A PROPOSED LEGISLATIVE FRAMEWORK TO PROTECT DIGITAL COPYRIGHT FROM END USER INFRINGEMENT ON THE INTERNET IN THAILAND: A COMPARATIVE APPROACH

PRASERT JARUNRATANASRI

A thesis submitted in partial fulfilment of the requirements of Nottingham Trent University for the degree of Doctor of Philosophy

October 2016

Abstract

This thesis argues that Thailand does not have adequate specific legal remedies to protect copyright work on the internet, for example, the use of copyright content on public websites or file-sharing platforms. The aim of the study is to construct a legal framework to provide effective copyright protection remedies. In particular, more effective remedies are needed for copyright infringement by end-users using client-server and Peer-to-Peer (P2P) file sharing technology.

In terms of methodology, this thesis is documentary research. The thesis employs a comparative system legal approach. It compares Thailand's Copyright Act (No.2) B.E.2558 (CA 2015) with digital copyright enforcement systems in two foreign jurisdictions: (1) the Notice and Takedown (N&T) system of the United States; and (2) the Graduated Response (GR) of France. It examines and compares functional aspects between the CA 2015 and N&T as applied to the client/server technology. The same comparative system method is also employed with respect to digital copyright infringement under the CA 2015 compared with the GR system as it applies to P2P technology. The thesis constructs a proposal for a more effective legislative framework to protect copyright on the internet for Thailand.

The thesis finds that the practical enforcement problems relating to both client/server and P2P end user infringers in the online environment is threefold. First, it involves fast widespread distribution of content. Second, there is a large number of potentially infringing internet end users. Third, there are significant difficulties in identifying an actual infringer. The author argues that Thailand's CA 2015 court procedure is not suitable because it is slow, costly and does little to solve any of the aforementioned problems. The thesis finds that generalised characteristics of a suitable enforcement remedy should include several elements, namely, end user educative and awareness-raising functions and gradually increasing legal sanctions such as warning, fines as well as internet access restriction. It is recommended that the N&T and GR remedies in use in the US and EU respectively be adopted in Thailand with certain adjustments to suit the Thai context and replace existing unwieldy criminal and civil litigation. To this end, it is recommended that in order to overcome the difficulty of infringer identification, a new internet subscriber's duty should be introduced in Thailand.

Acknowledgements

This thesis would never have been fulfilled without the encouragement of many people. I am grateful to my supervisors, Dr. Janice Denoncourt, Dr. Elizabeth Chadwick and Professor David Ong for reading various drafts, discussing complicated issues; and providing comments, guidance and all other supports. For four years, all of these have illuminated my knowledge and the understanding of PhD study, and have greatly contributed to the success of my PhD thesis. I am privileged to work under their supervision. Many thanks are also due to academic and non-academic staff of Nottingham Law School and Graduate School for providing support academically and administratively throughout the course of my study.

I would also like to thank my parents, Mr.Thongchai and Ms. Somchit Jarunratanasri, who are the most important persons in my life and who are always my motivation of all time. I thank my sister and brothers and their families who have taken good care of my parents in Thailand while I could not do so. Special thanks go to my own family, my wife Onusa Krisanalome Jarunrattanasri and my daughter Jittibhorn Jarunratanasri, who always stand beside me in any difficult situation and inspire the positive side of my life here in the UK. The language in the PhD thesis would not have been more precise and smooth without assistance from my proof reader, Mr. Alan Kitson, who is also my friend, my English teacher and my daughter's English and Spanish teacher. I would like to thank him for all of these contributions and, many times, his encouragement. I would not have had an opportunity to study PhD and to complete the thesis without permission and financial support from the office where I work, the Thailand Office of Attorney General. I would like to express my gratitude to the office, to all Thai tax payers and to my mother land, Thailand.

Finally, the most appreciation is for the Lord Buddha and his disciples (Buddhist saints) whose teaching (Dharma) enlightens my wisdom, discloses the focus on the present moment, not the past and the future, and helps me abandon ignorance and other negative thoughts. This relieves me from stressfulness and confusion, not to mention health issues such as migraine, gastritis, eye strain. I would not have made it without them and it is to them that I dedicate this thesis.

Table of Contents

List of Abbreviations

ADSL	Asymmetric digital subscriber line
B.E.	Buddhist Era
Berne Convention	Berne Convention for the Protection of Literary and Artistic Works
CA 1994	(Thailand) Copyright Act B.E 2537 (1994)
CA 2015	(Thailand) Copyright Act (No.2) B.E.2558 (2015)
C.D. Cal.	Central District of California
CAS	Copyright Alert System
CCC 1925	(Thailand) Civil and Commercial Code B.E.2468 (1925)
CIPIT	(Thailand) Central Intellectual Property and International Trade Court
9th Cir.	the United States Court of Appeals for the 9th Circuit
CIPC 1934	(Thailand) Civil Procedure Code B.E.2477 (1934)
CPU	Central Processing Unit
CROA 2007	(Thailand) Computer-Related Offence Act B.E. 2550 (2007)
CRPC 1934	(Thailand) Criminal Procedure Code B.E.2477 (1934)
DADVSI	Law on Authors' Rights and Related Rights in the Information Society (French: *Loi sur le Droit d'Auteur et les Droits Voisins dans la Société de l'Information*)
D.C. Cir.	The United States Court of Appeals for District of Columbia Circuit
DIP	Thailand Department of the Intellectual Property Department
DMCA	Digital Millennium Copyright Act 1998
DNA	Deoxyribonucleic Acid
DNS	Domain Name System
DPI	Deep packet inspection
DRM	Digital Right Management
EC	European Community
ECHR	European Court of Human Right

E.D. Va.	Eastern District of Virginia
e.g.	*exempli gratia* - for instance
etc.	et cetera
et al.	*et alla* - and others
EU	European Union
EUR	Europe
EWHC	England & Wales High Court
F., F.2d, F. 3d	Federal Reporter, printed in three series
FDN	French Data Network
FIPC	French Intellectual Property Code
F.Supp.2d	Federal Supplement
FUP	Fair Usage Policy
GR	Graduated Response
HADOPI	The High Authority for the Dissemination of Works and the Protection of Rights on the Internet (Law: French Intellectual Property Code 2009) (in French: *Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet*) (Unofficial English translation available at: http://www.laquadrature.net/wiki/HADOPI_translation)
Hadopi	The High Authority for the Dissemination of Works and the Protection of Rights on the Internet (Organisation)
IAP	Internet Access Provider
Ibid	*ibidem* - in the same source
ICP	Internet Content Provider
i.e.	*id est* - that is to say
IEHC	Ireland High Court of Ireland
IFPI	International Federation of the Phonographic Industry
IHP	Internet Hosting Provider
Inc.	Incorporated
IP Address	Internet Protocol Address

IPRs	Intellectual Property Rights
ISP	Internet Service Provider
LL.M.	Master of Law
M.D. Fla.	Middle District of Florida
MPAA	Motion Picture Association of America
MPLS	Multi-Protocol Label Switching
MICT	The Ministry of Information and Communication Technology (of Thailand)
MOU	Memorandum of Understanding
N.D. Cal	Northern District of California
NP	Network Provider
N&S	Notice and Staydown
N&T	Notice and Takedown
NSP	Network Service Providers
op.cit.	*opere ciato* - in the work already cited.
p.	page
pp.	pages
PC 1956	Thailand Penal Code B.E.2499 (1956)
P2P	Peer-to-Peer
RIAA	Recording Industry Association of America
RPC	Rights Protection Commission
S.D.N.Y.	Southern District of New York
S.D.Tex.	Southern District of Texas
SP	Service Provider
TECA	Thailand Entertainment Content Trade Association
TPM	Technological Protection Measure
TRIPs	The Agreement on Trade-Related Aspects of Intellectual Property Rights
UGC	User-Generated Content
UMG	Universal Music Group

URL	Uniform Resource Locator
US	the United States of America
	Or the United States Supreme Court
U.S.C.	the United States Code
VCD	Video Compact Disc
WCT	WIPO Copyright Treaty
W.D. Wash	Western District of Washington
WIPO	World Intellectual Property Organisation
WPPT	WIPO Performances and Phonograms Treaty
www	World Wide Web

List of Tables

List of Figures

Chapter 1: Introduction

1.1 Introduction

The internet and digitalisation revolutionise copyright in terms of, e.g., creation, exploitation, infringement, extent of protection and enforcement. As copyright works can be in a digital form, where it is much easier to reproduce and adapt than in a material form, the risk is that more and more works are being infringed. The situation is exacerbated by the ease of communication which makes distribution of works so widespread and hard to control. A myriad of players are two key groups responsible for online copyright infringing activities: 1) commercial entities; and 2) individual end-users. Commercial entities are involved in, or contribute to, such activities by providing content, facilities and tools.[1] "End-users" can adapt, distribute and acquire copyrighted content without permission from content creators.[2]

In terms of protecting digital copyright works online, undertakings need to adopt different approaches. A business that infringes digital online copyright may be pursued by legal action in civil and criminal courts. However, protecting digital copyright works from infringement by internet end-users is more complex and is not easily resolved by traditional forms of enforcement litigations. The issues arising in this context include the rationale, process, practicality and proportionality of digital copyright online enforcement. These issues challenge any jurisdiction when seeking a suitable remedy or measure for end-user online copyright infringement protection and this includes the nation of Thailand.

1.2 Motivation for the Research

Digital copyright piracy is the main threat to creative content industries that could significantly disrupt their growth rates.[3] Globally, internet streaming (client/server

---

[1] Examples of such contributions are: a website, a server for an infringing website, a content storage site (cyber locker), search engines or a provider of potentially copyright-infringing programs.

[2] The term 'end-user' is defined in this thesis as 'an individual internet user, not a business or commercial entity, who uses the internet and, without permission, may distribute copyrighted content to the public, of which the activity is not classed as personal use that can be legitimate as fair use/dealing'.

[3] Organisation for Economic Co-operation and Development (OECD), 2009, *Piracy of Digital Content*. Available: http://www.oecd.org/sti/ind/piracyofdigitalcontent.htm p.23 [Accessed: 6 May 2014]. However, another research has found that in Europe, digital piracy has no effect on music sale. (Aguiar, L. and

---

technology), and P2P have dominated internet traffic.[4] In the Asia-Pacific region, video and audio streaming accounts for 50% of peak downstream internet traffic.[5] Client/server and Peer-to-Peer file sharing technologies dominate online digital copyright infringement. It is projected that one fourth, or to be more precise 28 per cent of internet users access unauthorized services every month.[6] Half of these are using peer-to-peer (P2P) networks.[7] Internet end-users are the primary infringers who employ these technologies and are responsible for copyright infringement.[8]

The statistics above suggests that a country should focus on internet streaming and P2P file sharing enforcement. This can be done on both the demand side (end-users) and the supply side (business/commercials). The demand side has its challenges in many respects. A large number of end-users engaging in similar wrongful activities undermine any justice system. Civil cases take-up time and resources and yield considerable negative publicity. Moreover, end-user infringers are likely to be "judgment-proof" -- 'meaning that they lack the financial resources to pay a substantial liability judgment'.[9] Criminal proceedings require a country's resources and raise issues of proportionality.

Thailand has encountered identical problems to those discussed above. The country has been criticised by its trade counterparts, e.g., the European Union (EU) and the US, regarding its inadequate online copyright protection measures. The EU alleged

---

Martens, B., 2013. *Digital Music Consumption on the Internet: Evidence from Clickstream Data,* [Online], Available at: http://www.scribd.com/doc/131005609/JRC79605 [Accessed: 23 June 2014])

[4] Between them, internet streaming traffic has surpassed that of global P2P. '[T]he prevalence of real-time entertainment traffic (Flash, YouTube, Netflix, Hulu, etc.) with a decrease in the fraction of P2P file sharing traffic is usually the result of cheap and fast Internet access and is more typical for mature broadband markets'. (Dunaytsev, R.; et al. 2012, "A Survey of P2P Traffic Management Approaches: Best Practices and Future Directions." *Journal of Internet Engineering*, 5(1) 318, p.318. Available at: http://www.jie-online.org/index.php/jie/article/viewFile/90/52 [Accessed: 2 May 2014]) Another survey finds the same result where real-time entertainment lead source of internet traffic with supplant files sharing activities back in a decade ago. (Sandvine, 2013, *Global Internet Phenomena Report,* [Online] p. 2 [executive summary]. Available at: https://www.sandvine.com/downloads/general/global-internet-phenomena/2013/2h-2013-global-internet-phenomena-report.pdf [Accessed: 2 May 2014])

[5] Sandvine, *ibid*.

[6] International Federation of the Phonographic Industry (IFPI), 2012. *Digital Music Report 2012*, Available at: http://www.ifpi.org/content/library/dmr2012.pdf [Accessed 23 October 2013] p.16. *See* also Envisional 2011, *Technical Report: An Estimation of Infringing Use of the Internet*, [Online] p.2. Available at: http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf [Accessed: 14 June 2014]. (In turn, "across all areas of the global internet, 23.76% of traffic was estimated to be infringing".)

[7] IFPI, *ibid*.

[8] The German court refused to block a website for reasons, *inter alia*, among which is that a right holder must try to pursue primary infringers first. (IP Kat, 2015. " BGH on blocking injunctions: first go after the source"[Online] Available at: http://ipkitten.blogspot.co.uk/2015/11/bgh-on-blocking-injunctions-first-go.html [Accessed: 20 May 2016])

[9] Teran, G. 1999, "ISPs Liability for Copyright Infringement" [Online], Available at: http://cyber.law.harvard.edu/property99/liability/main.html [Accessed: 19 June 2014] [emphasis in original]

that "[t]he Thai copyright law is considered not in line with technological advancement and the Thailand's actions against digital piracy have not been sufficient."[10] Similarly, the United States Trade Representative (USTR) asserted that Thailand remained on Priority Watch List (PWL) on the ground, *inter alia*, that Thailand needed "to establish improved legal mechanisms to address the rapidly growing problem of copyright piracy and trademark counterfeiting on the internet".[11] In Thailand, civil procedures are lengthy and expensive, provisional injunctions in digital online copyright enforcement matter are rarely granted.[12] Criminal sanctions appear to be an insufficient deterrent.[13] The author, as a public prosecutor in Thailand, found that, as yet, no right holder has ever attempted to apply for a court injunction to stop the distribution of copyrighted content online by an end-user, nor has an infringement case against such an end-user ever been initiated in the criminal or civil courts.

To address these problems, many countries have introduced legislation and procedures, e.g., the US N&T and France GR, which circumvent a traditional court procedure remedy. the US N&T and France GR systems are designed to deal with many infringing end-users. The world-renowned N&T is a cooperation system which puts a stop to quick, widespread dissemination of copyrighted content online. GR has a warning system and many desirable qualities such as educative and informative functions, the internet subscriber obligation principle, presumption of facts and its ability to deal with minor offences.[14] The challenge of identifying suitable digital copyright protection measures, through the development of current N&T and GR, motivates the author to conduct research on this topic to ascertain whether these enforcement remedies may be suitable for Thailand.

---

[10] European Commission, 2009. "Intellectual Property Rights - Deficient protection and enforcement." [Online]. Available at: http://madb.europa.eu/madb/barriers_details.htm?barrier_id=095301&version=3 [Accessed: 7 January 2014].

[11] The US., Office of United States Trade Representative, 2014. *2014 Special 301 Report*, p.46.

[12] European Commission, 2009. "Intellectual Property Rights - Deficient protection and enforcement." [Online]. Available at: http://madb.europa.eu/madb/barriers_details.htm?barrier_id=095301&version=3 (last updated: 11 September 2014) [Accessed: 22 July 2016]

[13] *Ibid.*

[14] Whether GR system is effective is in doubt. Some surveys found more than 70 per cent of P2P users would stop infringing but the number is lower than 10 per cent in some other surveys. (See Duke, 2012, "The Effectiveness of Anti-Piracy Laws; Lessons to Learn from Hadopi" [Online] Available at: http://legalpiracy.wordpress.com/2012/03/06/effectiveness-hadopi/ [Accessed: 25 June 2014])

1.3 Aim of the Thesis

The aim of this thesis is to propose a legislative framework for effective legal measures for Thailand digital copyright protection. The measures target the deterrence of end-user infringement in client/server and P2P file sharing technology.

1.4 Objectives of the Thesis

1.To investigate and identify in substantive law any gaps in application to digital copyright infringement on the internet;

2. To explore and compare the US Notice and Takedown (N&T) remedy and Thai Copyright Act No.2 B.E.2558 (2015) (hereinafter "CA 2015") § 32/3 court proceedings in order to identify the extent of their effectiveness, limitations and solutions to them, as regards the protection from client/server end user infringement[15];

3. To explore and compare the French Graduated Response(GR) remedy and Thai CA 2015 § 32/3 court proceedings to identify the extent of their effectiveness, limitations and solutions to them, as regards the protection of copyright in P2P file sharer infringement;

4.To construct and evaluate a proposed legislative framework for Thailand which responds to its culture and socio-economic context.

1.5 Methodology

The thesis involves documentary doctrinal research. The aim of this thesis is to construct a legal protection remedy for online copyright infringement because it is argued that Thailand substantive law is sufficient for online copyright protection. In supporting this argument, it will begin with identifying the scope of Thailand substantive law, i.e. Copyright Act 1994 (CA 1994), which confers to protected rights to the copyright creators.[16] In other words, it will find an answer to the question whether client/server and P2P end users activities, e.g., download, upload and file sharing, are in conflict with rights

[15] Slash (/) as used in "Section 32/3" is exactly the same as the legislated CA 2015. In the Thai legal system, slash is the conventional form and is used in order to add a section between two sections. CA 2015 adds Section 32/1, 32/2 and 32/3 in between Section 32 and 33 of Copyright Act B.E.2537 (1994).

[16] *See* Chapter 3: Thailand Substantive Copyright Protection Legislation Applicable to Client/Server and Peer-to-Peer User Infringement below.

conferred under CA 1994, e.g., reproduction, adaptation and communication to the public.[17] If the answer to the first question is in affirmative, to what extent these activities infringe copyright of others.[18] Having identified the scope of protection under substantive law, this thesis aims to demarcate the scope of remedial protection for online copyright enforcement under procedural law.[19]

The remedy provided under CA 2015 is a court proceedings remedy. It is argued that the current proceeding is not suitable in many respects. The court proceedings are impractical, expensive, and disproportionate especially when dealing with the problem of a large number of infringing end-users.[20] Many countries crack down on the users infringement problem by circumventing the court remedy. The development of Thailand's remedy requires the study of foreign countries systems. It follows that this thesis needs to employ a comparative legal study. Comparative law can be considered as an essential method of study towards the development of law in a specific country.

The thesis has chosen the US N&T and the GR of France as comparators. There are many reasons for this. First, these jurisdictions focus on end-users' internet client/server and P2P file sharing enforcement; the US N&T system is designed to apply with client/server (which is also applicable to internet streaming) and the GR of France with P2P. Second, these systems circumvent the court proceedings with the quick and cooperative actions by stakeholders. Moreover, they incorporate many other desirable qualities such as warning, education and information. Third, N&T and GR are studied and adopted by many countries in different parts of the world which guarantees its international acceptance.[21] Finally, the two systems have developed over time through usage and court interpretation that have revealed their advantages and disadvantages that Thailand can

---

[17] *See* chapter 3 – 3.2 Can Client/Server and Peer-to-Peer User Activities be classed as Civil Offences under Copyright Act B.E.2537 (1994)? *and* 3.3 Are Client/Server and Peer-to-Peer User Activities Criminal Offences under Copyright Act B.E.2537 (1994)?

[18] *Ibid*.

[19] *See* Chapter 4: Notice and Takedown: Thailand and US Approaches and Chapter 5: The Thailand and France Approaches to Graduated Response *below*.

[20] *See* 1.3 Motivation for the Research above for more details.

[21] *See notes 23 and 24 above*.

learn. Having elaborated benefits from these legislations, there are, however, potential limitations which also arise therein.

The limitations of the US selection subsist in the US legal principles. The US N&T system has developed over years through case law discussing principles of vicarious and contributory liability, i.e., ISP responsibility for third party infringement.[22] To solve the problem of inconsistent court precedent, the US Congress enacted ISP safe harbours legislation. The legislation instructs how an ISP can be shielded from liability without laying down the circumstances where an ISP is liable for the third-party infringement, i.e., internet subscribers. The ISP liability and exemptions have never been discussed by the Thai court and will be excluded as such a discussion is beyond the scope of this thesis. This thesis focuses only the N&T proceedings -- notification and the action to be taken by certain types of ISPs.[23] The question raised is, how an ISP will cooperate with the proposed remedy if it obtains no advantage in exchange.[24] In the last chapter of this thesis, the reasons why an ISP would wish to cooperate with the recommended legal remedies will be analysed. Although ISPs liability and their safe harbours are excluded from this study, the definition of ISPs, along with their functions are clarified because the definitions relate to the implementing functions of ISPs in legal remedies.

The discussion of the French jurisdiction in Chapter 5 of this thesis is limited to legal criminal proceeding and issues concerning end users and business entities. In order to initiate a criminal case in France, an official does not need consent from a right holder. If infringement persists after two warnings, the case must be referred to the prosecution and it is in the prosecution's discretion whether it will prosecute a repeat infringer or not.

---

[22] Throughout this thesis, the contractions "ISPs" represents Internet Service Providers, "IAPs" Internet Access Service Providers, "IHPs" Internet Hosting Service Providers and "ICPs" Internet Content Providers. The term "ISPs" is a common term for all types of the above service providers. It incorporates IAPs, IHPs and ICPs.

[23] An IHP and ICP, upon notification, responds expeditiously to remove, or disable access to, the infringing material; hence, notice and takedown. (17 U.S.C. § 512 (c)) There are other ISPs' safe harbours which are disregarded by this thesis because this thesis studies deterrence of end-user activities in client/server in application with N&T system which is not concerned with ISPs such as IAPs, ISPs' cache system or Information Location Tool. (17 U.S.C. § 512 (a), (b) and (d))

[24] To the certain extent, Thailand has adopted the US safe harbours principle in that, similar to the US ISP, a Thai ISP is safeguarded from copyright infringement and contractual liability if it implements the court order under § 32/3 and if it operates in its normal communication system. (CA 2015 § 32/2)

However, a copyright infringement charge in Thailand is a compoundable case, meaning that in order to initiate a public prosecution an inquiry official is required by the Thai law to receive a complaint from an injured person, i.e., a copyright holder.[25] Without such a complaint, any criminal inquiry is void. This affects the study in that a Thai copyright infringement case cannot be referred automatically to the prosecution. The prosecution must acquire a right holder's consent beforehand and must be aware of the fact whether such prosecution conflicts with a right holder's will.[26]

Another limitation to this thesis, concerns a recently changed policy for targeting infringers in France. France was the originator of GR as a response to end-user infringement. It now aims to deter commercially infringing organizations.[27] This thesis is pursuing an end-user approach, whereas the originator itself is shifting towards the pursuit of infringers in other areas for the following reasons. Firstly, in this thesis a preference has been shown for the study of mechanisms which can be used for end-user deterrence. Secondly, while France changes its priority, "most countries target infringement from both the supply-side (content providers and other companies that facilitate access to material that infringes copyright online) and the demand-side (individual subscribers)".[28] Finally, P2P user deterrent measures can be different from those directed towards commercial organizations. An approach towards end-users can also

---

[25] Thailand Criminal Procedure Code B.E.2477 (1934) (CRPC 1934) § 121 states:
"The inquiry official is empowered to undertake an enquiry in criminal affairs.
In case of compoundable offences, an enquiry shall not be initiated unless a complaint is lodged."
Moreover, if a right holder has lodged a complaint, the right holder is entitled to withdraw the complaint and the prosecution is dismissed at any stage of prosecution, from the inquiry to before the court decision. (CRPC 1934 § 126)

[26] *See recommendation 1 in* 6.5.2 Recommendations for Thailand in Adopting the Principles of France and Graduated Response Remedy for Peer-to-Peer Online Copyright Protection.

[27] France, Hadopi, 2013. *Report on the prevention of unlawful streaming and direct downloading*, Available at: https://hadopi.fr/sites/default/files/page/pdf/Rapportstreaming_eng.pdf [Accessed: 7 October 2016]. (*See also* France, Minister of Culture and Communication, 2015. Press Release: *Government strategy on the fight against piracy of works on the Internet*, [Online] Available at: http://www.culturecommunication.gouv.fr/Presse/Communiques-de-presse/Lutte-contre-le-piratage [translated by Google Translate][Accessed: 7 October 2016].

[28] United Kingdom, Intellectual Property Office, 2015. *International Comparison of Approaches to Online Copyright Infringement: Final Report,* Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/404429/International_Comparison_of_Approaches_to_Online_Copyright_Infringement.pdf [Accessed: 30 June 2016]. p.2.

be employed in addition to that of business organizations. A country does not have to choose one kind or another.

Given the above limitations in US and France selection, this thesis can effectively employ the functional comparative law methodology. A comparative functionality is of the comparative law methods and is the method of study here. "It is particularly concerned with how to compare the law's consequences across legal systems and therefore allows rules and concepts to be appreciated for what they do, rather than for what they say."[29] The functional method has five steps.[30]

First, it directs towards the law's surface explanation in a home country, i.e. Thailand, through its CA 2015 court procedure. This explanation can be gained from institutional and academic commentary as well as other resources. It should be an objective explanation, that is, free from any critical evaluation.[31] The rules of Thailand CA 2015 will be described through its legislative framework and commentary. Essentially, the thesis will disclose the history and purpose of the CA 2015. It will illustrate how the CA2015 § 32/3 remedy deals with protection from client/server and P2P infringement. Clarification of ISPs definitions and their classification under § 32/3 and relevant legislation is included. The thesis explores provisions regarding types of ISPs that are subject to court order in client/server and P2P information exchange. Moreover, for the purpose of comparison between Thailand and France, this step explores if Thailand legislation has similar principles to that of GR's, e.g., subscriber obligations and presumption of guilt, copyright infringement as the minor offence, internet suspension.

Secondly, the functional aspects of the CA 2015 provisions are considered. The law as interpreted by institutions such as government agencies, or even the court, through its decisions will be critically analysed. "As a consequence, its objects are often judicial decisions as responses to real life situations, and legal systems are compared by

---

[29] Brand, O. 2007, "Conceptual Comparison: Towards a Coherent Methodology of Comparative Legal Studies", *Brooklyn Journal of International Law*, 32(2), 405-466. p.409.

[30] *Ibid.*

[31] Zweigert, K. and Kotz, H., 1987, *An Introduction to Comparative Law*, 2nd ed. Oxford: Oxford University Press. p. 41.

considering their various judicial responses to similar situations."[32] Thailand judicial decisions on CA 2015 § 32/3 as responses to client/server and P2P infringement are raised here. As CA 2015 only came into force in August 2015, there are, as yet, no current examples of its judicial consideration or judgments. Therefore, the research will attempt to clarify issues, e.g., the make-up of a filed motion acceptable to the court, the court consideration in granting the order, by inferring the Supreme Court's ruling on a motion pursuant to interlocutory injunction provisions under Civil Procedure Code B.E.2477(1934) (CIPC 1934). The inference is necessary for some reasons. First, the interlocutory injunction is somewhat similar to CA 2015 court injunction as they aim to cease the ongoing illegal actions and/or damages. Secondly, in its decision the Supreme Court used terminology similar to that of CA 2015 § 32/3, e.g., 'necessary', 'reasonable', which can be interpreted in the same fashion as those of CA 2015 §32/3.

