the case of domain-name blocking, users could switch DNS service providers or set up local DNS resolvers on their own computers so as to avoid any DNS servers that have been ordered to block a desired online content. Blocking orders could be defeated by foreign DNS servers which continue to be more popular and widely available in countries enforcing blocking orders.

Darknets such as the Tor Browser, provides an online communication network including access to Darknet websites that thrive on multiple layers of encryptions, directed through a global network of about 6,000 randomly selected servers.[188] At each hop, the Onioin router strips of the next layer of encryption and identifies the next router without discovering its true origin or final destination.[189]

Piercing the dense layers of anonymity has led law enforcement to adopt network investigating techniques similar to those of online hackers.[190] However, in the US, although the Federal Bureau of Investigation (FBI) has reportedly conducted several operations such as 'Operation Torpedo in 2012, 'Operation Onymous' in 2014 and 'Operation Shrouded Horizon' in 2015, these operations targeted online child

[187] Ibid 1
[188] ibid
[189] ibid
[190] D Sui, J Caverlee, D Rudesill, '*The* Deep web *and The Darknet; A Look into The Internet's Black Box'* (3 October 2015) < https://www.wilsoncenter.org/publication/the-deep-web-and-the-Darknet> accessed on 9 October 2017

pornography and money laundering on the 'Silk Road' and not necessarily copyright infringement.

It is noteworthy that, there have not been, so far, any reported active law enforcement operations in the Darknet in Kenya and or south Africa. The burden of detection of the illegal distribution of copyrighted material could therefore be assumed to rest solely on the copyright owners.

The level of sophistication of the Darknet by providing security and anonymity make it near impossible for copyright owners to monitor, detect and identify infringers who use the Darknet as a distribution channel for their digital content. Copyright owners therefore rely on access control TPMs are the primary mode of enforcement since upon circumvention, detection and prevention from further distribution in the Darknet is impossible.

Case laws in different jurisdictions have provided information on the inner workings of the proprietary software used.[191] Firstly, a file registry of copyright material could be maintained, by getting files from copyright holders. Any subsequent uploading and distribution of files, subject to copyright, would then be compared to the registered copies in the database to see if there is a match. This is achieved by deep packet inspections (DPI) when a subscriber of to the ISP attempts to download an infringing copy.[192]

The software would then identify the user by their IP Address together with the relevant time, date and the identification of the copyright material.[193] However, this approach could be limited, in situations where proxy servers and encryptions were used and also the lack of technical capacity for any one ISP to maintain an entire catalogue of digital content and at the same time monitor the entire web traffic in real time without experiencing loss of bandwidth. Identification of infringers also raises privacy concerns and a debate on the line between copyright enforcement and user privacy.

---

[191] *EMI v UPC* (Irish High Court), [2010] <http://www.scribd.com/doc/39104491/EMI-v-UPC> accessed on 22 May 2017; *Roadshow v iiNet* [2010] FCA 24 <http://www.austlii.edu.au/cgi-> accessed on 22 May 2017

[192] ibid

[193] ibid

Despite the abovementioned challenges, the graduated response has gained the perception as a more effective, economic and efficient enforcement mechanism than court based ligation.[194] According to an impact assessment conducted prior to the legislation of the Digital Economy Act, the graduated response was determined to be a much more effective deterrent to online piracy than Court based sanctions and also a proportionate response to the copyright infringement.[195]

It has been seen as a less alienating recourse than criminal sanctions, when content industries enforce their copyright against their own consumer base since. It is predicated on the belief that it will encourage users to migrate to legal online file sharing services and thereby deprive any remaining infringers from available 'seeders' due to their diminishing number online.

In effect, it does not illegalize P2P file sharing but reduces instances of infringing file sharing where artists receive a return on their investment. It has been advanced as a soft handed approach, since it gives infringers multiple chances to reform before imputing sanctions. It protects users' privacy as only the ISP will be in contact with the infringer and hence safeguard his identity. This differs from court based litigation whereby proceedings begin by the identification of the infringer in public proceedings.

In the Darknet environment, copyright enforcement through litigation against individual infringers and ISPs or through effecting the graduated Response, would not be practical. This is because all the above methods rely heavily on the identification of infringers by either; the copyright holders or their agents so as to facilitate the issuance of detection notices or to commence a legal suit for infringement.[196]

---

[194] A Strowel, 'Internet Piracy as a Wake-up Call for Copyright Law Makers- Is The "Graduated Response" A Good Reply?' (2009) 1 WIPO J 75 < https://www.google.co.ke/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjJx9C4nIPUAhXkDMAKHXf_BrwQFggqMAE&url=http%3A%2F%2Fwww.wipo.int%2Fedocs%2Fpubdocs%2Fen%2Fintproperty%2Fwipo_journal%2Fwipo_journal_2_1.pdf&usg=AFQjCNFayBFXByaMLCRBlVTs7ep1O6guBg&sig2=b69Brta9kqw7WW6QEB4NVg> accessed on 22 May 2017

[195] L Edwards, (n 177) 9

[196] ibid 27

CHAPTER FOUR:

4.1. LIABILITY OF DARKNETS & ITS USERS FOR ILLEGAL PARALLEL DISTRIBUTION

4.1.1. Jurisdiction & Attribution of Liability to Darknets

Since individual infringers cannot be identified nor ISPs operating in the Darknet permanently shut down, it's worth pursuing whether liability could be attached to Darknet browsers or software, as the enabling technological infrastructure providers of the parallel markets.