Moreover, this second step will examine how a motion requesting the court order similar to sanctions provided by N&T and GR can be regarded as 'necessary' and/or 'reasonable'. In client/server, a request of taking down content in service provider systems, and of disabling access to the content, is discussed its probability and effect. In P2P, a request of sending warning notifications and internet connection restriction is examined. These will be shown in relevant sections under chapter 4 (discussing client/server) and 5 (discussing P2P). In some instances, it is necessary for this step to uncover the law when it applies to client/server and P2P technologies in forms of legal argument rather than functions because there has been no comparable court interpretation of CA 2015 § 32/3.[33] For example, types of ISPs affected by the court order under CA 2015 § 32/3 and the extent of the court order--how the court can interpret "to cease the infringement". Moreover, the thesis will identify certain potential practical limitations in the application of the CA 2015 court system to client/server and P2P users infringement in Thailand.

---

[32] Michaels, R. 2006, "Chapter 10: The Functional Method of Comparative Law" In: Reimann, M. and Zimmermann, R., eds. *The Oxford Handbook on Comparative Law*, Oxford: Oxford University Press, 2006. p.342.

[33] This approach is similar to some works. (*See Ibid*., p.341. "Stefan Vogenauer explicitly places his comprehensive comparative study of statutory interpretation within the functional tradition, although his analysis focuses on forms of legal argument rather than functions.")

Thirdly, the functional aspects of foreign legal systems, i.e. the 17 U.S.C. § 512 and relevant French Intellectual Property Code (FIPC) provisions, will be considered. The thesis will discuss response of these jurisdictions to the same problem, i.e. client/server and P2P users infringement, the method of which follows.

In the US paradigm, it will discuss court interpretation of ISPs definitions and functions in N&T procedure in client/server users infringement remedy. In essence, it will deliberate how 17 U.S.C. § 512(k)(1)(B) ISPs definitions incorporates different ISPs safe harbours under 17 U.S.C. § 512 (a)-(d). It will identify types of ISPs, i.e. websites (Internet Content Providers) (ICPs) and/or website hosting services (Internet Hosting Providers) (IHPs), affected by N&T remedy under 17 U.S.C. § 512 (c). Moreover, the research will identify certain potential practical limitations. The N&T system is in the process of amendment by the US Congress. The research will explore legal issues raised by the US Congress Sub-Committee as to what the limitations are and how the amendment will overcome them.

In French model, arguments will be raised as to why ISPs, e.g., ICPs, IHPs, are less involved in the GR system and how some type of ISPs, i.e. IAPs, involves in the system. It will discuss how French courts apply the HADOPI Act. It will disclose how the law is interpreted by the French and European courts when they consider legal principle and procedure under the HADOPI Act. These courts decisions will be explored with regard to identifying the justifications that underpin the GR principles (e.g., subscriber obligations, reverse burden of proof, and presumption of guilt in minor offence) and its remedial proceedings (e.g., IP addresses disclosure, mail notification, internet disconnection) in relation to the fundamental rights guaranteed by French Constitution and EU legislation such as freedom of speech, presumption of innocence, right to privacy.

Fourthly, the research will identify the DMCA 1998 N&T and FIPC GR provisions. It will consider their procedural remedies through their legislation history.[34] Regarding the DMCA 1998, it will examine how the law was intended to be, what relevant N&T

[34] History, religion, geography, morals, custom, philosophy or ideology, are among the substructural forces that influence law. (Eberle, E.J., 2009. "The Method and Role of Comparative Law", *Washington University Global Studies Law Review*, 8(3), 451, p. 452.)

provisions can be used in client/server infringement, which sorts of ISPs, under 17 U.S.C. § 512, practice N&T in a given situation and how the N&T system works. With FIPC, it will examine GR's historical background, creation of subscriber obligation for P2P online copyright protection, Hadopi and its subordinate, and GR procedure.

The fifth and final step involves the actual process of comparing the laws and their functions, the proposal of legislative framework of Thailand, and evaluation of the framework. The ISPs in N&T system will be compared with that of Thailand. Points of comparison will include the relevant element similarities and differences regarding ISPs definitions and operations. For example, whether the definitions of ISP under the US jurisdiction differ from those in Thailand, whether the interpretation of the definition of ISPs takes into account the operations of ISPs. Moreover, comparative law principle of functional equivalence will take part in this step. Institutions such as ISPs, Court and Hadopi, though doctrinally different ones, are comparable institutions because they are 'functionally equivalent' in fulfilling the same function.[35] They fulfil the function of online copyright protection. This thesis will discuss how these institutions respond to end-user online copyright infringement. For example, how the Thai court reacts to different requests in the motion against client/server end-user infringement and how the US ISPs react to the similar situation.

Moreover, for the purpose of its legal reform and evaluation, Thailand's system can be considered against the French functioning legal system.[36] Thailand's legal principles, remedial proceedings and extent of the remedies will be contrasted with those that exist in France. For example, Thailand lacks the French legal theory relating to, e.g., monitoring duty on part of internet subscribers, minor offence and presumption of guilt which will be examined. Thailand's lack of GR mail notification will be compared and contrasted with its current 'cease and desist' letters including practical aspects of notification, internet access restriction and traffic management in the context of Thailand.

---

[35] Michaels, R. 2006, *op.cit.* p.342.

[36] "One's own system can be put in a perspective with another functioning legal system, for the purposes of evaluation, and especially for the purpose to reform one's own valid law." (Karhu, J. 2004. "How to Make Comparable Things: Legal Engineering at the Service of Comparative Law" In: Hoecke, M.V., ed. *Epistemology and Methodology of Comparative Law*, Oxford: Hart Publishing, 2004. p. 81.)

The analysis will reveal the advantages and disadvantages of the objects under comparison. It will be used as a foundation that forms part of a recommendation for the development of Thailand's digital copyright protection law. This thesis will construct a suitable legislative framework by taking advantages of different legal systems while solving their limitations, while evaluating the legal framework. For example, should Thailand adopt a system of N&T proceedings to replace its existing court remedy? How would the adoption of N& T proceedings benefit Thailand's online copyright protection system, e.g., avoidance of violation of due process and freedom of speech? How might Thailand overcome circumstantial limitations to the US system, e.g., a large number of notices and recurring posting of infringing works? On the other hand, should Thailand decide not to adopt the foreign method, what are solutions to the problems inherent in the Thai court proceedings in terms of efficiency, due process, and end-users' awareness and acknowledgement?

In relation to the GR system, should Thailand adopt the French model legislation as a solution to P2P user infringement? If so, how should Thailand approach the adoption and what are benefits? This thesis will evaluate necessity of compulsory copyright protection terms and information in the internet subscriptions, storage of traffic data under CROA 2007, advantages of principles such as subscriber duty, presumption of guilt, minor offence in solving anonymous nature of end user identity. It will highlight importance of avoiding inferred fact in civil litigation from criminal prosecution. This includes illuminating the desired aspects of noticing/warning system in raising users' awareness and promoting education. Finally, the thesis will suggest and assess potential solutions to the French approach which involves the draconian suspension internet access by P2P users through the introduction of technological assistance, e.g., traffic management, internet disconnection.

In conclusion, this thesis attempts to develop Thailand's online copyright protection remedy as a key aspect of its digital online copyright infringement legal framework by employing functional comparative legal method. The study will be conducted following the traditional functional method. It begins by studying the mother country legislation, its functional aspects, followed by the selected foreign jurisdictions

)the US and France) with a view to answering the research question as to how to develop an effective legal online copyright protection remedy for Thailand.

1.6 State of the Field and Deficits in the Current Research and Literature and Contribution to the Knowledge

Thailand's intellectual property rights regime appears to have sufficient substantive law against copyright infringement activities, but it needs a suitable system that supports enforcement.[37] The CA 2015 came into force on 4th of August 2015. Section 32/3 provides copyright holders with a process to apply for court order/injunction to stop online infringement. To date, there has not been any current Thailand research or literature discussing any application of CA 2015 section 32/3, including any application to end-user infringement through client/server and P2P. Moreover, there exists no current Thailand research or literature comparing CA 2015 § 32/3 with N&T and GR. It follows that a contribution to knowledge can be seen as a comparative and critical discussion of these issues with suggestions for legal reform in Thailand within the online digital copyright protection discipline.

1.7 Scope of study

1.7.1 End users accessing internet at home.

This thesis is limited to the study of infringement by end-users who use the internet at home. In Thailand, in 2012, a majority 50.6% of users used Internet at home.[38] Educational institutions were next at 47.3 % and usage at working offices was third at

[37] 'A survey conducted by WIPO in 2002 indicated that the principal barriers to eliminating counterfeiting and piracy did not subsist in the substantive law, but rather in the remedies and penalties available (or not available) to stop and deter counterfeiting and piracy'. (Blakeney, M. n.d., "Guidebook on Enforcement of Intellectual Property Rights" [Online]. Available at: http://trade.ec.europa.eu/doclib/docs/2005/april/tradoc_122641.pdf [Accessed: 10 Nov. 2013])

[38] Thailand, National Statistical Office (NSO), n.d., "The Household Survey on Information and Communication Technology", [Online] p. ix. Available at: http://web.nso.go.th/en/survey/data_survey/560619_2012_Information-.pdf [Thai] [Accessed: 3 June 2014]. Electronic Transactions Development Agency (Public Organization)(ETDA) is another Thailand institution that has recently conducted survey on Thai internet user's behaviour in 2015 which shows that 87.6% of respondents use the internet at home, with 49.5% and 19.7% using it at an office or a university respectively. (Thailand, ETDA, 2016, *Thailand Internet User Profile 2016*, [Online] Available at: https://www.etda.or.th/publishing-detail/thailand-internet-user-profile-2016-th.html [Thai] p.44. [Access: 14 October 2016].)

30.7%.[39] This data suggests that the thesis should focus on home users. There should be less difficulty in copyright protection and enforcement in universities or work places because the identity of end users is easily confirmed and proved as access to the internet at such venues usually requires identification prior to logging on.

1.7.2 No Technological Protection Measure (TPM)

The TPM protects copyright work from unauthorised access and reproduction. This thesis excludes TPM because the coverage of the issue would be too extensive.[40]

1.7.3 Domestic Infringement, not International.

The thesis does not include the problems associated with the investigation or the jurisdiction of the court. Although the internet is borderless, the measures are only aimed at practices within the jurisdiction of Thailand. Clearly, foreign ISPs and end users cannot be forced by Thai laws as they do not come under a Thai jurisdiction. Where this is relevant Thai copyright owners may use the N&T and GR legislation as recommended in this thesis, but successful enforcement action wholly depends on the foreign ISPs and users whether they wish to cooperate.

1.7.4 Copyright Infringement Exception Exclusion

Throughout this thesis, a discussion of statutory fair use or other copyright exemptions is avoided simply because such a discussion could lead to excess in word constraint. In other words, whether or not the allegedly infringing client/server and P2P activities are exempted from infringement is not included in this study.

The following section, chapter 2, will examine the theoretical justifications underpinning the N&T and GR systems. This chapter will also shed light on relevant technological aspects of this thesis and include a discussion of current trends in the field of digital infringement and legal online copyright enforcement techniques. Potential digital copyright enforcement remedies, along with thoughts on copyright infringement detection and the identification of infringers, will be critically analysed.

---

[39] When considering the activity of using the Internet, it was used mostly for downloading movies or listening to the radio or to music, recorded at 64.6%'. (Thailand, National Statistical Office (NSO), *Ibid*.)

[40] Thailand is not yet a signatory state to the two World Intellectual Property Organization (WIPO) treaties which deal with copyright protection in technological progress -- (1) the WIPO Copyright Treaty (WCT); and (2) the WIPO Performances and Phonograms Treaty (WPPT)-- which outline TPM.

Chapter 2: Justification for Digital Copyright Protection Remedies and Technological Aspects of Protection of Copyright on the Internet

2.1. Justification and Characteristics of Digital Copyright Protection Remedies

The rationale for copyright protection is on a collision with the fundamental rights guaranteed by a democratic regime such as freedom of speech, right to privacy, etc. For decades, the existence of copyright and the necessity of its protection have been well accepted. As a materialised copyrighted work must be protected, so must a digitalised one. The fundamental issue here is how far can enforcement measures be taken without interfering with fundamental rights. This section attempts to find justification for both online copyright measures and other rights such as freedom of speech. In doing so, it examines two measures -- The Notice and Takedown (N&T) System and The Graduated Response System (GR).

2.1.1 The Notice and Takedown (N&T) System

There are many arguments against N&T on different grounds.[1] Perhaps the most important one is that it denies individual users freedom of speech and due process. In an American case, the Ninth Circuit court in *Perfect 10, Inc. v. Ccbill Llc* stated:

"Accusations of alleged infringement have drastic consequences: A user could have content removed, or may have his access terminated entirely. If the content infringes, justice has been done. But if it does not, speech protected under the First Amendment could be removed."[2]

[1] For examples, a notice may run counter to legitimate fair use, it may be produced by an entity which is not a copyright holder of the dispute material, the dispute material may not be copyrighted, a notice can be overly broad that it causes a shutdown of the whole website rather than solely infringing content, etc. (Lee, Y.H. 2015, *Copyright and Freedom of Expression: A Literature Review,* [Online] Available at: http://www.create.ac.uk/publications/copyright-and-freedom-of-expression-a-literature-review/ pp.160-161. [Accessed: 15 July 2017])

[2] 488 F. 3d 1102, 1112 (9th Cir. 2007)

When a notice is produced and sent to an ISP by a right owner claiming infringing content furnished by an end user in the ISP's system, the ISP takes down the requested content without verification.[3] In doing so, the ISP is incentivized by the benefit from safe harbours from two risks -- copyright infringement liability and default of subscription liability.[4] In this circumstance, the system can deter freedom of expression of a user and limit his right to due process.[5] In order to prevent this occurring, it is argued that a notice should not be easily produced by a right holder. The right holder should investigate the infringement before the notice can be filed. The case below discussed this issue.

In another American case, *Rossi v. Motion Picture Association of America*, Michael J. Rossi produced the "internetmovies.com" website.[6] The website provided directory of websites containing information about movies which he described it as an "online magazine".[7]

The Motion Picture Association of America (MPAA) was a right holder representing its members, the movie studios, in preventing unauthorized copying, transmittal, or other distribution of the studios' motion pictures.[8] The MPAA found that Rossi's website showed the following statements: "Join to download full length movies online now! new movies every month"; "Full Length Downloadable Movies"; and "NOW DOWNLOADABLE."[9] These statements were followed by graphics for a number of the MPAA's copyrighted motion pictures.[10] The MPAA viewed the website and believed that Rossi was illegally infringing

---

[3] 17 U.S.C. § 512 (g)(B)(C)

[4] *See e.g.,* Concepcion, C.M. 2010, "Beyond the Lens of Lenz: Looking to Protect Fair Use During the Safe Harbor Process under the DMCA", *George Mason Law Review*, 18, 219, p.236, 240; Seltzer, W. 2010, "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment", *Harvard Journal of Law & Technology*, 24, 171, pp. 181-182; Lemley, M.A. 2007, "Rationalizing Internet Safe Harbors", *Journal on Telecommunication & High Technology Law*, 6, 101, p. 114.

[5] Hugenholtz, P. B., 2012, "Codes of Conduct and Copyright Enforcement in Cyberspace." In Stamatoudi, I.A., ed. *Copyright Enforcement and the Internet*, Amsterdam: Kluwer Law International, 2010, p.317. Available via SSRN: http://ssrn.com/abstract=2017581

[6] 391 F. 3d 1000, 1001 (9th Cir. 2004)

[7] *Id. at* 1002

[8] *Id.*

[9] *Id.*

[10] *Id.*

on its copyrighted materials.[11] The MPAA filed several notices to Rossi and his Internet service provider (ISP) asserting the infringement.[12] As a result, his website was shut down before it operated again within a new website host. According to Rossi, internetmovies.com was offline for "[a]pproximately 1 second to 72 hours," and the amount of money he lost due to the website's shutdown was "unmeasureable."[13]

Rossi brought various tortious claims including libel, defamation and intentional infliction of emotional distress.[14] The District Court granted a motion for summary judgment in favour of MPAA.[15] It held that the MPAA "had more than a sufficient basis to form the required good faith belief that [Rossi's] site contained infringing content prior to asking [the ISP] to shut down the site."[16]

Rossi appealed to the circuit court that MPAA did not attempt to download any movies from Rossi's website or any links to the site. Rossi argued that had it done so, it would have been no question that no content can be retrieved. Therefore, Rossi contended, the MPAA did not provide sufficient information to constitute a "good faith belief" under § 512(c)(3)(A)(v) that he infringed the MPAA's copyrights.[17]

The Ninth Circuit court had before it the dispute whether a right holder must conduct a reasonable investigation in making the judgment the alleged infringement, or the holder's belief is purely subjective that the use of the material is not authorized.[18] The court answered this question by affirming the District Court's ruling. It ruled that case law indicated "a good faith belief" standard is rather subjective than objective.[19] When comparing the 'a good faith' phase of this case with the same words shown in other federal statutes, it concluded that the reasonableness is an objective standard, which is

---

[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id* at 1003.
[18] Id at 1004.
[19] *Id.*

distinct from the subjective good faith standard.[20] Moreover, DMCA suggested that Congress did not put an objective standard of reasonableness when it could have done so.[21] This indicated "an intent to adhere to the subjective standard traditionally associated with a good faith requirement."[22] Legislative structure of DMCA predicated the interpretation that a right holder could be liable for misrepresentation of the allegedly infringing content only if there was some degree of actual knowledge on part of the right holder that the website was not actually infringing.[23] An unknowing mistake and unreasonably making a mistake did not qualify for the 'good faith' standard.[24] Finally, because the website contained statements such as "Join to download full length movies online now! new movies every month"; "Full Length Downloadable Movies"; and "NOW DOWNLOADABLE", it led the MPAA employee and Rossi's customers to conclude in good faith that motion pictures owned by MPAA members were available for immediate downloading from the website. "There is little question that these statements strongly suggest, if not expressly state, that movies were available for downloading from the site."[25]

The ruling in *Rossi* sets the precedent in the US that courts in the same and different circuits follow.[26] *Rossi* confirmed the DMCA language directing the court's

---

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.* at 1004-1005. *See also* 17 U.S.C. § 512(f) "Any person who *knowingly materially misrepresents* under this section — (1) that material or activity is infringing, or (2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages...." [Emphasis added]

[24] *Id* at 1005.

[25] *Id*. [Internal citation omitted.]

[26] In the US, there are twelve different United States regional circuits each of which has one United States court of appeals, i.e., the circuit courts (13 courts nationwide including the Court of Appeals for the Federal Circuit that hears appeals in specialized cases, e.g., patent laws, international trade claims). A circuit court has geographical jurisdiction over the United States district courts (94 courts nationwide). A US district court is a trial court that has subject matter jurisdiction over federal issues including that of copyright. A US district court and a US circuit court is only bound by its own circuit court's precedent, not other's. (In cases where there appear different rulings laid by different circuit courts, the US Supreme Court is able to grant *certiorari* (that is, they agree to hear a case) in order to settle the circuit court conflict of rulings.) (Federal Bar Association, n.d., "About U.S. Federal Courts", [online] Available at: http://www.fedbar.org/Public-Messaging/About-US-Federal-Courts_1.aspx [Accessed: 27 October 2017])

Rossi is followed by subsequent cases decided by the Ninth Circuit itself in *Lenz v. Universal Music Corp.* 801 F.3d 1126 (9th Cir. 2015) and by district courts located in other circuits, for examples, the US District Court for the District of Colorado (in the Tenth Circuit) in *Dudnikov v. MGA Entm't, Inc*., 410 F. Supp. 2d 1010 (D. Colo. 2005), the US District Court for the Northern District of Ohio (in the Sixth Circuit) in *Smith v. Summit Entertainment LLC.*, No. 3: 11CV348 (N.D. Ohio June 6, 2011) and the US District Court for the

---

interpretation of the 'good faith' to the subjective standard. A right holder need not conduct reasonable investigation as to when the allegedly infringing content is permitted under the statutory fair use. Still, the right holder is required to consider fair use before sending a notice[27] because fair use is "authorized by the law"[28]. Such consideration is subjective in that it is simply part of 'initial review' of the potentially infringing material[29] and 'need not be searching or intensive'[30].

In addition, there is justification of the N&T procedures subsisted in the *Rossi* case. As the court stated § 512 was intended to "balance the need for rapid response to potential infringement with the end-users *[sic]* legitimate interests in not having material removed without recourse."[31] Inflicting an investigative duty on part of the right holder before filing a notice could have affected the efficacy of the system expected by the provisions. The ruling in this case may discomfort those who are proponents to freedom of speech. Theoretically speaking, as a notice is easily produced by a right holder on a subjective standard, freedom of speech is easily diminished. Practically speaking, this argument is weak. The actual, current situation is largely different from the theoretical scenario. Allegedly infringing content can be reposted a moment after take down.[32] This seems to be a problem of a notice sender more than that of the repost end-user especially when a large amount of reposting is concerned and when an individual creator herself,

---

District of Massachusetts (in the First Circuit) in *Tuteur v. Crosley-Corcoran, No. 13-10159-R6S, 2013 WL 4832601 (D. Ma. 2013)*.

[27] *Lenz*, 801 F.3d at 1132, 1134-1135.

[28] 17 U.S.C. § 512(c)(3) provides in part:

"(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

...

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of *is not authorized by* the copyright owner, its agent, or *the law*." [Emphasis added] (See also *Lenz*, 801 F.3d at 1132.)

[29] *Lenz v. Universal Music Corp.,* 572 F.Supp.2d 1150, 1155 (N.D.Cal.2008)

[30] "A copyright holder who pays lip service to the consideration of fair use by claiming it formed a good faith belief when there is evidence to the contrary is still subject to § 512(f) liability." (*Lenz*, 801 F.3d at 1135)

[31] *Rossi.* 391 F. 3d at 1003

[32] Cobia, J. 2009, "The Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process", *Minnesota Journal of Law, Science & Technology*, 10(1), 387, p.393.

not a representing collection society, needs to file a notice to the re-postings. Chapter 4 of this thesis will readdress issues of reposting infringing content, the advantages and disadvantages of the current N&T system, while chapter 6 will characterise a system that compromises between freedom of speech and copyright.

2.1.2 The Graduated Response System (GR)

The GR system, like other legal enforcement measures, has pros and cons. On the positive side is that there is no human rights argument or any other arguments against educative and informative aspects of GR. On the negative, there are GR aspects that have been charged with conflict with human rights and principles, *inter alia*, privacy, freedom of speech, and proportionality.[33]

On a right to privacy, the question is whether (and/or to what extent) GR is invasive of the individuals' right to privacy. In the first place GR involves surveillance of user internet activities in order to detect illegal file sharing via the file sharer's IP address.[34] "IP addresses constitute a crucial element of the alleged copyright infringers' identification."[35] The IP address itself is not the identifier but it can be associated with other information and processed by the subscriber's ISP to reveal user's identity.[36] In pertinence, it is disputed whether a user's IP address in a P2P client is personal data and whether a right holder can collect and process such data for copyright enforcement purpose. These questions are intertwined. Whether or not an IP address is personal data will depend on who collects such a data and whether that person is able to associate such data with another information to identify the data subject, i.e., an internet account subscriber.

In *Scarlet Extended v. SABAM*, the Court of Justice of European Union (CJEU) ruled an IP address can be personal data from Internet Access Providers' (IAPs) perspective if

---

[33] Giblin, R. 2014, "When ISPs Become Copyright Police", *IEEE Internet Computing*. 18(2), 84, p.86.

[34] Deep packet inspection is the device that uses specialized high-speed hardware and software that can identify P2P packets in real-time. It distinguishes P2P traffic, or even just traffic from a single P2P application, blocks it or reduces its available bandwidth. (Werbach, K., 2005, "Breaking the Ice: Rethinking Telecommunications Law for the Digital Age"*, Journal on Telecommunication and High Technology Law,* 4, 59, p.92.)

[35] Konstantinou, I., 2013. *The compatibility of a Graduated Response System at EU level with the fundamental human rights to privacy, data protection and freedom of expression*. LL.M. thesis, Tilburg University. p.35

[36] *See* 2.4.1 Internet Protocol Addresses (IP address) and Internet Account Identification *and* 2.4.2 Process of Identification of Infringement and Precise Wrongdoers *below*.

IAPs themselves can process the data to precisely identify the data subject (or a natural person).[37] Right holders themselves cannot precisely identify the data subject because they need to seek for disclosure of such data from IAPs. This may mean that the IP address is not deemed personal data to them.

In *Breyer v Bundesrepublik Deutschland*, the same court held that an IP address can also be personal data if a possessor of such data (e.g., website operators and Internet Hosting Providers (IHPs) who record a visitor's consultations on the website) is able to identify the visitor by the legal means.[38] By analogy, an IP address of a P2P user is a personal data if it can enable a collecting right holder to identify the user by legal means. This leads to the next question, whether a right holder is capable of revealing the user's identity via an IP address. In practice, a right holder cannot know the subscriber unless he proceeds to legal means to disclose such information. Whether he can request disclosure of users' identity for civil proceedings is answered by CJEU.

In *Promusicae v Telefónica*[39], Promusicae was a non-profit organisation representing producers and publishers of musical and audiovisual recordings. It applied to the Commercial Court for preliminary measures against the IAP, Telefónica, who provided internet access services for the public. In the application, Promusicae requested that Telefónica disclose the identities and physical addresses of persons whom Telefónica provided with internet access services and whose IP address and date and time of connection were known. According to Promusicae, such persons used the KaZaA file exchange program (P2P) and shared in personal computers files of phonograms in which the members of Promusicae held the exploitation rights; hence infringement of its copyright. It therefore sought disclosure of such information in order to be able to bring civil proceedings against the persons concerned. The Commercial Court judge decided to stay the proceedings and refer the following question to the CJEU for a preliminary ruling:

"Does Community law, specifically Articles 15(2) and 18 of Directive [2000/31], Article 8(1) and (2) of Directive [2001/29], Article 8 of Directive [2004/48] and Articles

---

[37] *Scarlet Extended v. SABAM*, Case C-70/10, para 51

[38] "[A] dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person." (*Breyer v Bundesrepublik Deutschland*, Case C 582/14, para 65)

[39] Case C 275/06

17(2) and 47 of the Charter … permit Member States to limit to the context of a criminal investigation or to safeguard public security and national defence, thus excluding civil proceedings, the duty of operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services to retain and make available connection and traffic data generated by the communications established during the supply of an information society service?"[40]

In ruling the case, CJEU weighed between different Community Directives.[41] It held that these laws do not require the Member States to lay down an obligation to reveal personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, in application to the mentioned directives the Member States were required to strike a fair balance between the various fundamental rights taking into account of the other general principles of Community law, such as the principle of proportionality.

According to *Promusicae*, a Member State is not required to have a legislation that allows revelation of P2P users' IP addresses in a civil litigation. However, if it decides to do so, the legislation and the interpretation thereof must strike the balance of individual property protection and fundamental right to privacy taking into account other principles such as proportionality. In a more recent case, CJEU more directly contemplated the point in question.[42] It ruled that a Member State is able to legislate a law that permits an IAP in civil proceedings to identify an internet subscriber to whom the IAP provides an IP address which is allegedly used in copyright infringement.[43] It could be concluded that disclosure of users' identity for the purpose of copyright infringement enforcement in civil cases is

[40] *Ibid.*, para 34.

[41] In total, the Directives were Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[42] *Storyside AB v Perfect Communication Sweden AB*, Case C 461/10

[43] *Ibid.*

principally allowed. It is left to the Member States to provide the implementing law which balances the competing rights.[44]

In light of these CJEU rulings, an IP address can be personal data if it is processed by a person who himself is able to identify the IP address user or is able to manage to identify the data subject by legal proceedings. An IP address is uncertainly personal data when it is acquired by a right holder because whether a right holder is able to file a legal proceeding to disclose an end user in civil case or not will depend on EU Member States legislation. The legislation must balance between private property right with public fundamental rights taking into consideration other principles such as principle of proportionality. It is well-accepted that identity of users' IP addresses can be disclosed for the purpose of criminal prosecution.[45]

Lastly, a human right which may be restricted by GR is freedom of speech. This perhaps acquires the most attention. French internet suspension was criticized as being one of the most draconian sanctions taken against account owners.[46] It was argued that GR undermines freedom of speech when it authorizes disconnection to the internet.[47] An internet connection can be considered as part of the fundamental right to freedom of information.[48] In many countries the availability of the internet forms part of an infrastructure policy. Not allowing access to the internet goes especially against a strong argument for proportionality. While website blocking and content filtering deny users access to specific websites or content on the Internet, disconnection cuts users off from the Internet entirely.[49] Frank La Rue, the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, noted:

---

[44] Different countries have different implementation. In England and France for example, ISPs are only obliged to divulge personal details in response to a legal order. (Muir, A., 2013. "Online copyright enforcement by Internet Service Providers." *Journal of Information Science*, 39 (2), 256. p.264)

[45] In Italy and Germany, the courts have ruled that ISPs may only disclose subscriber data for the purpose of criminal proceedings. (*Ibid.*)

[46] Yu, P.K., 2013, "Digital Copyright Enforcement Measures and Their Human Rights Threats" in Geiger, C. ed., *Research Handbook on Human Rights and Intellectual Property*, Edward Elgar Publishing, 2015, p.11. Available at: http://ssrn.com/abstract=2363945

[47] *Ibid.*

[48] The French Constitution Tribunal Decision no. 2009- 580 (*See* chapter 5 -- 5.4.4 Should termination of internet access be Supplementary to minor offences?)

[49] Rue, F.L., 2011. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, para. 78, A/HRC/17/27.

"The Special Rapporteur considers cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, to be disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights."[50]

In order to discuss the proportionality aspect of the penalty of internet disconnection, "it is worth comparing the disconnection initiated by the graduated response system against the limited Internet access still enjoyed by prisoners and parolees".[51] In the US, an absolute prohibition on accessing computers or the internet on a supervised release condition splits circuit court decisions. In *United States v. Paul*, the 5th Circuit ruled "the supervised release condition at issue in the instant case is reasonably related to Paul's offense and to the need to prevent recidivism and protect the public".[52] However, the 10th Circuit disallowed such a condition by ruling that the condition was greater than necessary and fails to balance the competing interests.[53] In fact, the inherent nature of punishment is to enjoin absolute liberty to which a common citizen is entitled.[54] In these cases, disconnection cut off users from internet access completely. GR does not completely cut off a user from the internet but merely disconnects the internet at home.[55] A newspaper reader who cannot receive it via home delivery can read the newspaper anywhere. A subscriber who cannot access the internet at home can access the internet at a library, café or via a mobile service, etc. In light of this argument, a disconnection can be justified. If disconnection really has no justifiable grounds and is to be rejected, then the online copyright infringement solution that seems to be most acceptable to human rights

---

[50] *Ibid*. Indeed, Article 19 paragraph 3 allows restriction of the right to freedom of speech in the case of protection of rights of others which can include the property rights of others. Article 19 of the International Covenant on Civil and Political Rights stipulates:

"1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (*ordre public*), or of public health or morals."

[51] Yu, P.K., 2010. "The graduated response", *Florida Law Review*, 62(5) 1373, p. 1423.

[52] 274 F.3d 155 (5th Cir. 2001) paragraph 50.

[53] *United States v. White*, 244 F.3d 1199, 1206 (10th Cir. 2001).

[54] *United States v. Knights*, 534 U.S. 112, 119 (2001).

[55] Strowel, A. 2009, "Internet Piracy as a Wake-Up Call for Copyright Law Makers: Is the 'Graduated Response' a Good Reply?" *The WIPO Journal,* 1(1), 75, p. 83.

champions is that of the monitoring of access to the internet or filtering, or a combination thereof.[56] These technologies will be examined in the later section, 2.3 Legal Online Copyright Enforcement Techniques and Remedies, below.

2.2 Current Trends in the Field of Digital Infringement

This section examines different kinds of current digital infringement, how they work and may constitute illegal activities which infringe copyright. This will help further understand present deterring techniques and measures described in a later section, some of which may be proposed at the end of this thesis. From the view point of copyright protection, online copyright infringement can be generally categorised into three types.[57]

2.2.1 Client-Server Protocol

Client-server architecture is perhaps the most basic of internet activities. Since the early 1980s, the client-server model has traditionally distributed data through networks.[58] A central server stores websites and information.[59] End users, commonly referred to as clients, request the server for information which causes the server to return the requested information back to the client.[60] "The transfer of files from the server to client is called downloading, and the reverse is called uploading".[61] The material does not pass directly to the client; it is broken down into packets, each with the client's address (or IP address) and sent across the internet through other computers including the client's ISP system and finally to the client's computer.[62]

---

[56] "Under most circumstances, the draconian sanction of Internet disconnection is often replaced by monitored access, filtering, site blocking, unannounced manual inspection, or a combination of these options." (Yu, P.K., 2010, *op.cit*., p. 1423.)

[57] Internet Society, 2011, *Perspective on Policy Responses to Online Copyright Infringement: An Evolving Policy Landscape*, [Online] Available at: http://www.internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape p.16-17 [Accessed: 6 May 2014]

[58] Patel, A.R. 2010, "Bittorrent Beware: Legitimizing Bittorrent against Secondary Copyright Liability", *Appalachian Journal of Law,* vol. 10, pp. 118.

[59] A high performance computer is required to act as central server. It needs dedicated software to run the network. Not to mention the cost to pay professionals to fix problems that arise, a client-server system is therefore inevitably more expensive than peer-to-peer networks where there is no dedicated server and thus sidesteps all of these costs. (See below **2.2.3 Peer-to-Peer network** and Davies, W. and Media, D. n.d. "The Difference Between Peer-to-Peer and Client/Server Networks" [Online] Available at: http://science.opposingviews.com/difference-between-peertopeer-client-server-networks-1122.html [Accessed: 18 June 2014])

[60] Patel, *op.cit*., pp. 118-119.

[61] Sfetcu, N. 2014, "Client/Server Architecture" [Online]. Available: http://www.teleactivities.com/clientserver-architecture/ [Accessed: 13 June 2014].

[62] Stokes, S. 2009, *Digital Copyright: Law and Practice,* 3rd ed. Oxford: Hart Publishing, p.12.

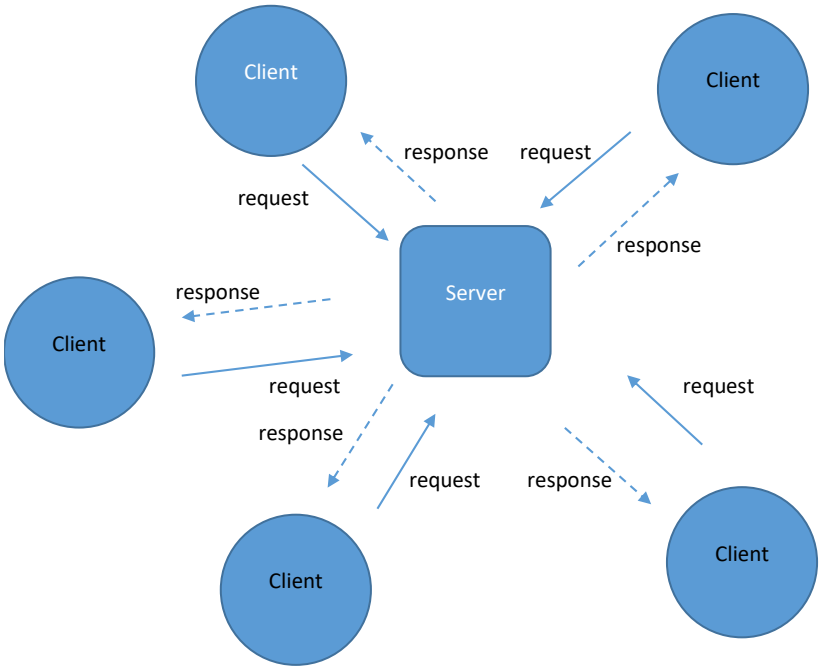

Figure 1: Communication between clients and server

A common instance of the model is a web site which provides media/video/music sharing including streaming. In this category, user-generated content (UGC) websites, e.g., YouTube, Dailymotion, Wikipedia, have recently become popular.[63] The client-server model includes social network sites such as Facebook, Twitter, MySpace, Linkedin, etc. There are many other situations where platforms can be used for copyright infringement:[64]

-local network exchange,

-dedicated file uploading and storage services[65],

-'Warez' sites (web and FTP)[66],

-'One click' hosting services (known as file lockers or cyberlockers)[67],

[63] For the history and effect of UGC, please see for example Halbert, D. 2009, "Mass Culture and the Culture of the Masses: A Manifesto for User -Generated Rights", *Vanderbilt Journal of Entertainment and Technology*, 11, 921; Monagham, J. 2011, "Social Networking Websites' Liability for User Illegality", *Seton Hall Journal of Sports and Entertainment Law*, 21, 499)

[64] Internet Society, *op.cit*.

[65] For example, Dropbox, Onedrive, Google Drive, etc.

[66] Warez pages or Web sites are the sites "that advertise or link to pirated software that is located elsewhere on the internet." (Shayesteh, S.A. 2000, "High-Speed Chase on the Information Superhighway: The Evolution of Criminal Liability for Internet Piracy", *Loyola of Los Angeles Law Review*, 33, 183. p.213.)

-File Transfer Protocol (FTP) sites[68]

Users of the client-server models can reproduce, adapt or communicate to the public, copyrighted works by uploading to/downloading from the sites where the public or a group of people are able to view, copy and forward. Without permission, all of these activities can constitute infringement. To deter this infringement, the 'notice and takedown' system is a remedy legislated and practiced in the US and other countries. More details are provided below in 2.3 Legal Online Copyright Enforcement Techniques and Remedies.

2.2.2 Store-and -forward System

This system transmits a client's request to a server and the server sends to another server or client.[69] The most common example of this system is email.[70] Email, or electronic mail, is the method of exchanging digital messages.[71] E-mail is an extremely popular communication tool.[72] Consisting of computer servers, the email system processes and stores messages on account of which users connect to the email infrastructure via an email client or web interface.[73] "When someone sends an email, the message is transferred from his or her computer to the server associated with the recipient's address, usually via a number of other servers."[74] The recipient can access the mail by logging into her email account stored in the email service provider's server and view the mail. A sender can delete her email on her computer which was sent to the recipient, and should

[67] One type of cyberlockers is the music locker where a group of people share the username and password of the same account and each member can upload and download music to/from the music locker. (Pavlick, P. 2013, "Music Lockers: Getting Lost in a Cloud of Infringement", *Seton Hall Journal of Sports and Entertainment Law*, 23, 247. p.248.

[68] "FTP is the protocol used to list the names of computer files located on a host computer, or *server*, so that a user may easily download files from that server onto his or her local computer." (Shayesteh, *op.cit*., p.189 note 53)

[69] Internet Society*, op.cit*., p.16

[70] Another example is USENET. "USENET is an extensive conglomeration of newsgroups that allows users to discuss topics of interest and to exchange computer files." (Shayesteh, *op.cit*., p.190.) For further detail about USENET, see Dachis, A. 2010, "How to Get Started with Usenet in Three Simple Steps" [Online] Available at: http://lifehacker.com/5601586/how-to-get-started-with-usenet-in-three-simple-steps [Accessed: 25 June 2014]

[71] Runbox.com, n.d. *How Email Works* [Online], Available at: https://runbox.com/email-school/how-email-works/ [Accessed: 17 June 2014]

[72] Brain, M. and Crosby, T., n.d. *How email works* [Online], Available at: http://computer.howstuffworks.com/e-mail-messaging/email.htm [Accessed: 17 June 2014]

[73] Runbox.com, *op.cit.*

[74] *Ibid.*

be able to delete it from her email account server.[75] The recipient can do the same with his computer and with his email server.[76] Each sender and recipient cannot delete the email residing in the other's server.[77]

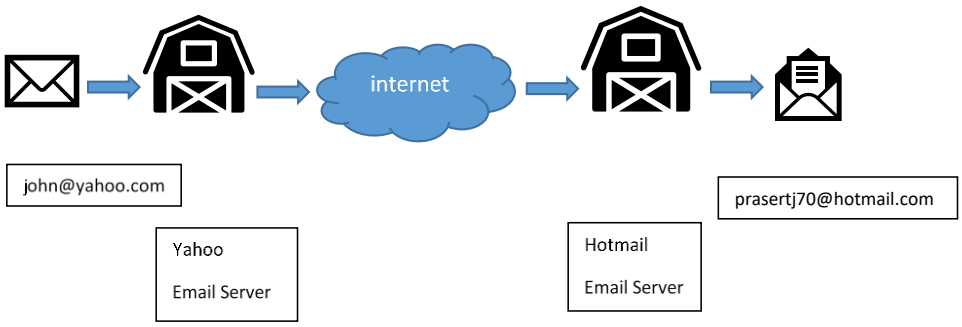

Figure 2: How the email system works

Content in the letter/email and in the attachment can be qualified as copyright work, e.g., literature, music, movies, etc.[78] Forwarding of such an email can constitute copyright infringement.[79] However, the store-and -forward system is not within the remit of this thesis.

2.2.3 Peer-to-Peer Protocol

The 'Peer-to-Peer network' (P2P network) is an alternate form to the client/server model of internet communication.[80] The network has no need of a central computer server which stores information, or software which runs inherently. It could be done through computer programmes other than a web browsing programme. "In peer-to-peer networks, every member, or peer, acts as both a client, by requesting data from other

---

[75] Watts Up With That?, 2011. *The Climategate email network infrastructure* [Online] Available at: http://wattsupwiththat.com/2011/11/30/the-climategate-email-network-infrastructure/ [Accessed: 18 June 2014]

[76] *Ibid.*

[77] *Ibid.*

[78] *Cembrit Blunn Ltd. v. Apex Roofting* [2007] EWHC 111 (Ch) paragraph 241

[79] Apart from the question of originality, creativity, quantity of the work taken and purpose of use, there are other controversial arguments such as whether sending emails to someone else is an implied licence for forwarding and whether forwarding them is fair use/dealing. (*See* Parker, K.R.L. 2014, "Do Not Forward: Why Passing Along an Email May Constitute Copyright Infringement", *Northwestern University Law Journal*, winter, [Online] Available at: http://nulj.org/sites/default/files/files/Parker_Final%20Draft_4_23_2014.pdf p.4 [Access: 18 June 2014], and Out-Law.com, 2007. "Emails can infringe copyright, ruling: Think twice before forward" [Online], Available at: http://www.theregister.co.uk/2007/02/15/email_copyright_infringement/ [Access: 18 June 2014])

[80] Mitchell, B. n.d. "P2P" [Online] Available at: http://compnetworking.about.com/od/p2ppeertopeer/g/bldef_p2p.htm [Accessed: 18 June 2014]

peers, and as a server, by contributing a portion of one's computing resources to the network as a whole."[81] As computers joining the system increase in size, the system's computational resource capacity increases.[82] To join the network, a P2P user needs a programme (or client) such as Skype, MSN, uTorrent, etc., rather than a web browser such as Internet Explorer, Safari, Chrome, etc.[83]

Examples of peer-to-peer protocols are: [84]

- Instant Messaging (IM) or Chatting[85]

- Internet Relay Chat ('IRC')(this type can also be one of the client-server model.)[86]

- File transfer or file sharing programmes[87]

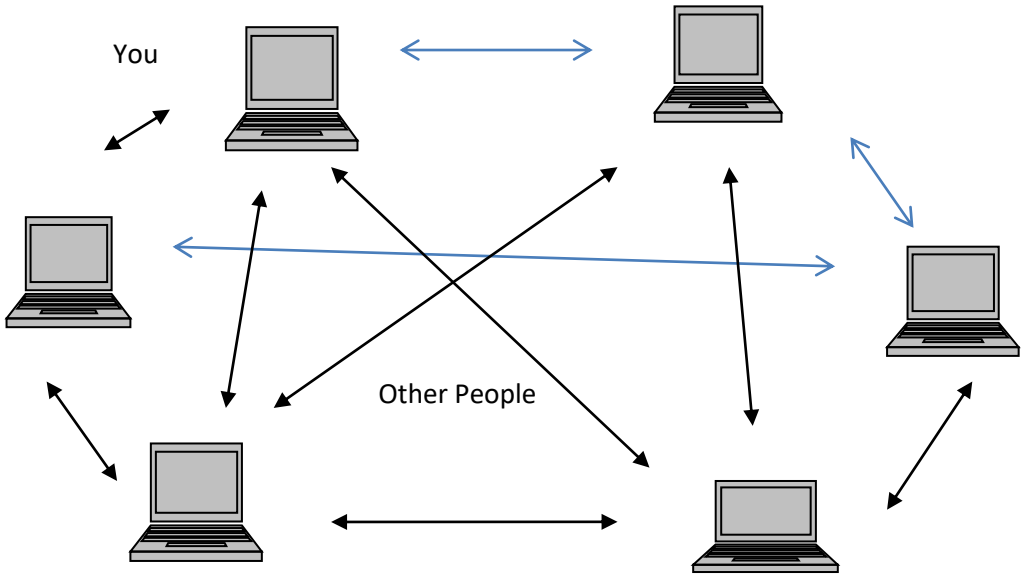

Figure 3: How P2P Protocol Works

[81] Patel, *op.cit*., p. 119.

[82] Instructional and Electronics Support, n.d., "Chapter 6: Distributed and Parallel Computing" [Online]. Available at: http://wla.berkeley.edu/~cs61a/fa11/lectures/communication.html#peer-to-peer-systems. [Accesed: 5 June 2014]

[83] Carmack, C., n.d., "How BitTorrent Works" [Online] Available at: http://computer.howstuffworks.com/bittorrent1.htm [Accessed: 27 June 2014]

[84] Internet Society, *op.cit*.

[85] For example, Skype, MSN, WASTE, Bitmessage, etc. For this type of P2P, information transfers from one computer to another until it reaches the recipient. Each computer works as a conduit.

[86] "IRC is a convenient forum for users to advertise and request pirated software in disguised chat rooms." (Shayesteh, *op.cit*., p.190.)

[87] For this type of P2P, the information is stored in each user's computer and will transfer to another user directly if requested. This could be served in Instant Messaging as an additional function.

P2P network is not the same as 'peer-to-peer file sharing' (P2P file sharing). Within the P2P protocol, P2P file sharing has been one of the most popular applications.[88] There are four different kinds of P2P file sharing. Firstly, the centralised indexing system.[89] Secondly, the completely decentralised indexing system.[90] Thirdly, the semi-centralised indexing system, e.g., BitTorrent, which is commonly referred to as Torrent.[91] Fourthly, the completely decentralised Bit Torrent is the programme called "Tribler". It has no server related to the network at all.[92] In essence, all P2P file sharing systems have common characteristics. They are systems involving file exchange between users without the information server. P2P file sharing can constitute copyright infringement by reproduction, adaptation and communication of works to the public. Download is reproduction by making copies of content available to the requesting user's computer while at the same time dispensing the content to other peers in the swarm which is classed as distribution or communication to the public. The process of breaking a complete content into chunks, sending them and then incorporating them again into a complete content can be classed as adaptation.

With regard to overall P2P file sharing applications such as Bit Torrent, eDonkey and Gnutella, more than half of their traffic is estimated to be non-pornographic copyrighted content shared illegitimately.[93] Moreover, Bit Torrent alone accounts for approximately 17.9% of all global internet traffic and, of this, nearly two-thirds is

---

[88] On average during 2008-2009, P2P occupied 56.32% of internet traffic in comparison with websites at 24.58% and streaming at 6.73%. (Schulze, H. and Mochalskilpoque, K. 2009, "Ipoque Internet Study", [Online] Available at: http://www.ipoque.com/sites/default/files/mediafiles/documents/internet-study-2008-2009.pdf p. 2 [Accessed: 3 June 2014])

[89] Napster architecture is an example of this system. (See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (2001))

[90] Gnutella is an example of this system. Some of the popular Gnutella clients include BearShare, Gnucleus, LimeWire, Morpheus, WinMX and XoloX. (Brain, M., n.d., "How Gnutella Works" [Online] Available at: http://computer.howstuffworks.com/file-sharing3.htm [Accessed: 26 June 2014])

[91] There are many kinds of open source torrent programmes (or clients) such as BitTorrent, Shareaza, uTorrent, Azureus, Bitcomet, XBT, etc. (Gil, P. 2014, "The Best Torrent Downloading Software, 2014"[Online] Available at: http://netforbeginners.about.com/od/downloadingfiles/tp/best-torrent-downloading-software-2012.htm [Accessed: 25 June 2014]). "BitTorrent" seems to be the most popular one. (Envisional 2011, *Technical Report: An Estimate of Infringing Use of the Internet* [Online] Available at: http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf p.2 [Accessed: 23 October 2013]).

[92] Ernesto, 2010, "Truly Decentralized BitTorrent Downloading Has Finally Arrived." [Online] Available at: http://torrentfreak.com/truly-decentralized-bittorrent-downloading-has-finally-arrived-101208/ [Accessed: 25 June 2014]

[93] Dunaytsev, R. et al. 2012, "A Survey of P2P Traffic Management Approaches: Best Practices and Future Directions", *Journal of Internet Engineering*, 5, 1, 318, pp.319-320. Available at: http://www.jie-online.org/index.php/jie/article/viewFile/90/52 [Accessed: 2 May 2014].

estimated to be copyrighted content such as movies, television series, music, and computer software shared illegitimately (63.7% of all Bit torrent traffic or 11.4% of all internet traffic).[94] Such widespread illegitimate use of copyrighted work can be justification in itself for the employment of legal remedies.

2.3 Legal Online Copyright Enforcement Techniques and Remedies

This section explores practice and laws applied at present by ISPs, right holders and relevant sectors, particularly with regard to their effectiveness in protecting copyright online. Any techniques which are found to be effective in deterring online copyright infringement are highlighted.

2.3.1 Notice and Takedown

Practiced in the US and other countries, the 'notice and takedown' (N&T) process deters client/server online infringing activities. Right owners may notify server owners, website owners or web masters. To permit them to locate the material, a notice will be sent with the relevant URL.[95] Web masters will then take down content which has been uploaded or made available to the public, and then inform the users of the matter.[96] Discussion of this legal measure can be found in chapter 4.

2.3.2 Suspension and De-subscription of an Internet Account

Graduated response(GR) is within this category. It focuses on P2P end-user infringement. Suspension of internet use, as part of the court sentencing, may follow educative and informative processes by warning mails in cases where such mails do not deter repeat infringers. It prohibits a user from applying for a subscription from any IAP during a given time. The suspension can be effected through the enactment of the law such as in France and in New Zealand, and through stakeholders' cooperation such as in the US. Whether the system is effective is in doubt.[97] Mere internet disconnection and suspension of internet use are somewhat different. Internet disconnection is commonly

---

[94] Envisional, *op.cit.*, p.2.

[95] Quinn, G. 2009, "Sample DMCA Take Down Letter" [Online] Available at: http://www.ipwatchdog.com/2009/07/06/sample-dmca-take-down-letter/id=4501/ [Accessed: 9 June 2016]

[96] 'ICPs (Internet Content Providers) are in a better position than ISPs (Internet Service Providers) to monitor relationships among online identities and Internet Protocol (IP) addresses'. (Monagham, *op.cit*., p.501.)

[97] Duke, 2012, "The Effectiveness of Anti-Piracy Laws; Lessons to Learn from Hadopi" [Online] Available at: http://legalpiracy.wordpress.com/2012/03/06/effectiveness-hadopi/ [Accessed: 25 June 2014]

used as part of a subscriber agreement around the world.[98] It cuts off a user's access to the internet if the user is in default because of not paying his subscription fee.[99] It limits to one IAP. A subscriber can apply to another IAP for a subscription. The disconnection can be of the alternative methods to the suspension. A discussion of this legal measure can be found in chapter 5.[100]

2.3.3. Traffic Management

Traffic management is essentially employed by ISPs in order to service their customers efficiently. It is a common tool in business practice and widely acceptable in the sense that its purpose is for the sake of all users. Users are obligated to comply with the traffic management clauses in their subscriber contracts. It can be divided into two types: Traffic Shaping and Traffic Capping.

2.3.3.1. Traffic Shaping or Bandwidth Shaping

At the heart of traffic shaping, IAPs have come up with a way to keep the internet running smoothly and efficiently.[101] IAPs have their own traffic management policy in order to prioritise one type of traffic over others under their terms of use.[102] On the internet, information is sent in packets, which are like blocks of data.[103] There are many types of internet data, e.g., emailing, browsing, internet phone calls, P2P file sharing, online gaming, audio/video streaming (YouTube, Spotify, iPlayer) or any other downloading/uploading. Streaming films, playing games and making video calls may be allowed more speed than file sharing in order to prevent them from suffering disruption (or buffering).[104] This is especially true during peak periods because 'most networks have a limited amount of bandwidth. Some internet access providers use traffic management

---

[98] Strowel, A. 2009, "Internet Piracy as a Wake-Up Call for Copyright Law Makers: Is the 'Graduated Response' a Good Reply?" *The WIPO Journal,* 1(1), 75, p. 83-84.

[99] *Ibid.*

[100] *See* 5.6.4 Internet Access Restriction and Traffic Management as a Solution.