Although there may be consensus on the recognition of copyright and what infringement entails, the attribution of liability for trans-boundary digital copyright infringement, in the Darknet, provokes the question of the jurisdiction of Courts of law. Under the principle of territoriality, rights under Copyright law cannot be extended outside the territory of the state that granted it. In order for any rights granted under copyright to be enforceable under any court of law, such court would have to dispense with whether it is competent to adjudicate the matter and which law to apply.[197] Jurisdiction is a mandatory precondition to the adjudication of any suit, without is, the cause of action fails.[198]Courts of law, as creatures of statutes, cannot bestow upon themselves jurisdiction in the event they do not have it.

In the advent of the digital era, the internet has been described as a digital world without borders which challenges the determination of jurisdiction at a national and international context.[199]Trans-boundary copyright infringement provokes issues relating to the choice of law, appropriate forum, and the potential economic impact of litigating against foreign internet users in an unfamiliar forum or determining the forum for a defendant who only has a virtual presence in a country.[200]

There was no universal copyright law but only numerous domestic laws restricted to their respective domestic territories. International efforts on regional and international levels were developed to ensure the protection of copyright. The Berne convention for

---

[197] *The Owners of the Motor Vessel Lilian 'S' v. Caltex Kenya Limited* (1989) KLR 1
[198] ibid
[199] CM Rieder, SP Pappas, '*Personal Jurisdiction for Copyright Infringement on the Internet'* (Santa Clara Law Review, 1998) < https://cyber.harvard.edu/property00/jurisdiction/rieder.html> accessed on 1 July 2017
[200] ibid

the protection of Literary and artistic works,[201]is considered as an international point of reference for the principle of national treatment. However, no international convention sufficiently addresses issues relating to the jurisdiction of courts, choice of law and enforcement of foreign judgements.[202] As such different jurisdictions have adopted different liability approaches. However, this dissertation will only look into their applicability in so far as they could be reconciled with the Darknet.

In the EU, the European Court of Justice (ECJ) in the case, *Peter Pinckney v KDG Mediatech AG,*[203] upon interpreting Article 5(3) of the Council Regulation (EC) No 44/2001 stated that, a defendant may be sued in a court of any member state in which the copyright is protected and where the harmful event occurred or may occur including, in the case of a website, where it is accessible.

That is, either the place where the damage occurred or the place of the event giving rise to it. Article 5(3) of the regulation only applies as a limiting provision 'if there is a particular close connection factor between the dispute and the courts of the place where the harmful event occurred'.[204] This is subject to also whether the alleged infringed right is protected in that member state and which court is best suited to determine whether the alleged infringement occurred.[205] The court would then only have jurisdiction to determine the damage caused in the respective member state.[206]

This decision has however been criticised as encouraging 'forum- shopping'. The United States of America (USA) has been criticised previously attempted to confer upon its courts extra-territorial jurisdiction over foreign websites through its Stop Online Piracy Act (SOPA)[207] and Protection of Intellectual Property Act (PIPA)[208].

The Bills proposed enforcement measures such as cutting off infringing sites from their US based funding and its financial intermediaries such as payment processors of

---

[201] Berne Convention, Sept 9, 1886, 828 UNTS 221

[202] R Xalabarder, '*Copyright: choice of Law and Jurisdiction in the Digital Age'* (Annual survey of international & comparative Law, 8, 1, 5, 2002) <http://digitalcommons.law.ggu.edu/annlsurvey/vol8/iss1/5> accessed on 1 June 2017

[203] C-170/12 (3 October 2013)

[204] F Maculan, '*Jurisdiction in a case of online copyright infringement'* (11 November 2013) < http://www.martinimanna.com/jurisdiction-in-a-case-of-online-copyright-infringement/> accessed on 1 July 2017

[205] ibid

[206] ibid

[207] House Bill HR 3261

[208] Senate Bill S 968

its advertising revenue.[209] Trans-boundary infringement brings about issues of the appropriate applicable law. The issue of conflict of laws determines the law applicable as well as which liability regime would take precedent.

4.1.2. Vicarious and or Contributory Liability of Darknets as Intermediaries:

Copyright owners faced the challenge of suing authors or distributors of P2P software since in some jurisdictions they could not be charged with direct infringement as it was their users who made copies of the protected works.

Secondary liability, in jurisdictions such as the US, South Africa and the EU, was developed into vicarious and contributory liability. Both forms of liability require that there be a direct infringer, however, contributory liability requires an infringer to have knowledge of the infringement and make a material contribution to it.

Vicarious liability requires the infringer to receive any, direct or indirect, financial benefit from the infringing conduct within its control. However, in the case of *Sony Corp v Universal City Studios v Sony Corporation of America,*[210] the US Supreme Court held that both vicarious and contributory liability will not attach if there are substantial non-infringing uses of the software. Constructive knowledge that customers may infringe copyright using the product is not sufficient to invite liability.[211]

The case of *A&M Records v Napster*[212] was the first major intermediary liability case in the USA to test the above precedent. Napster had hosted a centralised index of all files available in the system which directed users to where the actual files where stored. Napster argued that its software was capable of substantial non-infringing uses which included the swapping of files not protected by copyright or which the copyright owners had consented to.