[101] Office of Communications (Ofcom), n.d. "A Guide to Internet Traffic Management" [Online] Available at: http://consumers.ofcom.org.uk/files/2013/09/traffic.pdf p.1. [Accessed: 1 July 2014]

[102] Broadband Stakeholder Group, 2013, "Broadband providers launch new traffic management transparency code" [Online] Available at: http://www.broadbanduk.org/2011/03/14/broadband-providers-launch-new-traffic-management-transparency-code/ [Accessed: 2 July 2014]

[103] Wisegeek, n.d., "What is Traffic Shaping?" [Online] Available at: http://www.wisegeek.com/what-is-traffic-shaping.htm [Accessed: 4 July 2014]

[104] Ofcom, *op.cit*.

to slow down peer-to-peer (P2P) networks such as BitTorrent file-sharing.[105] An effective strategy is needed to ensure the network does not become overloaded, causing everything to slow down.[106]

2.3.3.2. Traffic Capping or Bandwidth Capping

Bandwidth capping is a limit of the speed of a subscriber's internet connection and/or of volume of data traffic.[107] Employed by IAPs, '[a] bandwidth cap is usually based on an Internet customer's monthly consumption and is generally measured in gigabytes (GB) of data'.[108] 'Some ISPs that began by supplying unlimited bandwidth to customers later established restrictions'.[109] 'If the user exceeds his monthly bandwidth cap, he may be subject to extra fees or his connection may be throttled for the remainder of the month'.[110]

Although traffic management was not created in response to the need to block or slow down copyright infringement activities, it is, however, technically possible to use it for such a purpose.[111] It may be deployed in assistance to major legal remedies such as GR or N&T.[112] Indeed, traffic management has already practiced in reducing internet speed of certain platforms, e.g., P2P downloads, Skype, or online gaming.[113]

---

[105] *See*, e.g., Virgin Media Cable traffic management policy at: http://help.virginmedia.com/system/selfservice.controller?CONFIGURATION=1001&PARTITION_ID=1&secureFlag=false&TIMEZONE_OFFSET=&CMD=VIEW_ARTICLE&ARTICLE_ID=3103 [Accessed: 25 August 2016].

[106] Wisegeek, *op.cit.*

[107] Murray, A. 2010, *Information Technology Law: The Law and Society*, Oxford University Press: Oxford. p.257

[108] Wisegeek, n.d., "What Is a Bandwidth Cap?" [Online] Available at: http://www.wisegeek.com/what-is-a-bandwidth-cap.htm [Accessed: 4 July 2014]

[109] *Ibid.*

[110] *Ibid.*

[111] Organization for Economic Cooperation Development (OECD), 2009, *Piracy of Digital Content*, Available at: http://www.oecd.org/sti/ind/piracyofdigitalcontent.htm [Accessed: 6 May 2014], p. 104-105.

[112] *See* chapter 6 -- 6.5.2 Recommendations for Thailand in Adopting Principles and Graduated Response Remedy for Peer-to-Peer Online Copyright Protection.

[113] Thomas, N. 2015. "ISP Traffic Management: BT vs Virgin vs Sky vs TalkTalk vs EE" [Online] Available at: https://recombu.com/digital/article/isp-traffic-management-bt-sky-virgin-media-ee-talktalk_M11045.html# [Accessed: 5 May 2016]

2.3.4 Blocking (IP Address, URL, Site, Port and protocol)[114]

Blocking is a measure that can be employed to prohibit access on the part of internet users to websites such as child pornography or gambling. In general, blocking can be effected on both users and websites. User blocking by an IP address can be used by a website to block an undesired user from participating in the website's activity.[115] For website blocking, there are four types of blocking techniques -- i) DNS name blocking, ii) IP address blocking using routers, iii) DPI-based URL blocking, iv) Two-stage systems.[116] In many countries, website blocking is imposed by court order on IAPs to block their subscribers from accessing specific websites.[117] Some countries use this measure when a notice is ignored by an ICP and a public prosecutor may order the ICP to block access to its website(s).[118]

Website blocking is controversial in many respects. It affects freedom of expression when access to the whole website is blocked instead of to a specific webpage (or URL). On many occasions, the European Court of Human Rights has refused to block access to an entire Internet site merely because only part of its content was the subject of infringement.[119] Singapore recently has amended its copyright law which elaborates criteria for blocking of the website that is flagrantly infringing copyright. Moreover, it is argued that "site-blocking does not totally stamp out illegal downloading as most piracy websites have 'proxy' Web addresses, or alternative addresses, that can take users to the

---

[114] Virgin Media, n.d. "Why are some websites not available through Virgin Media?" [Online] Available at: http://help.virginmedia.com/system/selfservice.controller?CMD=VIEW_ARTICLE&ARTICLE_ID=2374&CURRENT_CMD=SEARCH&CONFIGURATION=1001&PARTITION_ID=1&USERTYPE=1&LANGUAGE=en&COUNTY=us&VM_CUSTOMER_TYPE=Cable&buspart=web_block_CR [Accessed: 24 June 2014]) (See also Private Tunnel website, n.d. Available at: https://www.privatetunnel.com/index.php?referral=OPENVPN [Accessed: 24 June 2014])

[115] *Craigslist, Inc. v. 3Taps, Inc.*, 942 F.Supp.2d 962, 969 (N.D. Cal. 2013) (holding that circumvention of IP blocking to obtain information therein was intentionally access to a protected computer without authorization which was illegal under Computer Fraud and Abuse Act (CFAA) (18 U.S.C.A.) § 1030(a)(2), (e)(2))

[116] For details of all the four types of blocking, see *Cartier, Montblanc and Richemont v BskyB, BT, TalkTalk, EE and Virgin* [2014] EWHC 3354 (Ch).

[117] IP Kat, 2015. "Blocking orders across Europe: personality disorder or are the Swedes right?"[Online] Available at: http://ipkitten.blogspot.co.uk/2015/12/blocking-orders-across-europe.html [Accessed: 20 May 2016] (See also Tham, I. 2015. "Music and movie firms back website-blocking" [Online] Available at: http://news.asiaone.com/news/singapore/music-and-movie-firms-back-website-blocking [Accessed: 5 June 2015])

[118] Internet Society, Internet Society, *op.cit*., p.62.

[119] ECHR Press release, 2015. "Blocking without a legal basis users' access to YouTube infringed the right to receive and impart information" p.1-3.

blocked content".[120] Therefore, some right holders choose to go after the end-users who are sharing files on the internet.[121] The website blocking technique is discussed in more detail in chapter 4 -- 4.3.3.1 Website Blocking and Disabling Access to Content.

2.3.5 Content Identification and Filtering

Content identification (Content ID) is the system that YouTube uses to identify infringing content on its users' uploaded materials. The copyrighted works are initially submitted by right owners to be kept in a database of originals. The system compares users' uploaded materials with the database. If matched, copyright owners will be informed and can choose whether to mute audio music, block content from being viewed, monetise by running ads against it or track the video's viewership statistics. [122] Content ID has advantages in application to online copyright protection as follows:

Firstly, this system is one of business approach to copyright infringement which helps compromise legal difference among countries. It sets universal rules for YouTube users which any jurisdiction can endorse.

Secondly, the terms of use can provide other clauses such as repeat infringers can be banned and reported to authorities.[123]

Thirdly, options provided by YouTube offer copyright holders more alternatives than merely notice under N&T. They can bring a win-win situation where right holders, posters and YouTube have benefited from the content commercialisation.[124]

Fourthly, as far as technology is concerned, Content ID can be developed to build up an infringing database and to use the database to compare with subsequent posting. This can prevent the same infringing content from a repost.[125]

---

[120] Tham, *op.cit.*

[121] *Ibid.*

[122] Google, n.d., "How Content ID works" [Online] Available at : https://support.google.com/youtube/answer/2797370?hl=en [Accessed: 14 December 2014])

[123] YouTube, n.d., "Keep your YouTube Account in Good Standing" [Online] Available at: https://support.google.com/youtube/answer/2797387?hl=en&ref_topic=2778545 [Accessed: 8 July 2014[Accessed: 8 July 2014]

[124] The system is essentially in favour of right holders in that they can choose whether an action is employed in one country but the other action is exercised in another country, e.g., 'a video may be monetized in one country, and blocked or tracked in another'. (Google, *op.cit*.)

[125] As will be seen in Chapter 4, today's N&T problem is that it causes undue burden to the right owners in submitting notice for the same infringing materials. The developed content ID can help reduce the demand of notice.

Fifthly, in P2P technology, Content ID can be used by ISPs to filter content, applications(or computer programmes) and certain relevant copyrighted content by its titles.[126]

However, filtering is one of the most controversial measures. It leads to trespassing of the principle of net neutrality.[127] Moreover, in a region such as Europe, the CJEU (Court of Justice of the European Union) ruled that a court order requiring ISP installation of filtering systems was invalid.[128]

2.3.6 Other techniques and measures

In addition to all the above methods, there are other ways to cope with digital copyright protection as follows:

- Video fingerprinting, already in place in some music and video content, could be used to identify unauthorised copies.[129]

- Manipulating the Domain Name Designation

- Cutting off revenue to illegal sites[130]

- Digital Rights Management (DRM) and Technological Protection Measures(TPM)[131]

---

[126] Ernesto, 2013. "Music biz Demands Piracy Filter from Torrent Sites or else." [Online] Available at: http://torrentfreak.com/music-biz-demands-piracy-filter-from-torrent-sites-or-else-130701/ [Accessed: 25 June 2014]

[127] The term "net neutrality" can refer "to the network protocols and internet architecture that can direct, on the technical level, how ISPs discriminate among content, services, or applications." (Reicher, A. 2011, "Redefining Net Neutrality After *Comcast v. FCC*", *Berkeley Technology Law Journal*, 26 (1), 733, p.734.)

[128] Directives 2001/29 and 2004/48, read in conjunction with Directives 95/46, 2000/31 and 2002/58 and interpreted with regard to Articles 8 and 10 of the European Convention on Human Rights, preclude an injunction made against an IAP which requires it to install a system for filtering all electronic communications passing via its services, which applies indiscriminately to all of those users, as a preventative measure, exclusively at its expense and for an unlimited period. (*Scarlet Extended v. SABAM*, Case C‑70/10)

Moreover, CJEU also ruled in another case that Directives 2000/31, 2001/29 and 2004/48 preclude an injunction made against an IHP which requires it to install a system for filtering information stored on an IHP's servers by its service users, which applies indiscriminately to all of those users, as a preventative measure, exclusively at its expense and for an unlimited period. (*SABAM v. Netlog*, Case C‑360/10)

[129] OECD, *op.cit.*

[130] Pakinkis, T., 2014. "Weatherley: 'Cutting off ad revenue to illegal sites is key to piracy battle" [Online] Available at: http://www.musicweek.com/news/read/weatherley-cutting-off-ad-revenue-to-illegal-sites-is-key-to-piracy-battle/058830 [Accessed: 10 July 2014]

[131] Xu, C., 2014. "Redefinition of Current Legal Measures' Role as *Panaceas* in Digital Rights management Play", US-China Law Review, 11(2), 135. p.136.

-Attacking P2P architecture, e.g., Poisoning the Network or a denial of a service programme[132]

- Copyright Taxes/Levies[133]

2.4 Infringement Detection and Identification

Overall, this part is to study if the present system is able to find enough evidence to convict an alleged infringer. If the answer to this question is practical and positive, then we may not need a legal measure in replacement for traditional investigation. As will be seen below, the traditional investigation relies on IP addresses of infringing users which does not necessarily lead to the identification of an actual infringing user.

2.4.1 Internet Protocol Addresses (IP address) and Internet Account Identification

Internet communication is based on a simple process of assigning an address to any device connected to the internet.[134] The address permits the device to join into and communicate with any other connected devices using this same addressing scheme.[135] 'This addressing scheme is commonly referred to as the IP address'.[136] IP addresses signify the address of both sender and receiver of information on a network.[137] Simply speaking, it could be described as a home address or a telephone number to which a letter or a ring (or data) can be sent. Anytime a user connects to the internet, the user's computer is assigned a long number IP address.[138] Therefore, an IP address is the main source of user identification. It can be used to retrieve a user's physical address including an individual, specific computer or device that Is used at a given time.[139] For the purpose of fast response

---

[132] Chirgwin, R., 2012. "Russian upstart claims BitTorrent-killer: 'Pirate Pay' names Microsoft as investor" [Online]. Available at: http://www.theregister.co.uk/2012/05/13/pirate_pay_dos_against_torrents/ [Accessed: 30 June 2016].

[133] Peukert, A., 2009. A Bipolar Copyright System for the Digital Network Environment *in*: Strowel, A.2009, *Peer-to-Peer File Sharing and Secondary Liability in Copyright Law*, Cheltenham: Edward Elgar. p.154.

[134] Shipley, T.G. & Bowker, A. 2014, "Chapter 3 - How the Internet Works" in *Investigating Internet Crimes*, eds. T.G. Shipley & A. Bowker, Boston: Syngress, pp.42-43.

[135] *Ibid.*

[136] *Ibid.*

[137] Mundhra, A. n.d., GT Explains: What is an IP Address and Difference Between a Static and Dynamic IP Address?[Online] Available at: http://www.guidingtech.com/8987/gt-explains-what-is-an-ip-address-and-difference-between-a-static-and-dynamic-ip-address/#top [Accessed: 22 July 2014]

[138] Anon., n.d. "How to Block Your IP Address." wikiHow [online]. Available at: http://www.wikihow.com/Block-Your-IP-Address [Accessed 30 August 2013].

[139] Private Tunnel, [Online] Available at: https://www.privatetunnel.com/index.php?referral=OPENVPN [Accessed: 4 August 2014]

to online copyright infringement, IP addresses are generally used in the process of internet account holder identification as shown below.

2.4.2 Process of Identification of Infringement and Precise Wrongdoers

Whether it is the client/server or P2P environment, identification of wrongdoers must first involve identification of an internet account holder. An internet account holder can be traced by an IP address. In doing so, it needs several steps which are as follows:[140]

First: Establish an IP address.

An IP address can be obtained from various sources depending on platforms.[141] For client/server, "[w]hen a user views a Web site, a computer server logs his IP address."[142] An ISP requires a court subpoena to reveal its subscriber.[143] In YouTube, a requesting right holder needs a court subpoena to acquire an IP address (or a YouTube subscriber identity) of video posters or commenters. For P2P, the file sharing system directly exposes the IP address of peers to each other in a swarm which allows peers to know IP addresses of other peers who are transferring certain contents.[144] Moreover, an IP address can be obtained indirectly from the coordinating trackers.[145]

Second: Identification of the owner of the IP address.

This step is actually to find which ISP owns the IP address in order to find the ISP subscriber. It is usually revealed by a domain registration lookup or a Whois lookup.[146]

---

[140] Shipley, T.G. and Bowker, A., 2013. Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace. Amsterdam, London: Elsevier. p. 46.

[141] The email sender IP address may be at the received header fields of the email. The process is slightly different between different email service provider interfaces. (WhatIsMyIPAddress.com website, n.d., "How do I find email headers?" [Online] Available at: http://whatismyipaddress.com/find-headers [Accessed: 10 September 2014])

[142] McIntyre, J. J., 2011. "Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected as Personally Identifiable Information", *DePaul Law Review*, 60, 3, Available at SSRN: http://ssrn.com/abstract=1621102 p.3 [Internal citation omitted]

[143] *Ibid.,* p.5 [Internal citation omitted]

[144] Li, J., 2007, "A Survey of Peer-to-Peer Network Security Issues" [Online] Available at: http://www.cse.wustl.edu/~jain/cse571-07/ftp/p2p/#ddos [Accessed: 11 Sep. 2014]

[145] Piatek, M., Kohno, T. and Krishnamurthy, A., 2008. "Challenges and Directions for Monitoring P2P File Sharing Networks or Why My Printer Received a DMCA Takedown Notice", [Online] p.2 Available at: http://dmca.cs.washington.edu/dmca_hotsec08.pdf [Accessed: 10 Sep. 2014]

[146] Shipley, *op.cit.*

These first two steps in the IP address tracking process are normally done by a third party company.[147]

Third: Contact ISPs.

Subscriber's identity is the information in an ISP's system. This step usually requires a subpoena.[148]The ISP needs to be provided with the IP address, the date and time of use, including the time zone and Coordinated Universal Time (UTC).[149]

Fourth: Find the information of the account holder

The revealed account holder can be a house owner, an office or a public place where multiple persons can access the internet.[150]

Although an IP address could lead to retrieval of a user's identity, there are many causes that make the detection of infringement and the identification of an internet user uncertain, e.g., Network Address Translation (NAT), spoofed IP addresses[151], hijacked IP

---

[147] Ernesto, 2014. "This is how the UK piracy warnings will work."[Online] Available at: http://torrentfreak.com/how-uk-piracy-warnings-work-140517/ [Accessed: 18 Aug. 2014]

[148] Yurkiw, J. 2013. "Subpoenas seeking identifying information and login data associated with email addresses did not violate First Amendment or privacy rights"[online], Available at: http://www.technologylawsource.com/2013/08/articles/information-technology/subpoenas-seeking-identifying-information-and-login-data-associated-with-email-addresses-did-not-violate-first-amendment-or-privacy-rights/ [Accessed: 19 May 2016] quoting *Chevron Corp v. Donziger*, No. 12-mc-80237 (N.D. Cal. Aug. 22, 2013))

[149] Shipley, *op.cit.*

[150] Walden, I., 2007. *Computer Crimes and Digital Investigations*, Oxford: Oxford University Press. p.209.

[151] This is commonly known as proxy server which is the most common method used to hide real IP address. Basically, a proxy is an indirect network connection that allows you to use internet with your real IP hidden and with data protection. There are three types of proxy servers:

1) Virtual Private network (VPN), e.g., Hide My Ass (http://www.hidemyass.com/vpn/), VyprVPN (http://www.goldenfrog.com/vyprvpn/special/referral?offer_id=42&aff_id=1022&source=Hide_IP&processed=1#), PureVPN (http://www.purevpn.com/order/), Private Tunnel. (https://www.privatetunnel.com/index.php?referral=OPENVPN) Users can set their browsers to use VPN to protect their identities.

2) Website-Based Proxy Servers, e.g., Hide My Ass (http://www.hidemyass.com/vpn/)-- Users can log into the website servers and then logging into another website in order to conceal their IP addresses in the second website.

3) Browser-Configured Proxy Servers. There are several of these types of proxies that will hide IP address, which are Anonymous Proxy, Distorting Proxy, High-Anonymity Proxy. Firefox is an example of proxy setting browsers which has setting proxy as default.

(*See* WhatIsMyIPAddress.com website, n.d., "Hide IP" [Online] Available at: http://whatismyipaddress.com/hide-ip [Access: 10 May 2014])

To trace back to the real user, one needs to ask for the information from the service. This service, however, has some flaw of speed reduction because information has to pass the programme or the transit website.

addresses.[152] All of these contribute to the possibility of wrong infringement identification. The relevant question here is how great is the percentage of users using these camouflage techniques? Regarding this issue, a survey shows that globally "28% of the online population using tools to disguise their identity or location".[153] Therefore, an IP address can be considered reliable because it represents more precise than fault user information.

In a household, a subscriber may not be the infringer himself and may not be able to identify the infringer. There are many reasons why he may not be able to determine the real infringer, e.g., many people within a household, allowed/disallowed strangers, account hacking.[154] This creates obvious identification problems and gives a potential defence for suspected infringers.[155] Proof that a specific person was using a device at the relevant time raises substantial challenges for the investigation process.[156] Such information is probably impossible to acquire without a search warrant, intruding into the owner's privacy or requiring help from intimately involved domestic people.[157]

It is clear that an IP address is only a first step in the user identification process. Moreover, after the IP address is acquired, the following tracing process is complicated and impractical. At some stage court proceedings must be involved. It can be concluded that a traditional investigation to certify an actual infringing user is neither efficient nor effective. Indeed, all the above method is an approach towards court litigation. Resources are required for civil litigation and indemnity is not guaranteed while the criminal process seems disproportionate. Therefore, there needs to be a simpler measure that bypasses all these difficulties.

---

[152] Hackers can use user's IP address in illegal activities potentially exposing the user to law enforcement investigation. (Private Tunnel, [Online] Available at: https://www.privatetunnel.com/index.php?referral=OPENVPN [Accessed: 4 August 2014])

[153] Kiss, J., 2014. "Privacy tools used by 28% of the online world, research finds" [Online] Available at: http://www.theguardian.com/technology/2014/jan/21/privacy-tools-censorship-online-anonymity-tools [Accessed: 11 Sep. 2014].

[154] Clayton, R., 2012. "Online traceability: who did that?" *Consumer Focus*, Available at: http://www.consumerfocus.org.uk/files/2012/07/Online-traceability.pdf p.30 [Accessed: 10 Sep. 2014]

[155] Walden, *op.cit.*

[156] *Ibid.*

[157] A household is different from a large business office or university environment where a worker or student may need to log into a computer system by using his account which reveals his identity. In *Parke v. RIAA*, a court subpoena to a university to disclose its student identity was successful. (Rimmer, M., 2007, *Digital Copyright and the Consumer Revolution: Hands Off My IPod*, Cheltenham: Edward Elgar. p.214)

The N&T process circumvents the above investigation process. From a technical perspective, it does not need an IP address because a website operator only requires the URL prescribed in a notice in order to take down content.[158] The N&T system will be further discussed in Chapter 4. Moreover, in France the GR concept includes subscriber duty of monitoring internet use which obviates the need for infringer identification. In France's copyright law, online copyright infringement is classed as a minor offence which legitimises reverse burden of proof on part of internet subscribers and which seems to resemble the approach the internet society has suggested.[159] The GR system will be examined in Chapter 5.

In order to be able to examine and develop adequate legal remedies for online digital copyright protection with regard to Thailand, it is vital to determine the degree to which Thailand's substantive law applies or is able to respond online copyright infringement. Discussion of these issues are followed in the next chapter.

[158] An IP address can also be used in N&T process against P2P file sharing where an ISP forwards the notice to its subscriber. (Piatek, *op.cit.*)

[159] It has proposed that the infringement notice establishes a rebuttal presumption that infringement has occurred. (Internet Society, *op.cit*., p.21.)

Chapter 3: Thailand Substantive Copyright Protection Legislation Applicable to Client/Server and Peer-to-Peer User Infringement

3.1. Introduction

To construct legal framework for digital copyright protection, it is necessary to examine Thailand substantive law in order to ensure that client/server and P2P users activities are illegal under Thailand online copyright protection regime. The illegality of these activities is the end that justifies the means, i.e. a legal remedy, in that the remedy cannot assert scope of enforcement beyond rights conferred by substantive law. If rights of reproduction, adaptation and communication to the public subsisted in copyright are not disturbed by posting or sharing of content on the internet, the remedy is then not necessary in such circumstances. This chapter will discuss the relevant sections of Thailand copyright legislation and consider whether they sufficiently protect copyright from online infringement activities.[1] An analyse as to whether client/server and Peer-to-Peer (P2P) end user infringing activities come under a classification of civil and/or criminal liability under Thailand's copyright law and under other substantive legislations will also be undertaken.

Under Thailand's legal frameworks for copyright statutory protection, there are three distinct pieces of legislation in existence relevant to digital infringement, namely: (1) Copyright Act B.E. 2537 (1994) (CA 1994); (2) Penal Code B.E.2499 (1956) (hereinafter PC 1956); and (3) Computer-Related Offence Act B.E. 2550 (2007) (hereinafter CROA 2007). This chapter will discuss these legislations by dividing content into two main parts -- civil and criminal liabilities. The civil liability part examines whether certain end-user activities are illegal under Thailand's CA 1994. The criminal liability part examines whether the same activities are also classed as criminal offences under CA 1994. In so doing, it highlights the requirement of a criminal intention as outlined in section 59 of PC 1956. The second part also considers if copyright infringing acts can be included in computer-related offences under CROA 2007.

[1] One commentator argued that some part of CA 1994 is unpredictable. (*See* Pitiyasak, S. 2003, "Does Thai law provide adequate protection for copyright infringement on the Internet?", *European Intellectual Property Review,* 25 (1) pp. 6-19.

The scope and methodology adopted in the chapter is discussed as followings.

Firstly, section 3.2 studies core Thai substantive copyright law -- CA 1994. It clarifies if client/server and P2P activities have civil liability and whether such activities can give rise to primary infringement (CA 1994 sections 27 to 30) or secondary infringement (CA 1994 section 31). Throughout this section the study analyses the exclusive right definitions in CA 1994 section 4 regarding reproduction, adaptation and communication to the public in conjunction with section 31, concerning elements of secondary infringement. It explores Supreme Court decisions in interpretation of these provisions and analyses when they apply to client/server and P2P circumstances.

Regarding primary infringement, section 3.2.1 discusses whether the exclusive rights of copyright owners can be affected by digital online infringement, what right(s) are affected and how they are affected. In so doing, this subsection explores the extent of exclusive right protection of a work in a digital form as guaranteed by the Berne Convention for the Protection of Literary and Artistic Works 1886 (1971 revision with 1979 amendments) (Berne Convention), by the Agreement on Trade-Related Aspects of Intellectual Property Rights 1994 (TRIPs), and by the World Intellectual Property Organization Copyright Treaty 1996 (WCT). This exploration will enable an evaluation of the extent of CA 1994 protection. Rights of reproduction, adaptation and communication to the public are discussed in subsections 3.2.1.1, 3.2.1.2 and 3.2.1.3 respectively. In particular, these subsections analyse whether client/server posting and P2P file sharing practices infringe exclusive rights under CA 1994.

Regarding secondary infringement, section 3.2.2 discusses four elements of prohibited practices that make infringing copies of copyrighted materials widespread. There is a clarification if end-users meet any or all of the elements. The four elements under discussion are: 1) if unauthorized upload, download, and distribution by client/server and P2P users is of the prohibited activities, 2) if a copy made from activities is infringing, 3) if client/server and P2P users know or should have known of the existence the infringing copy, and 4) if such users gain profit from their activities. This section investigates if either client/server and/or P2P users commit secondary infringement, if there is any difference between the two users in terms of their practice, and if any difference in practice results in different legal liability.

Secondly, section 3.3 discusses if CA 1994 provides grounds for criminal copyright infringement. It examines if the same infringing activities can be classed as both civil and criminal violations and what of CA 1994 civil elements need to be inferred and if any element that needs to be added in criminalisation. The section analyses if intention on the part of the perpetrator is a prerequisite for criminality as it is in general criminal counts, or if infringement by negligence is sufficient to constitute criminal liability. In so doing, this section incorporates CA 1994 criteria for primary and secondary civil liability, as provided in the previous section for external elements, and investigates PC 1956 section 59 for internal elements.

Thirdly, section 3.4 explores CROA 2007 offences that are relevant to end user activities. It clarifies the criminal elements of the importation of false or forged 'computer data' into computer systems and the dissemination or forwarding of the same data under CROA section 14 (1) and (5) respectively. Initially, it studies if copyrighted content can be classed as 'computer data' as the term is defined in CROA 2007. Having studied the definition, the section further examines if illegally-reproduced copyrighted content is forged or is otherwise false computer data. In so doing, the thesis scrutinises Supreme Court decisions in cases where the reproduction of copyrighted books was alleged to have been a document fabrication and discusses if cases can be held as precedents for the issues in question. Additionally, this section compares and contrasts upload, download and share in client/server and P2P activities with distribution, importation and forward of computer data of CROA 2007 offences. Finally, this section answers the question if client/server and P2P end-users commit importation of false or forged computer data into computer system and dissemination or forward of the data.

To begin with, section 3.2 examines subsisting rights, namely rights of reproduction, adaptation and communication to the public in CA 1994 and discusses whether or not these rights protect a work in digital format, whether or not client/server and P2P end user activities infringe these rights and whether or not such users are liable on secondary infringement grounds.

3.2 Can Client/Server and Peer-to-Peer User Activities be classed as Civil Offences under Copyright Act B.E.2537 (1994)?

CA 1994 as well as other Thailand intellectual property laws generally categorise infringement into two types, primary and secondary. Primary infringement (sections 27 to

30) is an act of reproduction, adaptation and communication to the public of copyrighted work. Secondary infringement (section 31) is a further action based on infringing copies, e.g., the selling, the occupying for sale or the offering for sale of the copies. CA 1994 sections 27 to 31 prescribe civil and criminal infringements of which their criminal penalties are from sections 69 to 75. According to CA 1994 the grounds for both civil and criminal liability are by and large identical.[2] However, criminal liability must have an element of intention whereas in civil cases even unintentional acts can entail liability, but reduced compensation may be awarded in such cases.[3] The following subsections discuss end-user infringement of copyright, and whether or not such end-users are liable for civil action in client/server and P2P technology.

3.2.1 Can Client/Server and Peer-to-Peer User Activities be Primary Infringement and What Are the Exclusive Rights Affected?

CA 1994 section 15 generally provides exclusive rights, namely reproduction, adaptation, communication to the public and licensing rights.[4] Primary infringement occurs when an offender exercises the rights of the copyright owners without permission

[2] Thailand's legal system allows copyright holders to seek for both civil and criminal action when their rights are infringed. There is legal prescription provided in both cases. In civil cases, CA 1994 section 63 allows the prescription for 3 years from the day the right holders learn of the infringement and know of the infringers, but no later than 10 years from the date of infringement. In criminal cases, CA 1994 section 66 prescribes that the offense under this act is a compoundable offence. It means that right holders who want to criminalise an infringer via public prosecution channels need to lodge a complaint with the authorities within 3 months after they learn of the incident and know of the infringer under PC 1956 section 96), or no later than 1 year for the fine-only penalty (CA 1994 section 69 and 70 paragraph 1) and no later than 10 years if the infringement is punishable by not more than a 7-year term of imprisonment (CA 1997 section 69 and 70 paragraph 2). These prescriptions are stated in PC 1956 section 95(5) and (3).

[3] Civil and Commercial Code section 438:

"The Court shall determine the manner and the extent of the compensation according to the circumstances and the gravity of the wrongful act.

Compensation may include restitution of the property of which the injured person has been wrongfully deprived, or its equivalent value, as well as damages for any injury caused."

[4] Section 15: "Subject to Sections 9, 10 and 14, the owner of copyright shall have the exclusive rights of:

(1) reproduction or adaptation;

(2) communication to the public;

(3) rental of the original or the copies of a computer program, an audiovisual work, a cinematographic work and sound recordings;

(4) assigning benefits accruing from copyright to other persons;

(5) licensing the rights mentioned in items (1), (2) or (3), with or without conditions, provided that such conditions shall not unfairly restrict competition.

Whether or not the conditions mentioned in item (5) in the first paragraph constitute unfair restrictions on competition shall be determined in accordance with the rules, methods and conditions set forth in the Ministerial Regulations."

or license.[5] Section 27 provides general acts of infringement.[6] Additionally, sections 28 to 30 stipulate specific acts against different categories of copyrighted works. Audio-visual works, cinematographic works and sound recordings are referred to in section 28, broadcasting work in section 29 and computer programs in section 30. For example, section 28 bars acts of renting out the originals of copyrighted works or their copies[7] and section 29 prohibits acts of rebroadcasting.[8] With regard to the internet, uploading and downloading and sharing content may transgress exclusive rights of reproduction, adaptation and communication to the public.[9]

3.2.1.1 Reproduction Right

This section discusses whether current CA 1994 protects a reproduction right when an original work is reproduced from a physical to a digital format, also *vice versa* and between digital formats. In particular, the question is whether the practices of client/server posting and P2P file sharing can be an infringement of the reproduction right under Thai law. These questions can be addressed by raising how international treaties deal with such questions and whether Thai law meets the international standard.

The Berne Convention for the Protection of Literary and Artistic Works 1886 (1971 revision with 1979 amendments) (Berne Convention) Article 9 (1) [10]guarantees the

---

[5] Section 15(5)

[6] Section 27: "Any of the following acts against a copyright work under this Act performed without permission in accordance with Section 15(5) shall be deemed an infringement of copyright:

(1) reproduction or adaptation;

(2) communication to the public"

[7] Section 28: "Any of the following acts against an audiovisual work, a cinematographic work or a sound recording copyrighted under this Act performed without permission in accordance with Section 15(5), whether against the sound or image, shall be deemed an infringement of copyright:

(1) reproduction or adaptation;

(2) communication to the public;

(3) rental of the originals or copies of a work."

[8] Section 29: "Any of the following acts against a sound and video broadcasting copyrighted under this Act performed without permission in accordance with Section 15(5) shall be deemed an infringement of copyright:

(1) making an audiovisual work, a cinematographic work, a sound recording or a sound and video broadcasting work whether in whole or in part;

(2) rebroadcasting whether in whole or in part;

(3) making a sound and video broadcasting work to be heard or seen in public in return for the payment of money or other commercial benefit."

[9] Pitiyasak, *op.cit.*, p.11.

[10] Berne Convention Article 9 (1) provides: 'The authors of literary and artistic works protected by this Convention shall have the exclusive right of authorising the reproduction of these works, in any manner or form.'

reproduction right by merely stating that the authors of the works shall have the exclusive right to authorise the reproduction. TRIPs Article 9 (1)[11]and WIPO Copyright Treaty (WCT)Article 1(4)[12]do not provide otherwise but merely refer to the Berne Convention provision. The detailed scope of reproduction depends on how member states implement the law.[13] For Thailand, the scope of 'reproduction' is provided by definition under CA1994, section 4 paragraph 13, which states:

"Reproduction includes *any method of copying*, imitation, duplication, block-making, sound recording, video recording or sound and video recording from an original, a copy, or a publication, for a *substantial part*[14], whether in whole or in part, and, in the case of computer programs, means duplication or making copies of the program from any medium for a substantial part by any method, not creating a new work whether in whole or in part." [Emphasis added]

Under Berne Convention Article 9(1), authors of literary and artistic works enjoy the exclusive right of authorising reproduction of their works 'in any manner or form.' 'In any manner or form' includes reproducing and storing in electronic means or form, whether temporarily or permanently.[15] Moreover, the texts of TRIPs and of the WIPO Copyright Treaty, which were designed to modernise protection of works in digital format, both made use of the Berne provision.[16] Although WCT has no provision clarifying that storing copyright works in digital medium is reproduction, the Diplomatic Conference took the following stance in an Agreed Statement:

---

[11] TRIPs Article 9 (1) provides: 'Members shall comply with Articles 1 through 21 of the Berne Convention (1970) and the Appendix thereto...'

[12] WIPO Copyright Treaty (WCT) Article 1(4) provides: 'Contracting Parties shall comply with Articles 1 to 21 and the Appendix of the Berne Convention.'

[13] Berne Convention Article 2 (4) provides: 'It shall be a matter for the countries of the Union to determine the protection to be granted to official texts of a legislative, administrative and legal nature, and to official translations of such texts.'

[14] It should be noted here that WIPO's translation does not include 'substantial part,' as existed in the Thai original, in its English translation.

[15] Article 9(2) permits the exception of temporary reproduction which is a normal operation of a computer system and does not usually conflict with the three step test--certain special cases, normal exploitation and unreasonably prejudice the legitimate copyright interests of the author. (International Bureau, WIPO, n.d. *The WIPO Copyright Treaty (WCT) and the Wipo Performances and Phonograms Treaty (WPPT)*[online]. Available at : http://www.wipo.int/export/sites/www/copyright/en/activities/pdf/wct_wppt.pdf p. 5. Accessed: 19 Dec. 2013.)

[16] *See* TRIPs Article 9 (1), WIPO Copyright Treaty (WCT) Article 1(4) and Berne Convention Article 2 (4) in notes 11, 12 and 13 above.

"The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention."[17]

The question of the defined 'reproduction' under Thai law is whether it is compliant with the Berne Convention, TRIPs and WCT; in other words, whether it gives protection against reproduction of a work into digital form. It is argued that the Thai reproduction right meets the requirements of Berne Convention Article 9(1). It protects digital reproduction even though the 'reproduction' definition does not employ the term 'in any manner or form' similar to Berne Convention Article 9(1). Rather, the protection is via the term 'any method of copying' from an original. The word 'method' may suggest that the definition merely covers the 'manner' through which reproduction is made while the word 'form' from the Berne provision is still missing. The definition does in fact cover a 'form' of copyrighted content of which reproduction is made in a digital form. The CA 1994 'reproduction' definition does not state the matter clearly but the Thailand Supreme Court has confirmed this standpoint on many occasions.

In Supreme Court case no.5036/B.E.2550 (2007), plaintiff, C.C. Co. Ltd., produced a literary work concerning a water filter machine. The work comprised the design, structure, assembly and installation of a water filter system, a water filter machine and an adjusting chemical substance. It also contained information about the plaintiff's company as well as product facts with figures carrying information about quality and efficiency along with machine pictures. The plaintiff had shown this work on the company website as well as in English catalogues and brochures, which described the company's history and gave a detailed product demonstration along with pictures. Defendants, Mr S. and two others, drew the information from the plaintiff's website, catalogues and brochures. They gathered, edited and printed the plaintiff's work in books distributed to their customers in the course of their business. The plaintiff sued the defendants in a criminal case for illegal reproduction and adaptation of a literary work. In preliminary examination, the Court held that the plaintiff's work was a copyrighted literary work and the defendants' act

[17] International Bureau, *op.cit*.

constituted reproduction and adaptation.[18] The Court ruled that the case had *prima facie* grounds for primary and secondary infringement of a literary work under Section 27 and 31 of CA 1994.

The above case is the transformation of a work from an electronic format to a physical format. It can be applied *vice versa* in cases where a tangible book is converted to a digital one.

In Supreme Court case no.6804/B.E.2548 (2003), Mr.S., a copyright owner, was the author of an academic article about *PuerariacandolleiGrah. var. mirifica (Airy Shaw et Suvatabandhu) Niyomdham* (Scientific name, or 'Pueraria mirifica' in short or 'Kwaokrua' in short in Thai), a kind of herbs in Thailand. The article showed research results and the use of different kinds of Kwaokrua in biotechnology as a herb. S.N. Co.Ltd., defendant no. 1 and the other 3 defendants used his article in commercialising their Kwaokrua products on their website. The defendants were convicted of copyright infringement by reproduction and adaptation of the plaintiff's article under CA 1994 section 27(1) and 69.

The copyrighted work in this case was a literary work which was initially authored in print. This case confirms that the copyrighted work can be reproduced illegally into a digital form. It is applicable to work distributed via the internet. Another case which ruled on the reproduction of a copyrighted work now follows, but this time concerning reproduction from a digital format to a digital format.

In Supreme Court case no.1829/B.E. 2553 (2010), the defendant used legitimate VCDs containing the copyright owner's music videos to reproduce the music videos into a computer. The Court held that the defendant was guilty of reproduction and adaptation violation under CA 1994 section 27(1) and 69 paragraph 2.

This case is not the only precedent where reproduction of copyrighted work in digital format was deemed to be an infringement.[19] All the Supreme Court 'reproduction' cases above did not address directly why digital reproduction fell within the reproduction

[18] A preliminary examination is the criminal 'proceedings conducted by a court with a view to finding a *prima facie* case against the accused' and it is required and conducted in cases of private prosecutions because the case is filed to the court directly without going through an inquiry stage managed by an inquiry official. (Criminal Procedure Code section 2(12) and 162)

[19] *See* also, e.g., the Supreme Court cases no.3882/2553 (ruling that the digital reproduction of a musical work onto a computer and onto a CD was an infringement of a reproduction right), and no. 6802/2553 (finding that the digital reproduction of a computer programme was an infringement of a reproduction right.)

definition and which an instance(s), e.g., 'imitation', 'duplication' or 'any method of copying', provided in the definition the digital reproduction was. The Court merely held that the defendant's acts of making a digital copy from a physical one, or *vice versa*, constituted 'reproduction' right infringement. The reason for this may be because such acts clearly reproduced a copyrighted work, which will also be true whatever platform is used. In a client/server platform, an upload results in a copy on the targeted site and a download produces one on an individual's computer. Similarly, file exchanges conducted in a P2P platform will result in more copies on their computers and will facilitate others in doing the same thing. The act of downloading a copyright work from other users constitutes an act of reproduction (or reproduction right).[20] These are infringements of a reproduction right under the definition of 'reproduction'.

In conclusion, the Thailand CA 1994 'reproduction' right includes digital reproduction from physical to digital, *vice versa*, or from digital to digital. This is so even though the CA 1994 'reproduction' definition does not state as such. In fact, digital protection emerges from Thailand Supreme Court precedents. A client/server and P2P user's upload, download and share of copyrighted work invites infringement of reproduction right under the CA 1994 section 4 paragraph 13 definition.[21] The next section discusses if Thailand protects adaptation of copyrighted work in digital format.

3.2.1.2 Adaptation Right

An adaptation right is the right that always comes along with a reproduction right.[22] Adaptation is actually another method of reproduction because CA 1994 section 4 paragraph 14 stipulates that adaptation is 'reproduction' that does 'not create a new work'. The question here is whether 'adaptation' under Thai law meets the international standard, whether it includes conversion of the original work between physical and digital formats and between digital formats. In particular, the question is whether practice of

---

[20] Depreeuw, S. and Hubin, J., 2014. *Study on the Making Available Right and its Relationship with the Reproduction Right in Cross-Border Digital Transmissions*, [Online] Available at: http://ec.europa.eu/internal_market/copyright/docs/studies/141219-study_en.pdf p.28 [Accessed: 3 December 2015]

[21] The question where infringement by reproduction of copyrighted works takes place or, in other words, which ISPs' system the infringement take place see chapter 4 -- 4.3.1 Service Providers Affected by the Court Order under Copyright Act (No.2) B.E.2558 (2015) and chapter 5 -- 5.2.1 Service Providers Affected by the Court Order in its Application to P2P under CA 2015 § 32/3.

[22] Indana, N., 2003. 'Copyright Protection in the Information Technology Age,' [Thai.] Available: http://people.su.se/~nain4031/copyrightIT.htm [Accessed: 13 Dec.2013.]

client/server posting and P2P file sharing is in fact a form of adaptation. CA 1994 provides an 'adaptation' definition in section 4 paragraph 14 which states:

"Adaptation" means a reproduction, not creating a new work, by conversion, modification or emulation of a substantial part of an original work whether in whole or in part, which

(1) with regard to literary works, includes a translation, a transformation or a collection by means of selection and arrangement,

(2) with regard to computer programs, includes a reproduction by means of transformation, modification of the program for a substantial part, not creating a new work,

(3) with regard to dramatic works, includes the transformation of a non-dramatic work to a dramatic work or a dramatic work to a non-dramatic work, whether in the original language or in a different language,

(4) with regard to artistic works, includes the transformation of a two-dimensional work or a three-dimensional work into a three-dimensional work or a two-dimensional work or the making of a model from an original work,

(5) with regard to musical works, includes an arrangement of tunes or an alteration of lyrics or rhythm."

An adaptation right under CA 1994 accords with the international standard. The WIPO Copyright Treaty, under its Article 1 (4), concurs with the Berne provision for an adaptation right.[23] Under Berne Convention Article 12(1), 'authors of literary and artistic works shall enjoy the exclusive right of authorising adaptations and other alterations of their works. Here, there is no 'in any manner or form' as appeared in Berne Convention Article 9(1) reproduction right.[24] However, it is irrelevant in the light of present technological change of format of work and method of reproduction, e.g., electronic means or form, and temporary or permanent reproduction, because the phrase 'other alterations' (as stated in Article 12(1)) of works, embraces change of work in any manner

[23]WIPO Copyright Treaty, art. 1(4) provides: 'Contracting Parties shall comply with Articles 1 to 21 and the Appendix of the Berne Convention.'

[24] Berne Convention Article 9(1): authors of literary and artistic works enjoy the exclusive right of authorising reproduction of the works 'in any manner or form.'

and form. The CA 1994 'adaptation' is the 'reproduction by conversion, modification or emulation of an original work' which covers all kinds of possible changes that are 'not creating a new work.' An adaptation right prohibits others from changing the work no matter how the work has been changed, e.g., translating a literary work from one language to others,[25] from a physical object to a digital version,[26] from a digital format in a website to a physical book,[27] or from a literary work to a cinematographic work.[28] As to adaptation between digital formats, the 1829/B.E. 2553 (2010) case found that reproduction of a digital work to another digital work was an infringement of an adaptation right. This case is applicable to client/server and P2P technologies where content is exchanged online digitally.

In client-server architecture, "[T]he transfer of files from the server to client is called downloading, and the reverse is called uploading".[29] Every time an end-user clicks on a website or its available contents, the user's browser requests the remote website's server computer to send a copy of content.[30] The material does not pass directly to the user; it is broken down into packets, each with the client's address (or IP address) and sent across the internet through other computers and finally to the user's computer.[31] This process constitutes 'reproduction by conversion, modification or emulation' of copyrighted work which may be classed as adaptation of a copyrighted work.

In the P2P file exchange process, the P2P programme takes apart a file into portions and different users exchange their portions directly to and from one another.[32] At a given time, a P2P user simultaneously collects and distributes pieces of a file from several peers who already have the file or who are in the process of obtaining it.[33] When all the pieces have been acquired, they are reassembled on his hard drive, at which time

---

[25] Indana, *op.cit*.

[26] See Supreme Court case no. 6804/B.E.2548 (2003) above.

[27] See Supreme Court case no. 5036/B.E.2550 (2007) above.

[28] Supreme Court case no.2572/B.E.2548 (2005).

[29] Sfetcu, N. 2014, "Client/Server Architecture" [Online]. Available: http://www.teleactivities.com/clientserver-architecture/ [Accessed: 13 June 2014].

[30] Stokes, S. 2009, *Digital Copyright: Law and Practice,* 3rd edn, Oxford: Hart Publishing, p.12.

[31] I*bid*.

[32] Brown, M., 2009. "White Paper: How BitTorrent Works" [Online] Available at: http://www.maximumpc.com/article/features/white_paper_how_bittorrent_works [Accessed: 26 June 2014]

[33] "Each peer distributing a file breaks it into chunks ranging from 64KB to 4MB in size and creates a checksum for each chunk using a hashing algorithm. When another peer receives these chunks, it matches its checksum to the checksum recorded in the torrent file to verify its integrity". (*Ibid*.)

the complete file (seed) is broken down again to allow other users to retrieve it.[34] The process of P2P file exchange is actually 'reproduction by conversion, modification or emulation' of copyrighted work which, without permission, is an adaptation right infringement.

It can be concluded that Thailand CA 1994 meets the international standard of adaptation right. The CA 1994 'adaptation' definition protects the right to the adaptation of work in digital format. Client/server and P2P technology constitutes adaptation within its process of communication.[35] The Supreme Court interprets the adaptation right to cover conversion of the original work between digital formats. This precedent can also apply to the conversion of a work in client/server posting and P2P file sharing.

3.2.1.3 The Right of Communication to the Public

This section discusses whether a right to communication to the public encompasses communication via the internet, whether it requires 'actual access', and whether client/server and P2P activities are communication to the public. These questions can be resolved by studying how the Berne Convention and WCT address these very issues.

Berne Convention Article 11(1) (ii) stipulates that an author of dramatic, dramatico-musical and musical works shall enjoy the exclusive right of authorising any communication to the public of the 'performance' of their works. Article 11bis (1) (ii) provides that authors of literary and artistic works shall enjoy the exclusive right of authorising any communication to the public 'by wire'. Finally, Article 11ter (1) (ii) provides that authors of literary works shall enjoy the exclusive right of authorizing 'any communication to the public of 'the recitation' of their works.[36] These Berne provisions confer limited modes of communication, i.e., 'performance', 'by wire' and 'recitation'. The term 'by wire' casts doubt on whether communication by wireless means is also applicable.

---

[34] Brown, *op.cit.*

[35] The question where infringement by adaptation of copyrighted works takes place or, in other words, which ISPs' system the infringement takes place see chapter 4 -- 4.3.1 Service Providers Affected by the Court Order under Copyright Act (No.2) B.E.2558 (2015) and chapter 5 -- 5.2.1 Service Providers Affected by the Court Order in its Application to P2P under CA 2015 § 32/3.

[36] Under Article 9 of TRIPs, TRIPs members have an obligation to comply with these provisions.

WCT Article 8 grants a copyright holder the exclusive right of communication to the public 'by wire or wireless means.' The term 'by wire or wireless' covers most, if not all, modes of communication.[37] Communication such as by cable, WIFI, radio frequency or satellite, sometimes comes with a wire or wireless option. The WCT Article 8 fills the gap in the Berne Convention definition where the same phase does not exist. It is clear that the internet is intended as one of its modes of communication.

There is nowhere in Berne Convention Articles 11(1) (ii), 11bis (1) (ii) and 11ter (1) (ii) that seems to deal with the issue of actual access. WCT Article 8 gives clarification to this issue by including a way of communication to the public that members of the public may access 'from a place and at a time individually chosen by them'. On the internet, if a work has already been uploaded and is ready for use on a site, does the work have to be actually viewed or listened to in order for the uploading to be classed as infringement? The clause 'making available to the public of works in a way that the members of the public may access the work from a place and at a time individually chosen by them' gives greater clarification with regard to its application to on-demand and interactive communication services.[38] By having a content prepared for anyone to access in an interactive service or on a website, a work is now made available to the public in a manner that the service customers or website viewers may request it from anywhere and at any time they please. Infringement occurs even if the content has not yet been accessed or is never likely to be. The right to communication to the public under the WCT is clearly more comprehensive than the right to communication to the public as shown in the Berne Convention. This may cause a problem to a country such as Thailand which is a member country of the Berne Convention but yet to be a member of the WCT.

The Thailand CA 1994 'communication to the public' definition articulates generally that making available a work to the public by any means is communication to the public. CA 1994 section 4 paragraph 15 defines 'communication to the public' as follows:

---

[37] WCT committees are committed to the objective of an exclusive right of authorization of the author or other copyright owner over the transmission of works on the Internet and in similar networks. (International Bureau, *op.cit*., p.7.)

[38] WIPO, n.d., Summary of the WIPO Copyright Treaty (WCT) (1996) [online]. Available: http://www.wipo.int/treaties/en/ip/wct/summary_wct.html [Accessed: 18 Dec. 2013.]

"Communication to the public means making a work available to the public by means of performing, lecturing, preaching, playing music, causing the perception by sound or/and image, constructing, distributing or by any other means."

The definition provides different means of communication by which a copyrighted content is made available. It does not explicitly provide communication by the internet nor does it have the all-in-one term 'by wire or wireless'. One commentator opined that the missing term leaves room for controversy as to whether it includes communication via the internet.[39]

A medium of connectivity does not necessarily indicate its relation to the internet. Even if the phrase 'wire or wireless,' is missing, the literal meaning of 'by any other means' suggests that, as long as work has been made available to the public, infringement can occur irrespective of the medium of communication. Therefore, any medium, including the internet, which makes a work accessible to the public can be accounted for by 'wire or wireless' transmission. The Supreme Court has not yet addressed directly the issue of wire or wireless mode. It decided that communication to the public could be done by making content available onto a website. In case no.6804/B.E.2548 (2003) the defendants were found convicted of communication to the public right infringement under CA 1994 section 27(2) and 69 when they displayed co-plaintiff's 'Kwaokrua' herb article on their website.[40] As will be discussed below, the Supreme Court has never stated a means that defendants can employ to communicate to the public, e.g., 'performing, lecturing, preaching, playing music, causing the perception by sound or image, constructing, distributing or by any other means'.[41] It has merely held that defendants have been guilty of communication to the public right infringement in general. Therefore, in so far as a conclusion can be made, the communication to the public definition is interpreted to encompass display of a work on the internet, in this case a client/server (website) system, whether or not it is through wire or wireless. The issue of means and medium of communication is related to another problem on the internet landscape -- that of actual access.

The CA 1994 "Communication to the public" definition does not state clearly whether infringement is conditional on actual access by members of the public. This issue

---

[39] Pitiyasak, *op.cit*., p.11.
[40] *See* Supreme Court case no.6804/B.E.2548 (2003) above.
[41] CA 1994 section 4 paragraph 15 'communication to the public' definition

is complicated in the Thailand paradigm. In order to resolve it there is a requirement to ascertain whether or not the means employed by the infringer is a live performance. Primary communication to the public infringement concerns a means for exposing a work in an intangible form. The words that come in series such as "performing, lecturing, preaching, playing, causing the perception (of image and sound), and constructing", suggest that there has to be an instantaneous display in front of an audience. It is clear that a live performance, without authorization, of a copyrighted work via a website or P2P streaming is infringement of the right of communication to the public by one of these means. However, communication to the public by 'distribution' and 'causing perception by image or sound' may be different. These two instances can be both live and not-live performances. Distribution suggests the involvement of a material in which copyrighted content is contained. Therefore, before moving to the question of actual use, it is suggested that an understanding of these two terms within this context is paramount.

Distribution of copyrighted works is not directly prescribed as being part of the exclusive rights of copyright owners.[42] There is no 'distribution' definition provided in CA 1994. The term 'distributing' in the communication to the public definition context could connote the act of display to the audience while distributing a work, e.g., the showing and selling of paintings, drawings, photographs, model cars or the real architecture of houses. It could also suggest the act of the non-display handing out of physical copies such as the selling of a musical CD. Associate Professor Thatchai Suphapholsiri, a Thai copyright expert, wrote that only the former connotation is valid:

"Thailand Copyright Act 1994 does not confer the exclusive right of distribution. […] Ones who sell the legitimate copies of the work without direct display of the content do not infringe communication to the public right of which the Copyright Act 1994 confers. This analysis is in accordance with the property ownership principle. The owner of an object containing intangible copyrighted work can sell or distribute the object. The

[42] CA 1994 Section 15 provides: "The owner of copyright shall have the exclusive rights of:
(1) reproduction or adaptation;
(2) communication to the public;
(3) rental of the original or the copies of a computer program, an audiovisual work, a cinematographic work and sound recordings;
(4) assigning benefits accruing from copyright to other persons; and
(5) licensing the rights mentioned in items (1), (2) or (3)."

copyright holder has no control over such selling or distributing because doing so will interfere with the ownership."[43]

To some extent, ownership seems to conflict with the communication to the public right as far as the term 'making a work available to the public by means of distribution' is concerned. In order to examine if the law confers a distribution right on a right holder, the genuineness of a distributed object needs to be determined. Has the object been made legally by a copyright owner or a licensed person? The above view has potential implications especially when a distributed object is a genuine copy. CA 1994 section 15 is not clear in cases where distributed copies are genuine because the exclusive right provision does not clearly confer a distribution right.[44] In contrast, CA 1994 section 31 is clear when distributed copies are counterfeit because secondary infringement disallows selling and distribution of counterfeit copies.[45] Therefore, CA 1994 implicitly confers a distribution right on copyright owners only in cases of illegal copies. The Supreme Court cases below show how the Court dismissed communication to the public (of the primary infringement) count on the point that the content came from a secondary source, not from the original source.