The court however rejected this defence noting that Napster had a greater degree of knowledge of the infringements than that which Sony had. Napster had actual and not just constructive knowledge of infringement. Where there is knowledge of actual

[209] Stop Online Piracy Act (SOPA) S102 (c)(2)(a)(i), S102(c)(2)(c)(1), S102 (c)(2)(d)(i)
[210] (1984) 464 US 417 (Betamax Case)
[211] L Edwards, (n 177) 37
[212] 239 F 3d 1004 (US)

knowledge of infringement, it was irrelevant that the product was capable of substantial non-infringing use.

The provision of support services in the form of indexing files constituted contributory infringement. Napster was also vicariously liable since it enjoyed a financial benefit having designed their system to lure more consumers of infringing material while its revenue stream was directly dependent upon their web traffic. Napster had the ability to supervise the infringing conduct and block users' access to its service therefore, it could not be deemed as a 'mere conduit'.

In *Re Aimster,*[213] Aimster did not maintain any copies of files in its servers but instead relied on its users' computers acting for hosting the files. Aimster only provided the software that connected the users' computers and helped in searching for files. In addition, the sharing of the files where encrypted. The court stated that although Aimster could demonstrate non-infringing uses of its software, it was also being used for substantial infringing purposes and therefore they needed to provide evidence in support of their non-infringing use.

The court needed actual and not just hypothetical evidence of its non-infringing use and stated that it was not enough that a product or service was capable of non-infringing use. The court determined that Aimster had chosen not to know and thereby cultivated an element of 'willful blindness'. The court held that, its refusal to discover the extent to which its system was being used to infringe copyright was merely evidence of its contributory infringement.

The case of *Metro-Goldwyn-Mayer Studios Inc (MGM) v Grokster Ltd*,[214] deliberated on the legality of the newly emerged second generation of P2P networks. It operated on a decentralised network, with each user maintaining an index of only the files which they wanted to share. Any user would thereby make a request which would then be processed by the software by broadcasting the search request to all other computers. The collective result was then passed back to the requesting computer.

The court held that, where the product was not capable of substantial or commercially significant non-infringing use, the copyright owner need only show that the defendant had constructive knowledge of the infringement. However, where the product was

[213] 334 F 3d 643 (7th Cir 2003)
[214] 545 US 913 (2005)

capable of substantial or commercially significant non-infringing uses, the copyright owner must show that the defendant had reasonable knowledge of specific infringing files and failed to act on that knowledge to prevent infringement.

Both the District and the Appeal Court found that, the Software application used, was capable of Substantial non-infringing uses citing that the test was how probable the product or service was capable of non-infringing use.[215]

However, the court did find Grokster vicariously liable since there was an element of financial benefit through advertising revenues. On the 'degree or ability to control' the court found Grokster have the ability to block access to individual users since there was no registration or log-in process in the first instance. The court ruled that the willful blindness theory was absent in the case of Grokster. However, on appeal, the supreme court found Grokster liable for inducing copyright infringement.

4.1.3. Darknet Intermediaries Under the Limited-Liability Regime

Having established how Darknets are being used to facilitate illegal parallel free markets, it now begs the question on whether they can be held liable, as intermediaries, for the illegal distribution of digital content in their network under the different immunity regimes recognized.

The legal genesis of intermediaries' immunity has been attributed to the EU Electronic Commerce Directive (ECD)[216] and the US Digital Millennium Copyright Act (DMCA)[217].[218] They, in effect created immunity from liability in the event that online intermediaries receive actual notice or were aware of facts or circumstances indicating illegal content or activity.[219]This has been attributed to the birth of voluntary Notice and Take Down (NTD) as a self-monitoring mechanism by intermediaries.[220]

In the EU's ECD, online intermediaries are exempted from copyright infringement on condition that; intermediaries should disclose the identity of infringers on request;

[215] L Edwards, (n 177) 21
[216] Directive 2000/31/EC of the European Parliament and of the Council
[217] DMCA 1998 (US)
[218] L Edwards (n 177) 1
[219] ibid
[220] ibid

they should also subscribe to a detailed code of practice relating to notice, take-down and put-back measures as well as access-blocking to identified repeat infringers.[221]

Online intermediaries are defined as any service normally provided for remuneration, at a distance, by means of electronic equipment, for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service.[222] This definition includes not only the traditional ISP but also hosting services, e-commerce merchants, social networking sites, cloud computing services, mobile providers among others.[223] It could therefore be argued that, by this definition Darknet service providers could be included.

ISPs would be absolved from any liability if they act as 'mere conduits' i.e transmit content originated by and destined for other parties without modifying the information contained in the transmission or initiating or selecting the receiver of the transmission.[224] This applies also when ISPs *Cache* material i.e make copies of remote web pages by hosts when requested, in order to speed up delivery of those pages on subsequent request to speed up the web for all other users.[225] Immunity is also subject to the ISP taking down cached copies once they obtain actual knowledge of the removal of the original content or its access disabled.[226]

The ECD provides immunity from criminal and civil liability in respect of third parties' stored information as long as they have no 'actual knowledge' of the illegal activity or are not aware of the facts and circumstances from which from which the illegal activity or information is derived.[227] However, ISPs are not obliged to seeks out these facts or circumstances and preserves the parties right to seek injunctive relief to terminate or prevent infringement, suffice to say, enforceability remains the burden of the Copyright holder.[228]