In Supreme Court case no.1829/B.E.2553 (2010), the defendant reproduced music videos of a copyright owner from a VCD to a computer and sold, offered for sale, or occupied for sale such music videos. The defendant was held guilty of infringement of reproduction and adaptation rights and not of communication to the public. The reason given was that he was not communicating music videos directly from the original VCD. The Court did not reason that the acts of "selling, offers for sale, or occupies for sale" *per se* were not communication to public right infringement. The Court did reason that

---

[43] Suphapholsiri, T. 1990, *Principles of Copyright Law,* Bangkok: Nititham Publishing House. pp.169-170. [Thai].

[44] *See* CA 1994 Section 15 in note 40.

[45] CA 1994 section 31: "Whoever knows or should have known that a work is made by infringing the copyright of another person and commits any of the following acts against the work for profit shall be deemed to infringe the copyright:

(1) selling, holding for sale, offering for sale, letting, offering for lease, selling by hire purchase, offering for hire purchase;

…

(3) distribution in a manner which may cause damage to the owner of copyright;"

communication to the public infringement was not applicable because the content came from a secondary source computer rather than from an original source VCD.[46]

In Supreme Court case no.3882/B.E.2553 (2010), the plaintiff asserted that the defendant infringed musical works by reproducing musical works onto a computer CPU, converting them into MP3 files, and sharing and playing the files among the defendant's customers; hence, requesting the court to punish the defendant under Section 28 and 69. The Court held that the defendant's act was not communication to the public of *original works* under Section 28 because the musical works were infringing copies under Section 31.[47]

Once again, the Thailand Court did not opine that distribution by sharing or, more pertinently, by playing (the musical files) itself was not communication to public but its decision was based on a matter of originals and imitated replicas.[48] Had the indictment alleged that the defendants committed secondary communication to the public infringement, the defendants would have been convicted. Be that as it may, the current legal status is that distribution of an infringing copy is illegal under CA 1994 section 31 (2) and (3).[49] Whether distribution of a legitimate copy (being displayed or performed or not) is communication to the public or not is questionable.

The 1829/B.E.2553 (2010) and 3882/B.E.2553 (2010) cases can apply to client/server and P2P users in that once a copy is produced onto an internet user computer in P2P or onto a website in client/server, the copy is already an infringing copy and it is this copy that is used or made available to the public. Distribution of such a copy can be communication to the public within a secondary infringement context. A client/server and P2P user can commit communication to the public infringement by distribution of a counterfeit copy.[50] The question still is whether the counterfeit copy needs actual access to it to constitute infringement of communication to the public right.

---

[46] See also Supreme Court case no.290/B.E.2548 (2005).

[47] See also Supreme Court case no.7873/B.E.2549 (2006)

[48] Under the Criminal Procedure Code section 158(6), the indictment has to state the substantive provision(s) and penalty provision(s) requested. The plaintiff in this case was possibly not raising Section 31 as the substantive and Section 70 as the penalty.

[49] CA 1994 section 31 (2) is 'communication to the public' and (3) is 'distribution in a manner which may cause damage to the owner of copyright'.

[50] The same act can also be 'distribution in a manner which may cause damage to the owner of copyright' under CA 1994 section 31 (3).

The Supreme Court decided in a case where a literary work was reproduced and distributed without permission.

In Supreme Court case no.994/B.E.2543 (2000), defendant no. 1 reproduced the plaintiff's work by printing books entitled 'Hot Attraction and Naked Angels' by means of a mould made by defendant no.9. The record showed that the books had indicated defendant no.1 as a printer and no.9 as a mould maker, which meant that defendants 1 and 9 conspired in the infringement by performing different missions. Defendants 1 and 9 were therefore principals of the reproduction of the works (under section 27(1)). Defendant no. 15 had been hired by company "S." to do a distributing mission. Defendant 15 was found guilty of communicating the infringing work to the public under Section 31(2) and 70 paragraph two.

In this case defendant 15 who distributed a copyrighted literary work in infringing books was found guilty. There was no proof of actual access and the Supreme Court did not reckon that such access was required to satisfy infringement of the right of communication to the public by distribution. To the extent of a physical form, a counterfeit copy does not need actual access. However, it could be argued that actual access can be required in client/server and P2P technologies. Indeed, the Supreme Court has already decided in client/server technology. In the 'Kwaokrua' case, defendants were held to be criminally responsible for making available the plaintiff's 'Kwaokrua' article on their website.[51] The defendants were convicted of infringement of communication to the public right under CA 1994 section 27 (2), 69. The Supreme Court stated that a website was a venue where the public 'may' access the plaintiff's copyrighted work.[52] The word 'may' describes the possibility that content can be accessed but it is not necessarily accessed. Therefore, it can be concluded that actual access is not a required element of communication to the public by 'distribution' in client/server and P2P technologies.

'Distribution' may not be the only example of the actual access consideration in client/server and P2P technologies. A more pertinent scenario is probably that of

[51] Case no.6804/B.E.2548 (2003)

[52] The court did not clarify about which types of communication the website had engaged in and whether or not infringement of the right of communication to the public had been completed without actual access because these were not the disputes at bar.

communication to the public by 'causing perception by image or sound'.[53] As suggested by the term 'image or sound', this seems to represent musical and cinematographic works which are the type of works mostly involved in client/server and P2P infringement. Still, the question is whether 'communication to the public' is complete merely by causing perception, as opposed to actual perception.

In Supreme Court case no.3054/B.E.2548 (2003), the issue at bar was whether or not defendants, by turning on a musical work at the front of the computer shop, infringed a co-plaintiff's right of communication to the public. There was no proof of the fact that there was the actual presence of a passer-by witness who heard from the speakers and looked on a computer screen displaying the copyrighted music video. The Supreme Court was affirmative that there must have been passers-by who heard and looked at the work because the musical work was playing at the front of the shop. This circumstance indicated a defendant's intention to infringe the right of communication to the public. Although the Court did not clarify under what category of communication the defendants' acts could be defined, this case is a stronger case for 'causing the perception of image and sound' than 'distribution' because the computer shop sold and repaired computers; it did not sell or distribute a musical work.

The term is quite clear that merely causing the perception is enough to satisfy the communication criteria. Whether there is an actual view or not is irrelevant. Presentation of the work in front of the shop clearly causes the perception of image and sound. There is no need to prove actual access of such image and sound. This case could be a precedent for copyrighted work being learnt instantly while it is being played. It can be said that in Thailand the act of simultaneous file exchange as suppliers and consumers of resources constitutes making available on the P2P file sharing network (right of communication to the public).[54]

To some extent, a website scenario is analogous to that of the physical book shop. A work put onto the website is similar to a book put onto a book shelf in a book shop in

[53] CA 1994 Section 4 paragraph 15

[54] Similarly, in EU, each user of the peer-to-peer network is potentially liable for infringements to the making available right. (Depreeuw, S. and Hubin, J., 2014. *Study on the Making Available Right and its Relationship with the Reproduction Right in Cross-Border Digital Transmissions*, [Online] Available at: http://ec.europa.eu/internal_market/copyright/docs/studies/141219-study_en.pdf p.29 [Accessed: 17 August 2016])

that the copyrighted content put onto the website is not learned instantly at the time of availability. In these circumstances, 'distribution' can be the same as 'causing perception by sound and image'. Regarding the book shop circumstance in the case of 'Hot Attraction and Naked Angels', a 'distribution' of books can be seen as an act akin to 'causing perception of image and sound'; hence, no actual access required.[55]

Regarding the website circumstance in Supreme Court case no.6804/B.E.2548 (2003), it can be assumed that the making available of the 'Kwaokrua' article on a website is communication to the public either by 'distribution' or 'causing perception of image and sound'. Either way, the public 'may' access the article. The word 'may' is used here in conjunction with the common meaning of the phrase 'causing perception'. Together, they mean that mere display of a work for public access can cause perception of the work; whether the public actually accesses it or not, and when and where the access takes place are not decisive factors. For this reason, modes of display (a book or a website) and formats of the work (physical or digital) are irrelevant. Therefore, it can be concluded that communication to the public by 'causing perception of image and sound' does not need to be a real time performance nor does it need actual access.

There is another comparison implication between case nos.994/B.E.2543 (2000) and 6804/B.E.2548 (2003) concerning the primary and secondary nature of communication to the public infringement. In 994/B.E.2543 (2000), copyrighted books were reproduced illegally; the result was infringing copies. The Court held that defendant no. 15 was guilty of secondary infringement (under section 31 (2) and 70 paragraph two). However, in 6804/B.E.2548 (2003), the plaintiff's article was reproduced illegally on the defendants' website. The defendants were found culpable of primary infringement (under section 27 (1) (2) and 69). These two cases seem to conflict with each other and the Supreme Court seems inconsistent with regard to infringing materials as to whether it is primary or secondary infringement. There is some difference between the 994/B.E.2543 (2000) case and the 6804/B.E.2548 (2003) case concerning issues at bar.

The Supreme Court in the 994/B.E.2543 (2000) case contemplated whether defendants conspired or intended to conspire through certain specific commissions -- reproduction and/or distribution, and whether an individual defendant's action should be

[55] Supreme Court case no.994/B.E.2543 (2000)

held culpable under specific sections of CA 1994. This was because the court of the first instance, the Central Intellectual Property and International Trade Court (CIPIT), erred in concluding a sentence that defendants no.1, 9, and 15 were guilty of jointly committing infringement under sections 27 (primary infringement) and 31 (secondary infringement). It did not identify specifically which activity was classed as reproduction and which activity was classed as communication to the public; and whether individual defendants committed primary or secondary infringement. Therefore, the Supreme Court corrected CIPIT by holding that defendants 1 and 9 were guilty of reproduction under section 27 and defendant 15 of communication to the public under section 31. In contrast, the 6804/B.E.2548 (2003) case did not directly address the nature of primary and secondary infringement. The Court deliberated whether the plaintiff was the copyright-owning author who actually composed the article, and if the defendants adapted the plaintiff's work, and if defendant no.3, as an authorised representative of the legal entity (defendant no. 1), shared responsibility with that entity. The primary/secondary issue was beyond the Supreme Court's dispute and that is why the Court did not touch upon the issue. Therefore, the first case is more likely to serve as the precedent because it directly addresses that issue. Finally, the third case following here is perhaps decisive.

In Supreme Court case no.3054/B.E.2548 (2003), a musical work was illegally reproduced from VCDs to a computer. The Court ruled that by playing the work from the computer the defendant was guilty of secondary infringement under sections 31 and 70. This third case confirms the basic concept that making infringing materials widespread is secondary infringement. CA 1994 section 31 should apply because it clearly states that an action made upon infringing copies is one of secondary infringement. Therefore, 994/B.E.2543 (2000) and 3054/B.E.2548 (2003) are more consistent with the law and are more likely to be used as precedents for this issue. It can be concluded that communication to the public must be associated with a means of communication. If unlawful communication to the public takes place by a real time and live performance means such as 'performing, lecturing, preaching' which exposes the work in intangible form, the act is one of primary infringement. If such communication is by any other means, not in intangible form and a copyrighted material is involved, e.g., 'distributing, causing perception by image and sound', the act is of secondary infringement.

It can be concluded that Thailand CA 1994 protects the right of communication to the public in digital format and in the internet environment. The right to communication

to the public does not require actual access to content; the CA 1994 definition itself does not clearly advocate such a conclusion, however, the train of Supreme Court case decisions does. An act of making works available on the internet, on a website or on a P2P torrent folder, where the public may have access to them is communication to the public.[56] Such an act is not necessarily a live performance; therefore, it is communication to the public by 'distribution' and/or 'causing perception of image and sound'. However, both client/server and P2P technology is not included in communication to the public primary infringement because the digital copy that is made available is an infringing copy. Communication to the public in this circumstance can be considered as secondary infringement provided that other factors are satisfied. Client/server users and P2P users are in different positions because a P2P user may not meet all factors of secondary infringement of the right of communication to the public. These factors are discussed below.

3.2.2 Are Posting and Sharing, Types of Secondary Infringement?

Thai CA 1994 secondary infringement relates to primary infringement in that it aims to prevent illegal works from becoming widespread.[57] This section examines whether or not client/server and P2P users can be liable for secondary infringement. Secondary infringement excludes acts of illegal reproduction and adaptation which derive illegal copies of a copyrighted work. Secondary infringement entails activities associated with the derived copies. These activities are limited to those prescribed under CA 1994 section 31 subsections (1) to (4). Section 31 states:

"Whoever knows or should have known that a work is made by infringing the copyright of another person and commits any of the following acts against the work for profit shall be deemed to infringe the copyright:

(1) selling, holding for sale, offering for sale, letting, offering for lease, selling by hire purchase or offering for hire purchase;

(2) communication to the public;

---

[56] The question where infringement by communication to the public of copyrighted works takes place or, in other words, which ISPs' system the infringement take place see chapter 4 -- 4.3.1 Service Providers Affected by the Court Order under Copyright Act (No.2) B.E.2558 (2015) and chapter 5 -- 5.2.1 Service Providers Affected by the Court Order in its Application to P2P under CA 2015 § 32/3.

[57] Suphapholsiri, *op.cit*., pp.210-211.

(3) distribution in a manner which may cause damage to the owner of copyright;

(4) self-importation or importation on order into the Kingdom."

The language of section 31 suggests that there has to be someone who primarily reproduces and/or adapts a copyrighted work which results in infringing copies. Without such copies, subsequent associated infringing activities cannot take place.[58] It is important to have an infringing article as an exhibit that shows a prerequisite primary infringement. The question here is whether posting and sharing can be classed as secondary infringement.

In principle, there are four elements of secondary infringement under CA 1994 section 31:[59]

(1) there has to be any act of subsection (1)-(4) of section 31;[60]

(2) any act in (1) has to be upon infringing works;

(3) the one who takes action knows or has reason to know that the work is made by infringement;[61]

(4) the act committed is for profit.

The first element is that the action of a wrongdoer has to come within one of the activities in subsection (1) - (4). 'Communication to the public' in subsection (2) is likely to be the relevant activity regarding client/server and P2P practices. It is the same phrase having the same definition as in section 27(2).[62] In both client/server and P2P technology, communication to the public of copyrighted work is basically not a live performance, e.g., 'performing, lecturing, preaching, playing music'.[63] A digital copy is involved because it is made available on a website or on a user's computer. Upload, download and share actions are communication to the public by means of 'distributing' and 'causing perception by

[58] Suwanprateep, D., 2010, "The Offence of Contributory Infringement of Intellectual Property Rights." *The Central IP and IT Court Journal 12th: Special Issue 2010*, 226. p. 226.[Thai]

[59] Supreme Court case no.3741/B.E.2549(2006)

[60] It should be noted that 'exportation' is not included in secondary nor is it included in primary infringement.

[61] The UK Copyright, Designs and Patents Act 1988, Sections 23-26 have a similar standard "…which he knows or has reason to believe…" or "…believe on reasonable ground…"(Suphapholsiri, *op.cit*., p. 211.)

[62] CA 1994 section 4 paragraph 15 provides the 'communication to the public' definition

[63] CA 1994 section 4 paragraph 15 'communication to the public' definition

image and sound'.[64] As mentioned earlier in Supreme Court case no. 6804/B.E.2548 (2003), a 'Kwaokrua' article made available on the website was found to be an infringement of the right to communication to the public. The actions can also be classed as an act of 'distribution in a manner which may cause damage to the owner of copyright' under section 31 (3). Making the work available for free in client/server and P2P may cause damage to the owner of copyright. The first element is satisfied.

The second element focuses on infringing copies. Content available in client/server and P2P can be similarly infringing copies. Upload is illegal reproduction and adaptation of content to a website. Download is illegal reproduction and adaptation of content to a computer. Content illegally uploaded and downloaded is therefore infringing content.[65] According to case no.1829/B.E.2553 (2010), posting and sharing of such content can account for secondary infringement of communication to the public by making it available to the public through distribution and/or cause of perception of sound and images under section 31 (2) and (3). This is the fact-based element which means that if the copies are legal and ones who act upon them do not know that they are legal then they cannot be secondarily liable even if they were under the impression that the copies were illegal.

The third element is that by engaging in the first and second elements, the user 'knows' or 'should have known' that the copy is an infringing one.[66] The Supreme Court has never before decided this factual knowledge in client/server or P2P user paradigms. This knowledge is affirmative in a street vendor case. Street vendors sell musical MP3, CDs and VCDs, these exhibits being clearly identifiable as infringing copies by a product package or a price difference. They can hardly deny that they lack the knowledge that the exhibits are counterfeit.[67] The factual knowledge can similarly be assumed in a client/server and a P2P case. Reproduction, adaptation or making available of the work underlies the fact that a user knows or should have known that the work is an infringing copy. In client/server, a digital copy is made from a user's computer and transferred onto

[64] CA 1994 section 4 paragraph 15 'communication to the public' definition

[65] In Supreme Court case no.1829/B.E.2553 (2010), music videos reproduced and adapted from a VCD to a computer were found to be infringing copies.

[66] Only the word 'know' was originally prescribed in section 27 of Copyright Act 1978 which was the version prior to the Copyright Act 1994 which repealed and replaced it. Section 31 of CA 1994 added the constructive knowledge 'should have known' to overcome the difficulty of proof of factual knowledge. (Tingsmith, W., Ending Remark of Supreme Court case no. 4250/B.E.2542 (1999))

[67] Supreme Court case nos. 4250/B.E.2542, 6558/B.E.2541, 3040/B.E.2541, 10/B.E.2542 and 5337/B.E.2542

a destination website.[68] A user still has his original copy on hand and it is the copy at the destination that the user intends to distribute. Such user cannot realistically deny that he does not know that the copy at the destination is an infringing copy. In P2P, the same knowledge can be assumed because a P2P user gains a copy from a swarm. The copy is then shared as an illegally reproduced copy. Such a user cannot legitimately deny that he does not know that the copy in his computer is an infringing copy. Certainly, if client/server and P2P users do not know, they at least 'should have known'.

The fourth 'profit' element is that the 'profit' has to be directly attributable to the infringement in question. This element includes a special intention where, in order to render a defendant culpable, it needs to be proved that he intends to have a direct benefit from such an act; mere proof of an infringing act is not enough.[69] In Supreme Court case no. 8220/2553 (2010), a defendant played music from an illegal VCD in her food shop without permission. She did so without charging for the music separately from or together with the food. The court found that she did not violate CA 1994 § 31 because she did not gain benefit directly from communication to the public of the infringing VCD. In online infringement, it must be proved that a user posts or shares content for profit and that the profit is made directly from such posting and sharing. This element applies to client/server users more straightforwardly than it does to P2P users.

In client/server, a user can monetise from content posted on a website in many ways, e.g., by obtaining revenue from an advertisement placed alongside the playing content or requesting for a subscription fee.[70] This benefit can accrue proportionately from an ever-increasing number of viewers. By the reaping of benefit from this monetisation, a client/server user's 'profit' element can be satisfied.

In P2P, an end-user is persuaded to share content by differing forms of incentive, e.g., the tit-for-tat mechanism, the reciprocity algorithm, the unchoke mechanism.[71] None of them involves a monetary return. It is certain that distribution of work via P2P by end-

---

[68] Indeed, the proved user can be held accountable for infringement of primary reproduction and adaptation rights.

[69] Supreme Court case no.3054/B.E.2548 (2003)

[70] Green, J., n.d., "How do people earn money from YouTube?" Available at: https://www.quora.com/How-do-people-earn-money-from-YouTube-1 [Accessed: 5 February 2016]

[71] Anagnostakis, K. et.al, 2006. "On the Impact of Practical P2P Incentive Mechanisms on User Behavior", *NET Institute Working Paper No. 06-14* [Online] Available at: http://netecon.seas.harvard.edu/NetEcon07/Papers/zghaibeh_07.pdf p. 2 [Accessed: 6 March 2016]

users is not 'for profit'. The question is whether or not free acquisition of copyrighted content can be classed as 'profit'. Considering the nature of the secondary infringement principle, a user is prohibited from supplying infringing copies. Acquiring a copyrighted work in the first place is not in itself the supplying of it. Therefore, the benefit a user receives from the free acquisition of content does not fall into this element.

It is concluded that a client/server user and a P2P user have different positions when it comes to secondary infringement. All four elements can apply to a client/server user. However, a P2P user is unlikely to commit secondary infringement because such user's act does not satisfy all four elements. The fourth element -- for profit -- is missing. A P2P end user does not gain financial profit from sharing content. The secondary infringement elements discussed above are also applicable in criminal cases. In addition, criminal liability needs an internal element namely, the intention to commit the criminal action. Unintentional copyright infringement can only be subject to civil liability. The criminal offence of copyright infringement is considered separately below.

3.3 Are Client/Server and Peer-to-Peer User Activities Criminal Offences under Copyright Act B.E.2537 (1994)?

CA 1994 does not differentiate civil and criminal acts. Infringing acts that are civilly liable can be criminally liable whether they are primary or secondary. Discussion provided in previous sections applies to this section. This section discusses an essential criminal element that is not required in civil action -- intention/wilfulness.

Thailand criminalises copyright infringers to a higher degree than is the practice internationally. TRIPs provide that parties shall have criminal penalties to be applied in the case of wilful and commercial scale copyright piracy under article 61. Under CA 1994 sections 27-30(primary infringement) and 31 (secondary infringement), Thailand copyright infringement criminalisation requires wilfulness on the part of the suspect but does not require an aspect of intended commercial gain.

With regard to the commercial aspect, CA 1994 requires a commercial aspect in secondary infringement but not in primary infringement. The former is similar to the 'for profit' element which will be discussed later below. The latter infringement is that an infringer is criminally liable by certain acts, e.g., reproduction, adaptation and communication to the public under sections 27-30. These sections do not require commercial gain from such acts. It is clear that a defendant can be found guilty of primary

infringement even though he does not have commercial benefit from his infringing acts.[72] In this instance, the criminal penalty is a fine only.[73] If a defendant is found guilty of this infringement with commercial benefit, penalties can increase to imprisonment and/or a heavier fine.[74]

For the wilful aspect, wilfulness differentiates civil from criminal liability. In civil cases, non-wilful acts can be liable although CA 1994 does not so state it. Copyright is a type of right. Copyright infringement is not only subject to CA 1994 but also to the general rules of tort under the Thailand Civil and Commercial Code (CCC). CCC section 420 provides that a wilful and negligent act can be an infringement of a right.[75] An end-user who negligently unlawfully injures the copyright of another is deemed to commit a wrongful act and is bound to make compensation. In such a case of mere negligence, the reparation required could be limited.[76]

In criminal cases, there are external and internal factors. In their application to copyright infringement, external factors are acts which exercise rights that are exclusively reserved for right holders, e.g., rights of reproduction, adaptation and communication to the public. These external acts encompass the same criteria already discussed in section 3.2.1. A client/server or P2P user commits an infringement of reproduction and adaptation rights when he uploads, downloads and shares a copyrighted work on a website or a P2P platform.

The internal factors incorporate wilfulness. Copyright infringement can be held to be criminal only if it is done through a wilful act. Wilful reproduction, adaptation or communication to the public is required as in a general principle of criminal law. Wilfulness is essentially similar to intention under PC 1956 Section 59 paragraph one which provides:

---

[72] *But see* European ASEAN Business Centre (EABC) 2013, "Protecting your Intellectual Property in Thailand," [Online] available: http://www.eabc-thailand.eu/images/files/EABC_PROTECTING_PROPERTY_RIGHT.pdf [accessed: 7 Jan.2014] p.50 ("[t]here is no criminal liability in case of reproduction, adaptation or communication of copyright work when there is no commercial intent of the infringer.")

[73] CA 1994 section 69 and 70 paragraph one

[74] See CA 1994 sections 69 and 70 paragraph two 'by way of trade'.

[75] CCC section 420 provides: A person who, wilfully or *negligently*, unlawfully injures the life, body, health, liberty, property or any right of another person, is said to commit a wrongful act and is bound to make compensation therefore. [Emphasis added]

[76] CCC section 438 paragraph one states: "The Court shall determine the manner and the extent of the compensation according to the circumstances and the gravity of the wrongful act."

"A person shall be criminally liable only when such person commits an act intentionally, except in case that the law provides that a person must be liable when such person commits an act by negligence, or except in case that the law clearly provides that a person must be liable even though such person commits an act unintentionally."

Criminal copyright infringement has to be with "intention" because there is no law provided to indicate that a person is liable when he commits copyright infringement by negligence or without intention. Intention refers to a state of mind in two cognitive areas: (1) consciousness and (2) knowledge of a result. PC 1956 Section 59 paragraph two provides:

"To commit an act intentionally is to do an act consciously and at the same time the doer desired or could have foreseen the effect of such doing."

Consciousness is an awareness state if there is no mental disorder, intoxication or other mental impediment. A client/server and P2P infringer acts consciously in distributing content. Knowledge of a result is satisfied if an infringer desires or could have anticipated the result from his act. An internet end-user desires or could have foreseen the effect of file exchange if he knows the facts which constitute the elements of copyright infringement offences. PC 1956 Section 59 paragraph three provides:

"If the doer does not know the facts constituting the elements of the offence, it cannot be deemed that the doer desired or could have foreseen the effect of such doing."

Knowledge of the facts is different from the facts themselves. Whether or not an upload is a reproduction of a copyrighted work from a user's computer to a website is the fact. Whether the uploader knows that such upload is a reproduction is the knowledge of the fact. Knowledge of a fact is different from knowledge of law. One cannot propose as an excuse that he does not know the law. An end-user could not legitimately claim that he did not know that these acts were prohibited by criminal law.[77] Facts constituting copyright offence elements differ with regard to primary and secondary infringement.

In primary infringement, knowledge of the facts is simply that an end-user has to know his act is one of reproduction, adaptation, communication to the public of the

[77] Buell, S.W. and Griffin, L.K., 2012. "On the Mental State of Consciousness of Wrongdoing", *Law and Contemporary Problem*, 75, 2, 133. [online] Available at: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1671&context=lcp p. 134. [Accessed: 4 March 2016]

copyrighted work without permission. It is not difficult to establish that an end-user knows that he reproduces, adapts and communicates to the public a content by upload, download and share on the internet. Virtually all cases of infringement have no dispute over knowledge of the elements. More commonly, the dispute is whether or not a defendant creates his own work and hence does not reproduce or adapt another's work.

In the 'Kwaokrua' Supreme Court case, no.6804/B.E.2548 (2003), defendants argued that they composed the 'Kwaokrua' article themselves and put it on their website. By taking the majority of words from the original work, with minor differences, the Court held that the defendants had adapted the plaintiff's work. It was argued that two works could be similar in structure and content without imitation. The Court eliminated this likelihood because the similarity was so marked that the work on the defendants' website could not have been made by a different author. The similarity was not just the academic content but also the statements and the use of common English vocabulary. This led the court to believe that the second work was adapted from the first work even though it had not been copied completely word for word. The defendants' argument was ungrounded; hence they were convicted of reproduction and adaptation infringement.