ISPs are only obliged to go as far as to act in good faith and reasonable care specified under national law when detecting illegal activity.[229] However, there remains to

[221] Ibid 7
[222] ECD S4
[223] L Edwards (n 177)
[224] ECD art 12
[225] L Edwards (n 177) 9
[226] Ibid 10
[227] L Edwards (n 177) 10; ECD Art 14
[228] ibid
[229] ECD Art 48; ECT Act S 78

debate on how 'expeditiously' an ISP should be when executing a take-down notice.[230] The ECD motivates an ISP to take down a site summarily since once upon the expiry of the grace period, liability is strict even if the delay to take down was due to technical or administrative issues.[231]

In the USA, the DMCA provides for similar 'safe habours' akin to those in the ECD but in addition, its 'safe habours' only apply to those ISPs which implement an NTD system, upon complaint of copyright owners, and also have a system of identifying 'repeat infringers' and have operational technical protection measures (TPMs).[232]

However, the DMCA faces the same criticisms as the ECD, in that, it creates internet censorship and privacy concerns in cases where ISPs would arbitrarily execute NTD for selfish reasons and also the need for detection by a copyright owner. Research has shown that the current regulatory settlement operates where the incentive to take down content from the internet is higher than the potential costs of not taking it down which brings about collusion of the ISP and complainants.[233]

In South Africa, the Electronic Communications and Transactions Act,[234] provides for immunity from liability for an ISP which acts as a 'mere conduit' by not; initiating the transmission; selecting the addressee; performing its functions in automatic, technical manner without selection of the data and; does not modify the data contained in the transmission.

Immunity is also granted to an ISP which acts as an information location tool.[235] The ISP would not be liable for:

> [R]eferring or linking users to web pages containing infringing data messages or infringing activity by using such information location tools, including a directory, index, reference, pointer or hyperlink where the service provider…is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data

---

230 L Edwards (n 177) 10
231 Ibid; ECD Art 14
232 ibid
233 L Edwards, '*Role and Responsibility of the Internet Intermediaries*' 28 May 2010 < http://www.wipo.int/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf> accessed on 9 October 2017, 12
234 Chapter XI, S70- 79 ECT Act
235 Ibid S76

> message is apparent…and removes, or disables access to, the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to such data message, infringes the rights of a person.

In Kenya however, there are no NTD provisions, policies or procedures in the Kenya Copyright Act or any other relevant legislations. There are also no 'safe habours' for intermediaries or implied provisions that limitation of their liability could be inferred upon. In addition, there are also no specified penalties for ISPs for failing to block or remove infringing content online. Any potential litigant would therefore have no legal basis for suing intermediaries and as a result will be limited to suing individual infringers for any online copyright infringements.

The case of *Bernsoft Interactive & 2 Ors v Communications Authority of Kenya & 9 Ors,*[236]is the only existing case on record dealing with intermediary liability but remains pending before the High Court. Therein, according to the Constitutional Petition filed, copyright owners are seeking injunctive orders to compel ISPs in Kenya to block websites enabling online piracy and declaratory orders that the state has failed in its constitutional and legal obligations to protect Kenyan's intellectual property rights.[237] The Communications Authority of Kenya (CAK) and Kenya Copyright Board (KECOBO) among other state organs were sued alongside ISPs, specifically, for allowing their consumers to use their networks to illegally acquire digital copies of works protected by copyright infringing content.

Despite legislative authorities in the US, UK and South Africa, these legislative developments have been criticised as ill-equiped and not generally designed to deal with copyright infringement in the context of P2P intermediaries and where meant for more straight-forward case of transmission, caching and hosting by the ISP.[238] The emergence of new network topologies as a reaction to these legislations, created the need for judicial intervention so as to address the growing legal lacuna and impute liability.

---

[236] Petition No 600 of 2014, Kenya Law Reports

[237] IP Kenya, '*Test Case on Liability for Online Copyright Infringement: Music Industry Players Sue ISPs, Telecos and Government'* 15 December 2014 < https://ipkenya.wordpress.com/2014/12/15/test-case-on-liability-for-online-copyright-infringement-music-industry-players-sue-isps-telcos-and-government/> accessed on 8 August 2017

[238] L Edwards, (n 331) 9

In light of the above, it could be argued that Darknets would not be held illegal at first instance and liability would be dependent on a Darknet's particular use. It suggests that under the COSNU doctrine, unless a copyright owner proves specific infringement of copyright in Darknets, Darknets qualify for immunity despite its ability to allow its users to infringe copyright with impunity.

4.1.3.1. Darknets under the Capable of Substantial Non-Infringing Use (COSNU) Defence

Darknet versions such as 'Freenet' operate on different protocol which closely resembles that of the BitTorrent. Therein, files are not only downloaded or uploaded in small bits from multiple sources, but are also optimized further, by reducing the knowledge of all the file-sharing parties through encrypting the files being transferred. This encryption affects even the ability of the host to identify a file, or part of it, being shared. In the event that an infringing copy is tracked down to any particular user, it would be difficult to pin point its origin in the network.[239] This frustrates any attempt to attribute to liability for distribution since mere possession of an infringing article is not a crime.

Darknets such as 'Tor Browser', allow their users anonymous communication through a free, worldwide, volunteer overlay network. It conceals users' location and usage from potential network surveillance to traffic analysis. Its intended use was for the protection of the personal privacy and freedom of speech of its users.

Its anonymity feature has been lauded as a method for vulnerable internet users such as whistle-blowers and human rights activists to communicate with journalists without the fear of surveillance and arrest. Developers of the Freenet software application defend the software's application as a tool to protect political dissidents' freedom of speech, in repressive regimes. In the absence of anonymity, the free flow of information vital to the growth of democracy would be suppressed through state-sponsored internet censorship.[240]

It is also used as a circumvention tool for internet censorship such as the Great Firewall of China (GFW) used by the Islamic Republic of Iran and the Peoples Republic of China to regulate internet domestically.

---

[239] J Wood, (n 210) 9

[240] P Biddle, P England, M Peinado & B William, *The Darknet and the Future of Content Distribution*, Microsoft Corporation <http://msl1.mit.edu/ESD10/docs/Darknet5.pdf > accessed on 25 May 2017, 20

As such, not only does the Tor Browser qualify for the COSNU defense, even in jurisdictions where they would not appreciate the same doctrine, its technical infrastructure renders any action against it or its users, futile.

The Darknets software's ability to aid in copyright infringement has been dismissed as an inevitable consequence of the design.[241] Darknets, as Open Source Software (OSS), have mutated to user friendly designs with improvements on their user-interfaces so as to be more appealing and inclusive to average tech-savvy users.[242] Also, as open source protocols, users could adopt and make available newer versions, resilient to detection or monitoring.[243] In absence of a central server, any potential injunction order becomes futile once the digital content is distributed since it would be difficult to eliminate all other infringing copies in circulation.[244]

It has been estimated that, the improvements in the technological infrastructure of the telecommunications industry would lead to the spread of Darknets and digital content sharing since they would be able to overcome file-size limitations common to conventional file sharing services such as email.[245]

In light of this facts, it remains highly probable that illegal, parallel, free markets of digital content, in the Darknet, will flourish with impunity since neither Darknet users or the Darknet service provider can be held liable. As such, a different approach to ensuring digital copyright owner's commercial success is necessary.

---

[241] Ibid.
[242] ibid
[243] P Biddle, P England, M Peinado & B William, *The Darknet and the Future of Content Distribution,* Microsoft Corporation <http://msl1.mit.edu/ESD10/docs/Darknet5.pdf > accessed on 25 May 2017, 24
[244] A Jacover, (n 8) 2245
[245] J Wood (n 210) 22

CHAPTER FIVE

5.1.RECOMMENDATIONS & CONCLUSION

Access-controlled digital works, offered for value, have been competing with their identical copies, offered for free, in parallel distribution networks. These parallel free markets have come to evolve into the Darknet that exist today, and where users benefit with impunity. The evolution and demand for these clandestine networks has been attributed to the need to escape liability.

The invincibility of Darknets against copyright enforcement and attachment of liability, under different liability regimes, creates a serious concern on the feasibility of digital copyright enforcement and provokes the question of whether copyright owners can only attain commercial success through access-control measures and thereby compete with their identical copies in parallel free markets.

5.1.1. RECOMMENDATIONS:

It can therefore be suggested that a new approach to the commercialization of dematerialized digital copyright is necessary. This can be effected through the adoption of open-access business models and or; creation of a 'digital use' exemption and or the adoption of alternative revenue business models such as ad-based as opposed to subscription-based models.

5.1.1.1.'Digital Use' Exemption:

Digitization of copyrighted works complicated copyright enforcement against illegal parallel distribution in the general online environment. The rise of the Darknet creates a further frustration in enforcement of copyright. Legal scholars have speculated that copyright holders may take either of two choices; surrender their pursuit of incorruptible TPMs and find alternative means of compensation or strive for tougher copyright protection legislations and risk losing control.[246]

However, stronger protection measures such as the criminalization of copyright infringement has been criticized as draconian and only deter innovation. The Darknet makes any proposed legislative enforcement unlikely to succeed.[247]TPMs without an

[246] L Edwards, (n 331) 27

[247] F von Lohmann, *'Measuring the Digital Millennium Copyright Act Against The Darknet: Implications for the Regulation of Technological Protection Measures (*Loyola of Los Angeles Entertainment Law Review, 2004) <http://ditigalcommons.lmu.edu/elr/vol24/iss4/4> accessed on 27 May 2017, 642

absolute guarantee against possible infringement would only equate to its failure. Not only is the achievement of absolute control impossible but 'fair use' activists advocating for public access to works have halted further development on TPMs. The right to fair use or fair dealing entails the public's access to works for purposes of parody or criticism.[248]

In the unlikely prospects of stronger TPMs and penal legislations succeeding, copyright owners could surrender control of their works and adopt alternative means of compensation.[249] Copyright holders in the online creative industry are likely to end up competing with free versions of their own digital works since consumers would be reluctant to pay for content they could otherwise get it for free. The lack of operability of copyright enforcement would eventually diminish, if not eliminate, any chance of maintaining an economic monopoly over their copyrighted works.

The creative industry would therefore need to shift to alternative revenue schemes so as to maintain an alternative equivalent revenue stream. This could be achieved by changing their business model to an ad-based model.