The above case ruled on client/user technology. It too applies to P2P. The Court made a comparison between the second work and the first work in order to infer the factual reproduction and adaptation of the plaintiff's work. The Court does not need to make a comparison between two works in client/server and P2P. They are bound to be virtually identical in that musical works and movies are not normally produced by end-users. An end user knows that his act actually reproduces and adapts a copyrighted work. Knowledge of the fact of infringement is satisfied; reproduction and adaptation knowledge is established.

Knowledge of communication to the public is different. This is because such knowledge of the fact depends on the fact itself. Whether communication to the public is a live performance or not will vary the outcome infringement. If it is a live performance, an end-user will be aware of the fact that that he is performing and airing a copyrighted work to the public via a website or P2P (primary infringement). If the communication is not via a live performance but by playing a copyrighted work through a medium, knowledge of the facts is knowledge of the four secondary infringement elements already discussed in section 3.2.2 above.

Knowledge of the first element is that the user has to know the fact that by uploading content to a website or leaving content in sharing directories in P2P he exposes the work to the public access and this constitutes communication to the public by making available a copyrighted work to the public by distribution or causing perception of content. The second and third elements are satisfied if such a user knows or should have known that the work made available is the copy derived from infringement. The fourth element is met if an infringer knows that he gains profit from his act. As suggested in section 3.2.2, a client/server user can satisfy all the elements. For a P2P user, the missing element is the fourth element. There is no profit knowledge because P2P users do not gain profit from doing this and they know it to be so. Therefore, this criminal element is not satisfied.

It can be concluded that in Thailand client/server and P2P practices are not always criminally liable. The intention of client/server and P2P users is established in primary but not in secondary infringement. In client/server and P2P, a user's intention to commit primary infringement by reproduction and adaptation is clear. A user's intention is also clear with regard to the right of communication to the public by live performance. Secondary infringement of the right of communication to the public sheds a different light. A client/server user's intention to gain benefit can be established while that of a P2P user cannot. Client/server users can commit criminal secondary infringement because they intend to gain profit from their post. In contrast, P2P users do not intend to gain profit because they do not have such benefit from their share on the P2P platform and hence they are not committing criminal secondary infringement.

3.4. Are Client/Server and Peer-to-Peer User Activities Criminal Offences under the Computer-Related Offence Act B.E. 2550(2007)?

The CROA 2007 copes directly with computer crime such as unauthorized access to a protected computer or the data therein. The declared offences relate to malicious code, internet service provider (ISP) responsibility, distribution of false information to the internet and so forth. It has no direct provisions concerning online IP protection. In this respect, there are CROA 2007 offences that are related to copyright infringement through an act against computer data. This is because computer data can be a copyrighted work. CROA 2007 section 3 paragraph 2 states:

"Computer Data means data, statements, or sets of instructions contained in a computer system, the output of which may be processed by a computer system including electronic data, according to the Law of Electronic Transactions."

The computer data definition includes all kinds of data, including sets of instructions, provided that such data is contained in a computer system and is able to be processed by a computer system.[78] A copyright work in digital format, e.g., literature, computer programme, music, movies, can be contained in and processed by a computer system. Therefore, a digital copyright work is in fact computer data. CROA 2007 offences against computer data are section 7 (unauthorised access to computer data)[79], section 14 (1) (importation of forged or false computer data) and section 14 (5) (distribution of forged or false computer data).[80] These offences can be classed as copyright infringement.

Unauthorised access to computer data is an offence related to the circumvention of copyright technological protection measures which is not within the remit of this thesis. Importation and dissemination of copyright work (computer data) is relevant to this thesis. A client/server and P2P user can be found guilty of the importation and dissemination of forged or false computer data under CROA 2007 section 14 (1) and (5). CROA 2007 section 14(1) and (5) states:

"Whoever commits one of the following offences shall be punished with a term of imprisonment lasting not more than five years, a fine of not more than one hundred thousand baht or both:

(1) imports to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to the third party or the public;

---

[78] Thailand, Office of the Court Judiciary, 2003, *Explanation of Computer-Related Offence Act B.E.2550(2007)*, Bangkok: Dokbier Publishing, p.4. [Thai]

[79] Section 7. If any person illegally accesses computer data, for which there is a specific access prevention measure not intended for their own use available, then he or she shall be subject to imprisonment for no longer than two years or a fine of not more than forty thousand baht or both.

[80] Section 14: "Whoever, committing any offence of the followings, shall be punished with imprisonment not more than five years, fined not more than one hundred thousand baht or both:

(1) imports to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to the third party or the public;

…

(5) disseminates or forwards computer data already known to be computer data under (1) (2) (3) or (4);"

…

(5) disseminates or forwards computer data already known to be computer data under (1) (2) (3) or (4);"

CROA 2007 section 14(1) is about the importation of forged or false computer data and section 14(5) is about the dissemination or forwarding of such data. The element of action in these offences is the importation or dissemination of computer data and the element of fact is that the computer data imported is forged or false. 'Dissemination or forwarding' signifies distribution by methods of computer transmission as opposed to physical submission.[81] Computer data can be copyrighted content. Clearly, a client/server user who posts content onto a website imports computer data into a computer system. Likewise, a P2P user can share, import, disseminate and forward computer data. The element of action is satisfied. It is a question of whether an illegally-reproduced copyrighted work is forged or it is otherwise false computer data.

The offence against a document relates to the facts shown on the document. A forged and false document is different. The former is a document that is produced by an unauthorised person in order to use it as a real document.[82] The latter is a document that is brought into existence by one who has a duty to issue the document but the fact the document is intended to certify is not true.[83] False documents do not seem to be involved in online copyright infringement. An infringer is not normally an authorised person who can issue a document, and copyrighted content is not normally issued as a document to certify any fact.[84] Yet, the forged document can be relevant here. An infringed copyrighted work can be deemed a genuine document issued by a copyright owner while an infringing work can be deemed a forged document that an internet user produces without authority.

---

[81] Thailand, Office of the Court Judiciary, *op.cit*., p.29.

[82] PC 1956 Section 264 paragraph 1 : "Whoever, in a manner likely to cause injury to another person or the public, fabricates a false document or part of a document, or adds to, takes from or otherwise alters a genuine document by any means whatever, or puts a false seal or signature to a document, if it is committed in order to make any person to believe that it is a genuine document, is said to forge a document, and shall be punished with imprisonment not exceeding three years or fined not exceeding six thousand baht, or both."

[83] PC 1956 Section 269 paragraph 1: "Whoever, in the pursuance of work in the medicine, law, accountancy or any other profession, making the certification of false document by the manner likely to cause injury to the other person or the public people, shall be imprisoned not more than two years or fined not more than four thousand baht, or both."

[84] Office of the Court Judiciary, *op.cit*., p.26. (explaining that an anti-virus program is false data if it is actually another program and not an anti-virus program.)

The Supreme Court has addressed the issue of differentiation of copyright reproduction and document forgery.

In Supreme Court case no. 96/B.E.2523 (1980), a defendant, without permission, printed 5,000 lesson books for which a co-plaintiff had copyright. The Court ruled that the copyright law was the specific Act which contained the specific offence therein. Reproduction of the whole book was copyright infringement, not the offence of fabricating a forged document. The defendant's act was not the production of a forged document under PC 1956 section 264.[85]

The Court is right in clarifying the different purpose of the two legislations. While PC 1956 protects the integrity of a tangible document, CA 1994 protects an intangible right which subsists in a document, not the document itself. An intangible right in a piece of literature can never be published as a real tangible book.[86] It follows that even though one produces exactly the same book as that produced by a right holder, such production is not the fabrication of a book.[87] The defendant did not produce books in order to disturb the integrity of the original book but to sell them for monetary benefit; hence, disturbing an intangible copyright. Such production is therefore copyright infringement. Indeed, the very same production can also be an act of forgery. Had the original book not been reproduced to commercialise but to assert the fact that the second book is actually the first book, such reproduction would have been the creation of a forged document under PC 1956 section 264.

In online copyright infringement, there has not yet been a case where the Supreme Court ruled directly to the issue whether reproduction of a copyrighted work in digital format came under the classification of copyright infringement or of the fabrication of a document. Applying the ruling of case no. 96/B.E.2523, reproduction of a digital file can be analogous to that of a physical book in that both can be reproduced. According to the Supreme Court, the copyright law applies in this case because it is the specific law provided with a specific offence therein. The internet user commits copyright infringement, not an offence of forgery. This is regardless of the type of format in which the document is produced. It is true that a copyrighted work that is reproduced by an

[85] *See* also, e.g., Supreme Court case nos.954/B.E.2476 (1933) and 466/B.E.2478 (1935).
[86] Suphapholsiri, *op.cit*., p.278 [Internal citation omitted]
[87] *Ibid.*

internet user can be a forged document because it is not produced by an authorised person, i.e., a copyright owner. However, the user does not usually aim to use a reproduced copy as a genuine copy. It is generally known that such a copy is not a genuine copy because it can be reproduced by anyone. Finally, the user aims to distribute the work as an intangible creative work, not to use the work as a fact-certifying document. With these reasons under consideration, a digitally reproduced copyrighted work is not a forged document.

It can now be said that online copyright infringement is not document fabrication. The importation or reproduction of a copyrighted work is not the importation of false computer data. A client/server or P2P user does not commit an offence under CROA section 14(1). Moreover, the dissemination or forwarding of such a copyrighted work is not the dissemination or forwarding of forged computer data under CROA section 14(5).

3.5 Conclusion

3.5.1 Civil Primary Infringement of Reproduction and Adaptation Rights

Thailand's reproduction and adaptation rights protect works in digital format. CA 1994 'reproduction' and 'adaptation' definitions do not clearly state as such.[88] It is the Thailand Supreme Court which interprets these provisions, ensuring the protection of works in digital format. The infringement was found where a physical format had been converted into a digital format.[89] In like fashion, the transformation of a work from an electronic to a physical format was illegal under CA 1994.[90] Finally, reproduction and adaptation can attract infringement when both contents are in digital form.[91]

It can be concluded that a client/server end-user reproduces and adapts copyrighted content when such user uploads the content to a website or a storage server. A P2P end-user reproduces and adapts copyrighted content when such a user downloads and shares the content on a P2P platform. Without permission, these activities are infringement of reproduction and adaptation rights.

[88] CA 1994 section 4 paragraph 13 and paragraph 14 respectively.
[89] Supreme Court case no.6804/B.E.2548 (2003)
[90] Supreme Court case no.5036/B.E.2550 (2007)
[91] Supreme Court case nos. 1829/B.E.2553 (2010), 3882/B.E.2553(2010) and 6802/B.E.2553(2010)

3.5.2 Civil Primary Infringement of the right of communication to the public

For the right to communicate to the public, the research finds that the term 'by any other means' in 'communication to the public right' definition in CA 1994 can signify 'wire or wireless' transmission which includes the internet.[92] The CA 1994 'communication to the public' definition does not require actual access to the content or a real time performance. Mere distribution of the books or mere playing of musical works is a violation of the communication to the public right.[93] If a work is made available at a place where members of the public 'may' access it, this constitutes infringement of the right of communication to the public. A digitised literary work made available on a website is an infringement of the communication to the public right.[94]

The right of communication to the public is subject to either primary or secondary infringement.[95] The means of communication differentiates the two infringements. If client/server and P2P users employ the means of a live performance where no material copies are involved such as 'performing, lecturing, preaching, playing music'[96], primary infringement of the right of communication to the public can take place. If the means is not a live performance where material copies are involved such as 'distribution, causing perception by image and sound', possible infringement will depend on the kind of copyrighted material involved.

If the material is genuine, then there is no infringement of the right of communication to the public by 'distribution'. CA 1994 does not protect the distribution of genuine copies, seeing that the owner of a copyrighted material has the right of ownership.

Of course, if the material is infringing, CA 1994 section 31 prohibits the 'distribution' of counterfeit copies. Selling of VCDs containing music videos produced from a secondary source computer was not primary infringement of communication to the

[92] Supreme Court case no. 6804/B.E.2548 (2003)
[93] Supreme Court case nos.994/B.E.2543 (2000) and 3054/B.E.2548 (2003)
[94] Supreme Court case no.6804/B.E.2548 (2003)
[95] CA 1994 sections 27 (2) and 31 (2) accordingly.
[96] CA 1994 section 4 paragraph 15 'communication to the public' definition

public because the content came from an infringing copy computer rather than from an original VCD.[97]

3.5.3 Civil Secondary Infringement

Secondary infringement concerns acts which use infringing copies under CA 1994 section 31 (1) – (4). There are four requisite elements of secondary infringement which apply to client/server and P2P users.

The first element is satisfied because the circulation of work on the internet by upload, download or share establishes that communication to the public has taken place by means of 'distribution' or 'causing the perception of sound and image' under CA 1994 section 31 (2). Moreover, such circulation also establishes 'distribution in a manner which may cause damage to the owner of copyright' as stated in CA 1994 section 31 (3).

The 2nd element is met. In client/server, distributed content is reproduced from a user's computer to a website. In P2P, such content is gathered into an internet user's computer. Content reproduced from original CDs or VCDs to a computer is described as infringing copies.[98] Accordingly, copies on a website and in a user's computer can be classed as infringing copies.

The 3rd element, the knowledge of infringing copies, is satisfied because a user 'knows' or 'should have known' that the distributing copy is an infringing one.

The 4th element is the commitment of the act for profit. In client/server, a user can gain profit from his content when it is posted on a website. In P2P, a user does not earn any profit which means that this element is non-applicable in P2P.

It is concluded that a client/server user can be culpable of secondary infringement if the user gains profit from posting a work on a website. A P2P user cannot be liable for secondary infringement because the 'profit' criterion fourth element is missing in his case.

---

[97] Supreme Court case no.1829/B.E.2553 (2010) (See also case nos.290/B.E.2548 (2005) and 3882/B.E.2553 (2010))

[98] *See,* e.g., case nos. 290/B.E.2548 (2005) and 7873/B.E.2549 (2006).

3.5.4 Criminal Infringement

The thesis finds that commercial gain is not a required criminal element but it is a factor that can result in an increased penalty.[99] Wilfulness is a required criminal element under Thailand CA 1994 sections 27-30 and PC 1956 section 59.

For primary infringement, it is concluded that client/server and P2P users can wilfully commit criminal actions regarding reproduction and adaptation rights. Wilfulness can be satisfied by knowledge of the fact. It is clear that when a client/server user posts content onto a destination website, he knows that his act actually reproduces and adapts the work on that platform. Client/server users can commit an infringement of the right of communication to the public by the initialization of a live performance of a copyrighted work.

For secondary infringement, the criminal liability of client/server users can only be established when they intend to gain profit from commercialisation of the post. There is no criminal liability for P2P users because the 'for profit' element is not established which means there cannot be an intention for monetary profit.

3.5.5 Computer-Related Offence Act B.E.2550 (2007)

CROA 2007 relates to copyright infringement through an act against computer data. Computer data are all kinds of data including a digitally copyrighted work. CROA 2007 offences against computer data are the importation of forged or false computer data (section 14 (1)), and the distribution or forwarding of forged or false computer data (section 14 (5)).[100] The elements of action -- the importation and dissemination of, or the forwarding of computer data -- are met by client/server and P2P user activities. However, an illegally reproduced copyrighted work is not forged computer data under the Supreme Court interpretation.[101] Neither can a copyrighted work be false computer data. An

---

[99] *See* CA 1994 sections 69 and 70 paragraph two 'by way of trade'.

[100] Section 14: "Whoever, committing any offence of the followings, shall be punished with imprisonment not more than five years, fined not more than one hundred thousand baht or both:

(1) imports to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to the third party or the public;

…

(5) disseminates or forwards computer data already known to be computer data under (1) (2) (3) or (4);"

[101] Supreme Court case no. 96/B.E.2523 (1980) differentiated copyright reproduction from document forgery. It ruled that reproduction of the copyrighted materials was copyright infringement, not the offence of the production of a forged document.

infringer has not been given the authority to issue a real document/content. Copyrighted content is originally produced as intelligible property created by a legitimate creator; it is not produced as a document to certify a fact. For these reasons, it is concluded that a client/server or a P2P user does not commit CROA 2007 offences, i.e., the importation of false or forged computer data into a computer system under section 14(1) and the dissemination or forwarding of computer data under section 14(5).[102]

This chapter concludes that the present relevant Thailand legislation is adequate to combat online infringement activities. Thailand has a similar extent of exclusive right protection of a work in a digital form to that guaranteed by the Berne Convention for the Protection of Literary and Artistic Works 1886 (Berne Convention 1971 revision with 1979 amendments) and also guaranteed by the Agreement on Trade-Related Aspects of Intellectual Property Rights 1994 (TRIPs) as well as by the World Intellectual Property Organization Copyright Treaty 1996 (WCT). Client-server and Peer-to-Peer (P2P) end user activities come under a classification of civil and/or criminal liability under Thailand's CA 1994 and PC 1956.

The civil liability part finds that a client/server and P2P user can be liable for primary infringement of reproduction and adaptation rights. There are some factors that have a bearing on the infringement of the right of communication to the public and its primary and secondary classifications (i.e., infringing/infringed copies and the means of communication).

With regard to the criminal liability, this chapter finds that perpetrator activities can satisfy the intention element required by the criminal principle. Primary infringement of reproduction and adaptation rights may have taken place whereas infringement of the right of communication to the public may not have taken place. This is very similar to the result found in civil liability with the exception of secondary infringement liability. The intention to gain profit from activities affects client/server and P2P user liability in criminal

[102] Another reason being CROA 2007 aims to suppress the public threat to computer communication systems, not the private rights or compoundable offence such as defamation. (Letter from Permanent Secretary of Ministry of Information and Communication Technology to the Superintendent 3 of Technology Crime Suppression Division, No. Tor Kor 0212.2/6312, Dated: 7 June 2016 [Thai]) It should be noted that copyright infringement is a compoundable offence and is not an offence under CROA 2007 § 14(1).

secondary infringement. Moreover, this thesis finds that copyright infringing acts cannot be criminalised under the CROA 2007.

Having concluded that Thailand substantive law is sufficient, this thesis now turns to examine the extent of current enforcement and the remedies provided. The next chapter discusses Thailand court remedies in comparison with US notice and takedown digital copyright protection.

Chapter 4: Notice and Takedown: Thailand and US Approaches

4.1. Introduction

It has been concluded in chapter 3 that client/server user activities in file dissemination are by and large an infringement of copyright as conferred by Thailand's substantive law, i.e., Copyright Act B.E.2537 (1994) (CA 1994). This chapter is concerned with online copyright protection remedies provided by Copyright Act (No.2) B.E.2558 (2015) (CA 2015). CA 2015 provides for court proceedings and its orders as a remedial means. However, it is argued that the application of court orders is not a suitable measure for client/server infringement, suggesting there needs to be a change of provision. The chapter discusses and compares CA 2015 section 32/3 with the US Digital Millennium Copyright Act 1998 section 512 (or Title 17 of United State Code which is the Copyright Act) (hereinafter '17 U.S.C. § 512') concerning Notice and Takedown (N&T) in application to the client/server online infringement protection. The chapter is structured in accordance with the functional comparative law method as described in the chapter 1 methodology part.

To begin comparing legal and functional aspects of online protection regime, a thorough understanding of the home country's black letter law is a prerequisite. Thailand CA 2015 provisions constitute the rules of the home country of which clarification is provided in the following section.

4.2. Thailand Copyright Act (No.2) B.E.2558 (2015) Provisions for Digital Copyright Protection

This section explores CA 1994 as amended by CA 2015. The section shows CA 2015's background, purposes and legislative surface. In addition, it focuses on provisions relevant to digital copyright protection measures. Such provisions will be explained particularly when they apply to internet user infringement on client/server platforms.

CA 2015 was proclaimed in the Government Gazette issue of 5th February 2015.[1] In preparatory work by the Department of Intellectual Property (DIP), Ministry of

[1] Under CA 2015 Section 2, the Act comes into force on the day after 180 days from the day of proclamation.

Commerce, the phrase "Digital Right Management Protection" was put in brackets after "Copyright Act (No…) B.E. …". This signals the importance of digital right management protection to Thailand on account of the key role it plays in the two WIPO treaties. CA 2015 aims to bring Thai copyright law into line with the two WIPO treaties of 1996. The "Reasons for the Enactment" (the Reasons) annexed to CA 2015 do not clearly show Thailand's intention to become a signatory to WCT and WPPT. However, they do apparently show the need to introduce digital rights management (DRM) and technological protection measures (TPM) into the Thai copyright system. The Reasons read:

"At present, digital right management and technological protection measures are employed to protect copyright and performer's rights. Digital right management and technological protection measures shall merit protection. The exceptions of, and limitations to, copyright and performers' rights shall be increased. Additionally, the courts shall be empowered to order infringers, who enable copyright work or performers' works to have widespread public access, to make more adequate compensation. Also, the courts shall be empowered to order the confiscation and destruction of the things used and, illegally produced or imported to the Kingdom of Thailand, in cases of copyright and performers' right infringing commissions. Therefore, it is necessary to ratify this Act."[2]

The main purpose of CA 2015 is to bring CA 1994 into line with technological advancement. CA 2015 provisions encompass many areas of digital copyright protection. In essence, DRM, TPM protection as well as the N&T system have been outlined.[3] CA 2015 addresses the following topics:[4]

(1) defines the terms DRM, TPM and circumvention of TPM;

(2) the introduction of exceptions to infringement of distribution of originals or copies of copyright work;

---

[2] CA 2015 Endnote

[3] The U.S. Commercial Service, the U.S., n.d., 'IPR Toolkits for the Kingdom of Thailand', [Online] Available at: http://origin.www.stopfakes.gov/sites/default/files/thailand_toolkit.pdf p.2 [Accessed: 8 March 2014].

[4] The Prime Minister office, Thailand 2013, "the Note" accompanied the Draft Copyright Act (No. …), Document enclosed with a Letter to the President of the House of Representative No. Nor Ror 0503/24266, dated the 10th of September 2556(B.E.)(2013), p.1.[Thai] Available:https://edoc.parliament.go.th/Meeting/MeetingViewer.aspx?id=143 [Accessed: 30 January 14.]

(3) the introduction of exception to infringement for necessary reproduction in computer systems and for ISPs who do not control, initiate or direct the infringement in their computer systems;

(4) grants performers' rights to identify themselves as the performers, and their rights to the integrity of the performance by prohibiting acts which could damage a performer's fame and honour;

(5) introduces additional protection for DRM and TPM, the filing of lawsuits, penalties to disruption of DRM and circumvention to TPM along with the fixing of the penalising fines thereof;

(6) empowers the courts to direct infringers to compensate for any damage incurred, increased to not more than double in the case of deliberate intention or knowingly making copyrighted work extensively accessible to the public;

(7) enhances the courts powers in criminal cases to order the confiscation of the things produced in, or imported to, the Kingdom of Thailand which are considered to be infringing, along with anything that is used in an infringing commission, and to order their destruction or the making of them unworkable.

There is no amendment to enlarge the extent of rights of copyright holders in digital format and in the internet as to online activities against reproduction, adaptation and communication to the public. This can be an indication that the current substantive copyright law is sufficiently applicable in such a circumstance; hence, no need to change.[5] Topic (3) above concerns ISP's exception from copyright infringement in online communication. The amendment also provides the court injunction as a remedy for the digital communication protection purposes. In the comparison between the US and Thai legislation, the first highlighted topic is the Thai procedural court remedies in contrast to the US notice mechanism.[6] The latter reveals the difference in ISP classifications and their exemptions. These topics follow in the two sub-sections below.

[5] *See* chapter 3: 3.2.1 Can Client/Server and Peer-to-Peer User Activities be Primary Infringement and What Are the Exclusive Rights Affected?

[6] *See* the US N&T procedure in 4.5.1 Types of Service Providers Received Notification and their Safe Harbours, below.

4.2.1 Thailand's Court Remedies for Online Copyright Infringement

In an attempt to enforce online infringement, CA 2015 section 4 adds section 32/3 to CA 1994. Section 32/3 concerns court injunctions and procedure to stop on-going infringing activities. It is in fact comparable to the US N&T system. Section 32/3 provides:

"In cases where it is reasonable to believe that copyright infringement has *taken place* within a service provider's computer systems, the right holders may file a motion to the court to *cease the infringement*.

For the purpose of this section, a service provider means:

(1) A person who provides service to the public with respect to access to the internet or other mutual communication via a computer system, whether on their own behalf, or in the name of, or for the benefit of, another person

(2) A person who provides services with respect to the storage of computer data for the benefit of another person

The motion in paragraph one shall have clearly defined details about information, evidence and request as follows:

(1) Name and address of the service provider;

(2) Allegedly infringed copyrighted work;

(3) Work allegedly made by infringement;

(4) Process of investigating time and date of detection and infringing acts or circumstance as well as infringement evidence;

(5) Potential damage incurred by the alleged infringing acts;

(6) Request to ISPs to *remove the alleged infringing content* from a service provider's computer system or to *cease infringement by other means*;

When the court receives the motion under the first paragraph, it shall hold examination. If it finds that the motion provides complete details in accordance with paragraph three and it is *necessary* and *reasonable* to grant an order, it shall make an imposition on the service providers to *cease the alleged infringing acts* or to *remove alleged infringing work* from the service provider's system within the time designated by the court. The order shall be enforced instantly. The court shall inform the service provider without undue delay. After the court orders have been served, the right holders

shall take legal action against infringers within the time designated by the court for such cessation or removal.

If service providers do not control, initiate or direct the infringement in their systems and the service providers execute the court order under paragraph four, they are exempted from liability for the alleged infringement which has taken place before the court orders were served and after the order lapses.

The service providers shall not be responsible for any damage incurred by executing the court order under paragraph four." [*Emphasis* added]

In general, Section 32/3 paragraph one provides that where it is reasonable to believe that copyright infringement has 'taken place' within a service provider's (SP's) system, a right holder can file a motion for a court injunction. As suggested in chapter 3, the infringement (both primary and secondary) has 'taken place' within online service provider's system when an end-user reproduces, adapts and communicates to the public copyrighted content by downloading, uploading and file sharing to the website or in a P2P platform.

It is the right holder's responsibility, not that of the SP, to investigate infringement on the SP's computer systems. Section 32/3 paragraph two defines the term 'service providers'. Upon detection of infringement, the right holder can gather evidence and initiate the case by filing a motion to the Central Intellectual Property and International Trade Court (CIPIT).[7] Paragraph three requires that the motion have the necessary information about service providers, infringed and infringing work, investigating data, any damage suffered, and the requested court order. Paragraph four states the proceedings after receipt of the motion by the court. If the court finds that the motion has sufficient information required by the law it will then hold an examination.[8] The motion is not the type of *ex parte* basis; therefore, before the court renders the order it has to summon the

[7] CIPIT has jurisdiction over an IP dispute countrywide pursuant to the Act for the Establishment of and Procedure for Intellectual Property and International Trade Court B.E.2539 (1996) Section 7 and 8. *See* CIPIT website at: http://www.ipitc.coj.go.th/?co=en for more detail.