5.1.1.2. Advertising-Based Business Model

An Ad-based business model is characterized by using advertisements as a primary revenue stream as opposed to using paywalls that allow access to content upon payment of subscription fees in online streaming services such as 'Netflix'. Advertising revenue will be derived from selling space on selected web pages on their websites with payment models such as 'pay-per-click' or 'pay-per-view' of any unique user visiting the website.

The ad-based revenue stream has been compared to that of the TV Industry which almost exclusively relies on selling airtime for commercial advertisers on their channel.[250] Online advertising has also been reported as successful on online based companies such as Google. The Ad-base model by design, benefits exponentially from increase in the volume of web traffic. It is therefore essential that copyright owners and online creative industry appeal to online consumers by granting them free access to their works and hence eliminate the need for users to go into the Darknet.

---

[248] L Edwards, (n 331) 28
[249] ibid
[250] L Edwards (n 331) 53

However, the success or pitfalls of this suggestions can only be speculated at this point as it would first require its implementation so as to gain any empirical evidence regarding its proven merits.

5.1.1.3. Commercialization of Data mines:

With the use of the statistical analysis of consumer web traffic, online creative industries could collect valuable data regarding their consumer preferences from their online activity and predict demand.[251] Users preference could be determined through online surveys, product reviews, downloaded or streamed content, volunteered personal data such as location which may be used to also establish consumer demographics.[252]

This consumer behavioral analysis is what culminates to 'data mining'. Data mining has been defined as 'the practice of collecting and analyzing digital consumer behavior data, is part of a lager category of business intelligence tools that help companies maximize profits'.[253]

Data mining is unique to only the surface web and cannot be adopted by Darknets since user activity cannot be tracked in the Darknet.[254] Online creative industries could capitalize on consumers' web traffic analysis by granting abandoning conditional access to their works and giving free access of their works online. By predicting trends and preference for every unique user, online creative industries could use data aggregation services to address individual needs and make more relevant and targeted recommendations to consumers.

5.1.2. CONCLUSION:

In summary, copyright owners' right to exclusive economic exploitation of their digital works online is presently maintained through subscription based business models effected through paywalls as access control TPMs. However, it has been established that no TPM is perfect or invincible from a technologically sophisticated user and hence they are only geared to manage only the average user.

Further, once an access control TPM has been circumvented, copyright owners rely on ISPs cooperation in detecting the illegal distribution of their works or be held

[251] ibid 54
[252] ibid
[253] ibid
[254] ibid

liable. However, the Darknet as an emerging distribution channel eliminates any possibility of ISP monitoring and hence leaves copyright owners vulnerable to unfettered infringement and unable to recoup on their investment.

Most countries have taken the initiative of legislating tougher criminal penalties for infringement through circumvention and or distribution so as to deter the vice. However, the growing use of Darknets and their development into more user-friendly versions for the average user, have created an environment of impunity for infringers.

The above described situation leaves the achievement of copyright owners' exclusive economic rights to be rethought. It has been observed that online access-controlled business models only lead to the creation of parallel free markets since consumers would be reluctant to pay for content they can get for free.

Copyright owners would also not have to worry about monitoring or detecting online infringement, a problem which was beyond the technological and financial capabilities of many. It is on the inability of copyright owners to monitor the internet, on a global scale, and detect infringement that this dissertation considers enforceability of online copyright inoperable. The pursuit of tougher legislative sanctions, has only led to the demand to more sophisticated technology that either provide anonymity or convenient access to Darknets.

It is on this basis that this dissertation advocates for a 'digital exemption use' where copyright owners would provide their content for free and commercially benefit alternative means of revenue creation. This would, in effect, eliminate the growing illegal, parallel, free markets and the appeal the Darknet provides.

These alternative-income-generating models would strike a balance between copyright owners' financial interest in their works and public interest in the form of access.

BIBLIOGRAPHY:

PRIMARY SOURCES:

3.1.5.1.LEGISLATIONS:

INTERNATIONAL INSTRUMENTS

- The Berne Convention
- The Paris Convention
- The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) Agreement

- Berne convention; Statement adopted by the WIPO Diplomatic Conference on Certain Copyright and Neighouring Rights Questions 20 December 1996.
- WIPO Copyright Treaty S. Treaty Doc. No. 105-17 (1997); 36 ILM 65(1997) (adopted 20 December 1996) (entry into force 6 March 2002) < http://www.wipo.int/treaties/en/ip/wct/pdf/trtdocs_wo033.pdf> accessed on 21 July 2017

REGIONAL & NATIONAL LEGAL INSTRUMENTS

UNITED STATES OF AMERICA

- Stop Online Piracy Act (SOPA) (the E-PARASITE Act)
- Protect IP Act (PIPA) (the Combating Online Infringement and Copyright Act (COICA)
- Online Copyright Infringement Liability Limitation Act,
- Digital Millennium Copyright Act (DMCA)

EUROPEAN UNION

- EU Copyright Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society (Information Society Directive or the InfoSoc Directive)

SOUTH AFRICA

- Copyright Act South Africa;

KENYA

- Copyright Act Cap 130 Laws of Kenya

3.1.5.2.JUDICIAL CASE LAWS

USA

- *Sony Corp. vs Universal studios, 464 U.S. 417 (1984)*
- *A&M Records v. Napster, 239 F. 3d 1004 (9th Cir. 2001)*
- *MGM v Groster, 545 U.S 913 (2005)*
- *Flava Works Inc. vs Gunter*

- *Bobbs-Merrill Co v Straus & Another* 1908, 210 US 339
- *Kirtsaeng v John Wiley & Sons Inc* 2013, 133 S Ct 1351

- *EMI v UPC* (Irish High Court), [2010] <http://www.scribd.com/doc/39104491/EMI-v-UPC>
- *Roadshow v iiNet* [2010] FCA 24

EUROPEAN UNION:

- *Atari Europe S.A.S.U vs Rapidshare AG*

SOUTH AFRICA

- *S v Norton (Four Corners Case)*

KENYAN

- *The Owners of the Motor Vessel Lilian 'S' v. Caltex Kenya Limited* (1989) KLR 1
- *Bernsoft Interactive & 2 Ors v Communications Authority of Kenya & 9 Ors*

SECONDARY SOURCES (Literal Jurisprudential Sources):

BOOKS

- Dean, A Dyer (eds), '*Introduction to Intellectual Property Law'* (Oxford University Press South Africa 2014) 33
- S Papadopoulos, S Snail (eds), '*Cyberlaw@SAIII; The Law of The Internet in South Africa'* (Van schaik, Pretoria, 3, 2012) 170

ARTICLES

- A Strowel, 'Internet Piracy as a Wake-up Call for Copyright Law Makers- Is The "Graduated Response" A Good Reply?' (2009) 1 WIPO J 75 < https://www.google.co.ke/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjJx9C4nIPUAhXkDMAKHXf_BrwQFggqMAE&url=http%3A%2F%2Fwww.wipo.int%2Fedocs%2Fpubdocs%2Fen%2Fintproperty%2Fwipo_journal%2Fwipo_journal_2_1.pdf&usg=AFQjCNFayBFXByaMLCRBlVTs7ep1O6guBg&sig2=b69Brta9kqw7WW6QEB4NVg>
- A Jacover, *I Want My MP3! Creating a Legal and Practical Scheme to combat Copyright Infringement on Peer-to-peer Internet Applications,* 90 Geo. L.J. 2207, 2208 (2002)
- A Kalvi, '*The Impact of Copyright Industries on copyright Law'* <www.juridicainternational.eu/public/pdf/ji_2005_1_95.pdf>
- A Christie, *'Reconceptualizing Copyright in the Digital Era'* (European Intellectual Property Review 1995, 522)
- Anderson N, 'No more lawsuits: ISPs to work with RIAA, cut off P2P users, <http://www.arstechnica.com/tech-policy/news/2008/12/no-more-lawsuits-isps-to-work-with-RIAA-cut-off-P2P-users.ars.>
- Balangesh, S 'Foreseeability and Copyright Incentives' (2009) 122 *Harvard Law Review* 1569 at 1577
- C Angelopoulos, '*CJEU Decision on Ziggo: The Pirate Bay Communicates Works to the Public'* 30 June 2017 (CIPIL, University of Cambridge) < http://copyrightblog.kluweriplaw.com/2017/06/30/cjeu-decision-ziggo-pirate-bay-communicates-works-public/>

- C Jooste, 'A diamond in the Rough- Technology and the Copyright Amendment Act' 19 August 2015 <http://www.blogs.sun.ac.za/iplaw/2015/08/19/a-diamond-in-the-rough-technology-and-the-copyright-amendment-act/ >
- Center for Democracy & Technology, *'The Perils of Using the Domain Name System to Address Unlawful Internet Content'* September 2011 <https://cdt.org/files/pdfs/Perils-DNS-blocking.pdf>
- D Sui, J Caverlee, D Rudesill, '*The* Deep web *and The Darknet; A Look into The Internet's Black Box'* (3 October 2015) < https://www.wilsoncenter.org/publication/the-deep-web-and-the-Darknet>
- D Crawford, '*VPNs for Beginners- What you Need to Know'* 20 January 2016 <https://www.bestvpn.com/vpns-beginners-need-know/>
- Deloitte, 'Digital Media: Rise of On-demand Content' < www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-rise-of-on-demand-content.pdf>
- E Duah, '*Internet Service Providers' Monitoring Obligations'* (2013) < chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://journals.muni.cz/mujlt/article/download/2605/2169>
- F von Lohmann, *'Measuring the Digital Millennium Copyright Act Against The Darknet: Implications for the Regulation of Technological Protection Measures (*Loyola of Los Angeles Entertainment Law Review, 2004) <http://ditigalcommons.lmu.edu/elr/vol24/iss4/4>
- F S McNeilly, '*The Enforceability of Law*' (Nous Vol 2 No 1 Feb 1968) < http://www.jstor.org/stable/2214413 >
- F Maculan, '*Jurisdiction in a case of online copyright infringement'* (11 November 2013) < http://www.martinimanna.com/jurisdiction-in-a-case-of-online-copyright-infringement/>
- H Klopper, T Pistorius, LA Tong et al '*Law of Intellectual Property in South Africa'* (2011 Lexis Nexis)
- IP Kenya, '*Test Case on Liability for Online Copyright Infringement: Music Industry Players Sue ISPs, Telecos and Government'* 15 December 2014 < https://ipkenya.wordpress.com/2014/12/15/test-case-on-liability-for-online-copyright-infringement-music-industry-players-sue-isps-telcos-and-government/>
- IP Unit, University of Cape Town, 'Our Views Regarding the "Four Corners" Piracy Case Sentence' 23 April 2014< http://www.iplaw.uct.ac.za/news/our-views-regarding-%E2%80%9Cfour-corners%E2%80%9D-piracy-case-sentence>
- J Hughes, "*The Philosophy of Intellectual Property*," (*Georgetown Law Journal*, 77, 1988)
- J Bhargava and A Klat, '*Content democratization: How the Internet is Fueling the growth of creative economies*' 5 January 2017 < https://www.strategyand.pwc.com/reports/content-democratization >
- J Meindertsma, '*Theories of Copyright'* (9 May 2014) < https://library.osu.edu/blogs/copyright/2014/05/09/theories-of-copyright/>

- Jayant Bhargava and Alice Klat, 'Content democratization: How the Internet is Fueling the growth of creative economies' 5 January 2017 < https://www.strategyand.pwc.com/reports/content-democratization >
- J Wood, '*The Darknet: A Digital Copyright Revolution*'(2010) < http://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1330&context=jolt>
- JD Lasica, '*Darknet: Hollywood's War Against the Digital Generation'* 264 (John Wiley & Sons Inc 2005)
- L Bygrave, '*The Technologisation of Copyright: Implications for Privacy and Related Interest'* [2002] European Intellectual Property Review 51-57
- L Edwards, '*Role and Responsibility of the Internet Intermediaries*' 28 May 2010 < http://www.wipo.int/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf>
- L Hautala, '*A VPN can Protect your online Privacy but there is a Catch' 29* March 2017 <https://www.cnet.com/news/vpn-protect-online-privacy-its-complicated/>
- M Conroy, '*A Comparative Study of Technical Protection'* 2009< http://uir.unisa.ac.za/bitstream/handle/10500/2217/thesis.pdf;sequence=1>
- M Chertoff and T Simon, '*The impact of the dark web on internet governance and Cyber security'* (CIGI 2015)
- M Suvanto, '*Privacy in Peer-to-peer Networks',* 3 (2010) < http://www.tml.tkk.fi/publications/C/18/suvanto,pdf >
- M Bide at al, '*Copyright Clearance and Digitization in UK Higher Education: Supporting Study for the JISC/ PA Clearance Mechanisms Working Party'* <http://www.ukoln.ac.uk/services/elib/papers/pa/clearance/ >
- M Jaconi in Business Insider, 'The 'On-Demand Economy' is Revolutionizing Consumer Behavior- Here's How' 13 July 2014 < http://www.businessinsider.com/the-on-demand-economy-2014-7 >
- M Owen, '*Exhaustion of rights and digital content'* (November 2013) < https://www.taylorwessing.com/download/article_exhaustion_of_rights.html>
- OECD, '*Chapter 5: Copyright in the Digital Era: Country Studies*' <www.oecd.org/sti/ieconomy/Chapter5-KBC2-IP.pdf>
- Nel '*Freedom of expression and the internet'* in Buys (ed) Cyberlaw @SA II: The Law of the interne in South Africa 2 ed (2004)
- N Elkin-Koren, '*Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic' (*9 NYUJ, Legis & Pub, Poly 15, 22, 2006)
- O Afori, 'Human Rights and Copyright: The Introduction of Natural Law Considerations into American Copyright Law' (2004 14 *Fordham Intellectual Property, Media and Entertainment Law Journal)*
- O Dean, A Dyer (eds), '*Introduction to Intellectual Property Law'* (Oxford University Press South Africa 2014)
- P Biddle, P England, M Peinado & B William, *The Darknet and the Future of Content Distribution,* Microsoft Corporation <http://msl1.mit.edu/ESD10/docs/Darknet5.pdf >

- Q Liu, 'Digital Rights Management for Content Distribution' (University of Wollongong School of Information Technology and Computer Science, 2003) < https://dl.acm.org/citation.cfm?id=827994>
- R Xalabarder, '*Copyright: choice of Law and Jurisdiction in the Digital Age'* (Annual survey of international & comparative Law, 8, 1, 5, 2002) <http://digitalcommons.law.ggu.edu/annlsurvey/vol8/iss1/5>
- Swiss Institute of Comparative Law (SICL), '*A comparative Study on Blocking, Filtering and Take-Down of illegal Internet Content'* 20 December 2015, 5 < http://www.coe.int/freedomofexpression>
- S Karjiker, '*The First-Sale Doctrine: Parallel Importation and Beyond'* (2015 Stellenbosch LR 633) < http://blogs.sun.ac.za/iplaw/files/2016/04/The-first-sale-doctrine-Parallel-importation-and-beyond.pdf>
- S Papadopoulos, S Snail (eds), '*Cyberlaw@SAIII; The Law of The Internet in South Africa'* (Van schaik, Pretoria, 3, 2012)
- S Androutsellis- Theotokis & D Spinellis, *A Survey of Peer to-peer Content Distribution Technologies, 36 ACM Computing Surveys 335, 335-36 (2004)*
- Symposium, *At the Crossroads of law & Technology: fifth Annual conference, Alternative Methods for Protecting Digital content,* 25 Loy. L.A ENT. L. REV. 63, 67 (2004)
- Yu P, 'the Graduated Response', (2010), 62, 16-17 Florida Law Review, <http://www.papers.ssrn.com/sol3/papers.cfm?abstractid=1579782 >