[8] If not sufficient, the court has a preliminary discretion to dismiss, accept or direct further information under Thailand Civil Procedure Code B.E.2477 (1934) (CIPC 1934) § 18. CIPC 1934 is the procedural Act which generally applies to all types of civil cases if a *sui generis* does not provide otherwise.

other party, namely an SP, to enter into the case.[9] After the examination, the court shall grant the order provided it is satisfied that the petitioner has shown ample evidence in proof of his plea. The court order must be necessary and reasonable concerning the circumstances.[10] The order can be granted pursuant to the right holder's request but must not contain 'something beyond or not requested'.[11] A request can be to cease the alleged infringing acts or to remove alleged infringing work from the service provider's system.[12] The court can stipulate the time period for implementation. In principle, the order shall be in force instantly. In practice, the directed party needs to know the order before it can act accordingly; therefore, the law stipulates that the party concerned must be informed without unjustifiable delay.[13] After the court order, the right holders have to initiate the infringement case within the time fixed therein or the order will be invalid.[14] The law does not specify whether the right holders have to initiate criminal or civil proceedings. The service providers characterised in paragraph two are discharged from liability provided they meet the qualifications stipulated in paragraphs five and six.

In terms of a comparison of procedure between the Thailand and the US systems, there are manifest differences. While the US right holders serve a notification to ISPs, Thai right holders file a motion. In the Thai system there is no notice by right holders to ISPs, no content taken down by ISPs, no ISP notifications to end-users, no counter-notice by end-users and other procedures as provided for in the traditional N&T system of the US.[15] Moreover, the motion does not require information about allegedly direct end-users. In effect, end-users are not notified and unable to enter into law proceedings.

CA 2015 stipulates that a service provider is subject to the court injunction if infringement takes place in its system. The term "service providers" is generally defined in

---

[9] CIPC 1934 § 21 stipulates:
"When a party files a statement or motion to the court;
…
(2) If this Code does not provide that the request is *ex parte,* the court shall not deliver the order without giving the opponent party or other parties a chance to contradict, pursuant to the provisions of default of appearance.
…"

[10] CA 2015 § 32/3 paragraph four

[11] CIPC 1934 § 142 paragraph one provides that "The court decree or order shall decide all claims in the complaint but it shall not decide or grant something beyond or not requested in the complaint…"

[12] § 32/3 paragraph four

[13] *Ibid.*

[14] *Ibid.*

[15] *See* N&T proceedings in 4.5.2 Notice and Takedown Procedure and Online Infringement below.

section 32/3 paragraph two (1) and (2). In order to file a motion against service providers, ones need to know who the service providers are, how the law defines service providers including how they are classified. The following sub-section addresses these questions.

4.2.2 Clarification of Meaning and Classification of Service Providers under CA 2015 § 32/3 and the Other Relevant Regulations

CA 2015 § 32/3 divides service providers into two main categories. The categories are characterised by their functions. The first category simply refers to telecommunication access service providers (section 32/3 paragraph two (1)). The second category suggests content storage service providers (section 32/3 paragraph two (2)).

The first category encompasses telecommunication via the internet and any other medium. The term 'other mutual communication via a computer system' makes it clear that the term 'service provider' signifies any telecommunication services such as mobile phone, fixed line telephone, satellite, etc.[16] In the same fashion, the second category includes content storage providers of all sorts of telecommunication services.

Therefore, 'service providers' has a broader meaning than 'internet service providers' (ISPs). "The term 'service provider' is defined to include telecommunication and broadcast carriers (including ISPs) as well as all access-point providers and online service providers."[17] The term, however, does not include telecommunications-related business which does not entail information exchange such as Physical Media, Cabling or Fibre Optic.[18]

In detail, section 32/3 paragraph two (1) and (2) definitions show there are different kinds of ISPs. ISPs normally provide internet access which makes them specifically called 'internet access providers' (IAPs). IAPs operate *on their own behalf* when they provide *internet access service* for other persons.[19] ISPs can be Internet Hosting Providers (IHPs) which provide services with respect to the *storage of computer data for*

---

[16] CA 2015 § 32/3 paragraph two

[17] Center for Democracy and Technology, 2011. "Data Retention Mandates: A Threat to Privacy, Free Expression and Business Development", [Online], Available at: https://cdt.org/insight/data-retention-mandates-a-threat-to-privacy-free-expression-and-business-development-1/ p. Appendix: Data Retention in Thailand [Internal Citation omitted], [Accessed: 21 August 2016].

[18] MICT Notification No. 5 (1) and Annex A below.

[19] Section 32/3 paragraph two (1)

the benefit of another person.[20] ISPs can be Network Service Providers (NSPs) which are the internet backbone that provides connections across IAP and IHP computer systems.[21] IHP's storage service covers the internet connection to the computer data stored.[22] The stored webpages, files and information can be owned by Internet Content Providers (ICPs) or individual end-users. IAPs and NSPs can also host the storage. These combination services blur ISP definitions and classifications. All IAPs, NSPs, IHPs and ICPs are nowadays collectively called ISPs under the term 'service providers' CA 2015 § 32/3. The communication across various ISP computer systems reflects the necessity of information exchange, hence the so-called internet. ISPs in this regard are service providers under § 32/3 paragraph two (1) because they are run by persons who provide service to the public with respect to *mutual communication via a computer system*. ISPs mutually assist the telecommunication system by allowing other networks or users to transmit data through their systems which means that they operate *in the name of* or *for the benefit of another person* -- other ISPs and/or users.[23] NSPs are larger than ISPs in that they may also contract to local ISPs allowing them to use their network connection or storage facility across countries.[24] Such NSPs operate *in the name of* their local ISP contractors pursuant to Section 32/3 paragraph two (1).[25]

The different types of the ISPs mentioned above are not clearly categorised by CA 2015. CA 2015 section 32/3 paragraph two defines 'service providers' exactly the same 'service providers' defined in section 3 paragraph four of Computer Related Crime Act B.E.2550 (2007) (CRCA 2007).[26] CA 2015 does not authorise any subordinate law in clarification of the definition. CA 2015 will require a court interpretation of the term 'service provider'. There is relevant legislation in a certain aspect of the term 'service

---

[20] Section 32/3 paragraph two (2)

[21] Techopedia, n.d., "Network Service Provider" [Online] Available at: http://www.techopedia.com/definition/27327/network-service-provider-nsp [Accessed: 20 June 2015]

[22] Amornpinyokiat, P. 2010, *Computer-Related Crime B.E. 2003 Explanation*, Bangkok: SE-Ed Plc. p.19. [Thai]

[23] Section 32/3 paragraph two (1)

[24] Techtarget, *op.cit.*

[25] Techtarget, *op.cit.*

[26] CRCA 2007 section 3 paragraph four states:

"Service Provider shall mean:

(1) A person who provides service to the public with respect to access to the Internet or other mutual communication via a computer system, whether on their own behalf, or in the name of, or for the benefit of, another person;

(2) A person who provides services with respect to the storage of computer data for the benefit of the other person."

providers' in computer crime which can be used in intellectual property crime as court's interpretative guidance.

CRCA 2007 section 26 paragraphs one requires that service providers store computer traffic data for the purpose of investigation and proof of evidence.[27] Paragraph three allows the Minister of Information and Communication Ministry to establish 'types of service providers to whom the provisions under paragraph one shall apply'.[28] The Ministry of Information and Communication Technology Notification on Rules for Service Providers' Computer Traffic Data Storage B.E.2550 (2007) (MICT Notification) implements the provisions by categorising service providers into two classes. The first class is associated with telecommunication access service providers under MICT Notification No. 5 (1) and the second is related to content storage service providers under MICT Notification No. 5 (2).

MICT Notification No. 5 (1) makes provision for telecommunication access service providers under CRCA 2007 section 3 paragraph four (1) to be characterised into four types:

a. Telecommunication and Broadcast Carrier, e.g., Fixed Line Telephone Service Provider, Mobile Telephone Service Provider, Leased Circuit Service Provider (Fibre Optic, ADSL, Frame Relay, etc.), Satellite Service Provider, etc.

b. Access Service Provider; e.g., Internet Service Providers (wired or wireless), Entrepreneurs who offer internet access in their premises (such as accommodation, rental rooms, hotels, pubs and restaurants), and Internet Access Services to governmental organisations, companies and academic institutions. [IAPs]

---

[27] CRCA 2007 Section 26:

"A service provider must store computer traffic data for at least ninety days from the date on which the data is input into a computer system. However, if necessary, a relevant competent official may instruct a service provider to store data for a period of longer than ninety days but not exceeding one year on a special case by case basis or on a temporary basis.

The service provider must keep the necessary information of the service user in order to be able to identify the service user from the beginning of the service provision, and such information must be kept for a further period not exceeding ninety days after the service agreement has been terminated.

The types of service providers to whom the provisions under paragraph one shall apply and the timing of this application shall be established by a Minister and published in the Government Gazette.

A service provider who fails to comply with this Section must be subject to a fine of not more than five hundred thousand baht."

[28] *Ibid*., paragraph one.

c. Host Service Provider; e.g., Web Hosting, Web Server, File Server, File Sharing, Mail Server Service Provider (E-mail provider) and Internet Data Centre [IHPs].

d. Internet Shop; e.g., Internet Cafés and Online Game Shops.

The reason why MICT Notification No. 5 (1) embraces IHPs (category c) of the telecommunication access service providers is because IHPs need to provide internet connection to their website or server clients although they themselves may not be the telecommunication corporations.[29] Therefore IHPs can hardly deny that they have a role as access service providers (category b). There are other instances where a service provider can fall into the two categories. The mobile telephone company (category a) can also provide internet access to its subscriber (category b). Table 1 below is the table in the MICT Notification Annex A which summarizes service providers under MICT Notification No. 5 (1).

Table: 1 Telecommunication Access Service Providers under MICT Notification No. 5 (1)

Types	Examples
a. Telecommunication and Broadcast Carrier	1) Fixed Line Service Provider 2) Mobile Service Provider 3) Leased Circuit Service Provider, e.g., Leased Line, Fibre Optic, ADSL (Asymmetric Digital Subscriber Line), Frame Relay, ATM (Asynchronous Transfer Mode, MPLS (Multi-Protocol Label Switching) except for mere physical media or cabling service without internet signal nor IP Traffic such as Dark Fibre, Fibre Optic 4) Satellite Service Provider
b. Access Service Provider [IAPs, ISPs]	1) Internet Service Provider (ISP): wire/wireless 2) Businesses serving computer network access service, e.g., hotels, restaurants, apartments 3) Private/Public Entities serving computer network access to others such as government offices, private companies, educational institutes

[29] The same is true for the US system. 17 U.S.C. § 512 (k) (1) (B) provides a definition of 'information residing services' to cover mere conduit ('Transitory Digital Network Communications').

Types	Examples
c. Hosting Service Provider [IHPs, NSPs]	1) Web Hosting, Web Server 2) File Server or File Sharing 3) Mail Server Service Provider (E-mail provider) 4) Internet Data Centre
d. Internet Café	1) Internet Café 2) Online Game Café

Table 1 indicates that all types of service providers offer internet, website hosting servers and other communication access to the public. These types of service providers are the same service providers as CA 2015 § 32/3 paragraph two (1). Web hosting/server (or IHPs in category c.) offers a cyber storage for websites and internet connection thereof.[30] This can be confusing with content service providers under MICT Notification No. 5 (2).

MICT Notification No. 5 (2) provides that content service providers under CRCA 2007 section 3 paragraph four (2) are the service providers who provide computer data and storage through applications (Content and Application Service Provider, in other words, Internet Content Providers (ICPs)). The term in CRCA 2007 section 3 paragraph four and CA 2015 paragraph two (2) "...provide...the storage of computer data for benefit of the other person." can lead to confusion between IHPs and ICPs. In this regard, the law is not clear whether or not a website providing data which are produced by themselves in order to attract visits from audiences is fallen into an ICP classification.[31] The storage can be deemed that it is only for the website owner's content; hence, not 'for the other person'. Put differently, the storage provided in such a website can be argued that it is the information for audiences; hence, 'for benefit of the other person'. Therefore, the websites are in doubt of being classed as an ICP under CA 2015 paragraph two (2).

[30] As to client/server user activities, upload results in a copy on the targeted server and a download produces one on an individual's computer. This constitutes reproduction of works. (*See* chapter 3: 3.2.1 Can Client/Server and Peer-to-Peer User Activities be Primary Infringement and What Are the Exclusive Rights Affected?) Therefore, IHPs can be pointed as a target in a court motion under CA 2015 § 32/3.

[31] e.g., newspaper, TV or radio broadcast websites.

On the contrary, the other websites operate business on a server computing system. In doing so, they need to keep their customer's data which in effect offer storage of data for their customers.[32] They can be fallen into a service provider providing 'the storage of computer data for benefit of the other person' under CA 2015 paragraph two (2). Some of these websites involve user-generated content which is potentially infringing copyright. These include social network websites/platforms such as Facebook, Instagram and video and music websites such as YouTube, DailyMotion. It is these websites that are the platform for client/server communication under scrutiny of this thesis. Table 2 below is one of the tables annexed to MICT Notification which summarises service providers under MICT Notification No. 5 (2).

Table 2: Content Service Providers under MICT Notification No. 5(2)

Types	Examples
Content and Application Service Provider [ICPs]	1) Web Board or Blog 2) Internet Banking and Electronic Payment Provider 3) Web Service 4) e-Commerce or e-Transactions

Table 2 consists of web board and blog, and web service.[33] It shows types and examples of service providers under MICT Notification No. 5 (2) which can be the same service providers as CA 2015 § 32/3 paragraph two (2).

To some extent, Thailand and the US service provider definitions are similar. The CA 2015 § 32/3 definitions encompass merely two classifications: telecommunication access service provider and content service provider. The US DMCA § 512 (k) (1) provides 'service provider' definitions which are divided into two classifications -- transmission function classification (§ 512 (k) (1) (A)) and all other functions classification (§ 512 (k) (1)

[32] e.g., Web Board Providers, Blog Providers, Internet Banking Services, Electronic Payment Services, Web Services, E-Commerce Services and E-Transactions Services.

[33] These ISPs were the origin of the early dispute between right holders and ISPs in the US. *See*, e.g., *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D.Fla. 1993), *Sega Enterprises Ltd. v. MAPHIA*, 857 F. Supp. 679 (N.D. Cal. 1994) and *Religious Technology Center v. Netcom Online Communication Services, Inc.*, 907 F.Supp. 1361 (N.D. Cal. 1995).

(B)).[34] ICPs and IHPs are both in the same latter classification which is different from Thailand whereas CA 2015 does not place ICPs in the same classification as IHPs. As will be shown in the later sections both ICPs and IHPs involve in client/server technology.

From the legislation point of view, it is clear that not all classifications apply to the client/server environment. However, from the business practice point of view, there are many occasions where a telecommunication access service provider can also be one type of content service providers. As examples, a mobile phone communication and internet access service can offer applications such as location finder, games, news, radio, television.[35] It can also offer application for P2P file sharing and client/server content distribution.[36] Therefore, such a service can be both telecommunication access and content service providers. This can be confusing in applying client/server protection measures. The question is against what ISP classification(s) the court motion can be filed. The next section will clarify different ISP systems which can inadvertently accommodate client/server infringement. As will be seen below, only an ISP with its specific function can be requested to implement the court order.

4.3. Functionality and Limitations of the Thai Court System in Client/Server Technology[37]

This section considers the functionality and limitations of CA 2015. The function of CA 2015 can be justified through its interpretation and usage. The section interprets

---

[34] DMCA § 512 (k) (1) provides:
(k) Definitions
(1) Service provider.--
(A) As used in subsection (a), the term 'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
(B) As used in this section, other than subsection (a), the term 'service provider' means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)."

[35] Cutlack, G. 2015, "Best free Android Apps 2015" [Online] Available at: http://www.techradar.com/news/phone-and-communications/mobile-phones/70-best-free-android-apps-2013-687252 [Accessed: 17 June 2015]

[36] Rogerson, J. 2016, "Best free Android Apps 2015: 100 You Must Download" [Online] Available at: http://www.techradar.com/news/phone-and-communications/mobile-phones/70-best-free-android-apps-2013-687252 [Accessed: 22 August 2016]

[37] At the time of writing in 2015, CA 2015 had just come into effect. There are no institutions, as yet, currently applying the law which otherwise might help this study on the practical aspect of the law. This section is the author's attempt to discuss the law functionality as applied to client/server technologies.

'taken place' to find the involved service providers in a client/server environment.[38] The following questions will be addressed; what service providers relate to the client/server, what is the service provider's function that determines its involvement, and what request can a right holder make? Here the practical extent of the court order from the interpretation of the term 'cease the infringement' is also discussed.[39] Finally, the section discusses if the CA 2015 court system has any functional limitations at all in client/server relationships.

4.3.1 Service Providers Affected by the Court Order under Copyright Act (No.2) B.E.2558 (2015)

CA 2015 offers a broad definition of 'service providers' and their telecommunication systems. Reproduction, adaptation and exposure of works to the public take place virtually in all modes of telecommunication services including telephone, television, radio and other carrier services.[40] CA 2015 § 32/3 paragraph one states that an SP can be requested to stop the copyright infringement if there are reasonable grounds to believe that the infringement has 'taken place' in the provider's computer system. An SP can be subject to the court order under CA 2015 § 32/3.[41] Musical works can simply be sent via a telephone system while movies can be broadcast through television. Note however, that in order to satisfy legal protection measures, simply serving a court motion on telephone and broadcast carriers is rarely helpful because they are a one-off measure.

Protection measures are needed to stop infringement repetition. These activities are repeating commissions.[42] Content is uploaded on the internet once but can be viewed unlimited times afterward. Individuals who use the internet can initiate an on-going infringement that may require a court injunction. Therefore, a service provider under CA 2015 Section 32/3 paragraph two can be narrowed down to an internet service provider (ISP). There are three relevant ISPs.

---

[38] CA 2015 § 32/3 paragraph one

[39] CA 2015 § 32/3 paragraphs one, three (6) and four

[40] The definitions of 'reproduction', 'adaptation' and 'communication to the public' in CA 1994 protect change of work in any manner. (*See* chapter 3: 3.2.1.1 Reproduction Right, 3.2.1.2 Adaptation Right and 3.2.1.3 The Right of Communication to the Public)

[41] It should be noted that although a service provider is subject to implementation of the court order under § 32/3, it is protected from copyright infringement liability in its normal operation under § 32/2.

[42] *See* Chapter 2 -- 2.2 Current Trends in the Field of Digital Copyright Infringement.

1) Internet Access Service Providers (IAPs) under MICT Notification No. 5 (1) (b);

2) Internet Hosting Service Providers (IHPs) under MICT Notification No. 5 (1) (c); and

3) Internet Content Service Providers (ICPs) under MICT Notification No. 5 (2)

All the three are referred to as ISPs. The first, IAPs, are in the telecommunication access provider class under CA 2015 Section 32/3 paragraph two (1). According to MICT Notification, the second, IHPs, are also in the same telecommunication access provider class. The third, ICPs, are classed as computer data storage service provider under CA 2015 Section 32/3 paragraph two (2). All of these ISPs are service providers that are subject to the court order under CA 2015 Section 32/3 paragraph two.[43]

IHPs offer central server storage. ICPs administer a web board, blog, and web service. Reproduction, adaptation and communication to the public of copyright 'take place' in the server computer's system when client/server users post, store or publish copyright content.[44] IHPs and ICPs are subject to the CA 2015 court order. IHPs and ICPs have capacity to remove the content posted or disable access to it. A right holder can file a motion against such ISPs.[45] The right holder can request the removal of the content, the disabling of access to such content or the prohibition of the whole website from operation (website blocking).[46] In cases where IHPs and ICPs locate and operate abroad, it is clear that a Thai court order for content removal cannot succeed in removing content residing outside its jurisdiction. In such instances the motion can request something be done with the connection established by domestic IAPs. This includes disabling access to a server/website (another kind of website blocking).[47]

---

[43] Service providers of the US and Thailand who cooperate with law enforcement can shelter themselves from liabilities. This thesis uncovers user's liabilities and the protection measures; ISP liabilities and exemptions are of no concern in this thesis.

[44] For discussion of how posting, storing and publishing the copyrighted content take place in ISP's server, *see* chapter 2: 2.2.1 Client-Server Protocol, and for discussion of how these acts can be the infringement of copyright, *see* chapter 3: 3.2.1.1 Reproduction Right, 3.2.1.2 Adaptation Right and 3.2.1.3 Communication to the Public Right.

[45] By analogy, to file a motion is the same as to send a notice for the content to be taken down in the US N&T. (*See* 4.4. Functionality of the US Notice and Takedown below)

[46] *See* 4.3.2.1 Website blocking and Disabling Access to Content below.

[47] An IAP internet connection system can be held as the place where the copyright infringement arises. (*See* chapter 5 -- 5.2.1 Service Providers Affected by the Court Order in its Application to P2P under CA 2015 § 32/3.)

IAPs are merely a conduit similar to a pipe that transmits information (Mere Conduit ISPs). Reproduction and adaptation can 'take place' in the cache system[48] when copyright content is sent through the pipe from one point to other points. The cache system facilitates later viewing by recipients. The viewing attracts infringement of communication to the public right.[49] Therefore IAPs can be vulnerable to the filing of a motion. As IAPs do not provide information or information space but only an information route, they are not actually the platform for end-users and are not the target for content removal. IAPs play more important roles in P2P with the connection to the internet. Chapter 5 of this thesis will discuss how IAPs can be affected by CA 2015.

In conclusion, copyright infringement 'takes place' across all sorts of ISP computer systems. All ISPs can be the subject of a petition and can be forced to take certain actions. The definitions are broad enough to cover all types of ISPs where online protection is sought. CA 2015 § 32/3 paragraph two categorises ISPs by the definition of their functions. ISP definition under CA 2015 § 32/3 paragraph two (1) encompasses IAP and IHP functions. ISP definition under CA 2015 § 32/3 paragraph two (2) involves ICP functions. The motion needs to address the appropriate ISP function. In doing so, the court can determine if an order is 'necessary' in the circumstances under CA 2015 § 32/3 paragraph four. The term 'necessary' is discussed in the next section.

4.3.2 Is a Court Order 'Necessary' in Online Copyright Infringement Especially in the Client/Server Platform?

Upon receipt of the motion, the court shall hold examination. Under CA 2015 § 32/3 paragraph four, if the court finds that it is 'necessary' to grant an order, it can make an imposition on service providers to stop the infringing activities.[50] This section examines

[48] System Caching is a temporary file storage system. It is one of the four classifications under DMCA § 512 (b) (*See* 4.5.1 Types of Service Providers Receiving Notification and their Safe Harbours below.)

[49] For a discussion of digital infringement of reproduction, adaptation and communication to the public rights, *see* chapter 3: Thailand Substantive Copyright Protection Legislation Applicable to Client/Server and Peer-to-Peer User Infringement.

[50] CA 2015 § 32/3 paragraph four states:

"When the court receives the motion under the first paragraph, it shall hold an examination. If it finds that the motion provides complete details in accordance with paragraph three and it is *necessary* and reasonable to grant the order, it shall impose upon service providers to cease the alleged infringing acts, or to remove alleged infringing work from the service provider's system, within the time designated by the court. […]" [Emphasis added]

how the term 'necessary' can be substantiated in client/server and P2P circumstances and if the term justifies extent of the injunction.

There is no definition of the word 'necessary' provided by the law. CA 2015 § 32/3 is a type of interlocutory injunction. On the one hand, the interlocutory injunction aims to facilitate the future judgment execution so that a winning party is able to confiscate a losing party's property temporarily during the hearing.[51] On the other hand, the injunction has an objective of stopping the defendant's on-going contract default or tort while alleviating the plaintiff's on-going damage.[52] Here, the latter principle can be imported to clarify the 'necessary' ground.

In Thailand, the civil procedure code that applies to civil cases is Civil Procedure Code B.E. 2477 (1934) (hereinafter CIPC 1934). CIPC § 254 allows a petitioner to request for an injunction as he files a lawsuit or at any time before the court renders its decision. CIPC § 254 stipulates different kinds of interlocutory injunctions, e.g., seizure of the property in dispute, holding the change of registration of the property in dispute, and arrest and temporary detention of the defendant, under CIPC § 254 (1), (3), and (4) accordingly. CIPC § 254 (2) enjoins the defendant from repeating or continuing infringing activities.[53] CIPC 1934 § 254 paragraph one (2) provides:

"In a case other than a petty case, the plaintiff is entitled to file with the Court, together with his complaint or at any time before judgment, an *ex parte* application requesting the Court to order, subject to the conditions hereinafter provided, all or any of the following protective measures:

...

---

[51] Thailand Civil Procedure Code B.E. 2477 (1934) § 254 paragraph one (1) provides:

"In a case other than a petty case, the plaintiff is entitled to file with the Court, together with his complaint or at any time before judgement, an *ex parte* application requesting the Court order, subject to the conditions hereinafter provided, to include all or any of the following protective measures:

(1) The seizure of attachment before judgment, of the whole or part of the property in dispute or the defendant's property, including any money or property owing to the defendant by a third person;

..."

[52] CIPC 1934 § 254 (2)

[53] CIPC 1934 § 254 (2) and CA 2015 § 32/3 are not similar in that a CIPC § 254 (2) petitioner can file an *ex parte* motion for the interlocutory injunction while the CA 2015 § 32/3 cannot. A CA 2015 § 32/3 petitioner can file the motion in a similar time frame as that of CIPC § 254 (2). Although CA 2015 § 32/3 does not state clearly when exactly a petitioner can file the motion, it can be implied from the language of CA 2015 § 32/3 paragraph four, "the right holders shall initiate a legal action against infringers within the time designated by the court for such cease or removal", that the motion needs to be filed before the claim itself is filed.

(2) A temporary injunction restraining the defendant from repeating or continuing any wrongful act or breach of contract or the act complained of, or other order minimizing trouble and injury which the plaintiff may henceforward sustain on account of the defendant's act, or a temporary injunction restraining the defendant from transfer, sale, removal or disposal of the property under dispute or the defendant's property, or an order stopping or preventing the wasting or damaging of such property, until the case becomes final or until the Court has otherwise ordered;

..."

While CIPC § 254 subsections (1) - (4) list the potential injunctions, CIPC § 255 subsections (1) - (4) designate different conditions for granting different injunctions. CIPC § 255 paragraph one provides that the court can grant the § 254 injunctions if it is satisfied that the plaintiff's claim is *prima facie* and there is 'a sufficient ground for applying the protective measures'. CIPC § 255 paragraph one (2) stipulates:

"The court shall grant any application filed under Section 254, when it is satisfied that the complaint is *prima facie* and that it has a **sufficient ground** for implementing the protective measures requested according to the following rules:

…

(2) In case of an application for any order provided in section 254(2), the court must be satisfied that:

(a) The defendant intends to repeat or continue the wrongful act, the breach of contract or the conduct complained of,

(b) The plaintiff will henceforward sustain suffering or damage because of the defendant's act,

(c) The property in dispute or the defendant's property is in circumstances to be wasted, injured or transferred, or

(d) There is any ground provided in (1) (a) or (b);

... " [**Emphasis** in bold added]

The *prima facie* factor does not apply here because the CA 2015 motion is brought prior to the main infringement claim. The 'sufficient ground' factor accords with the following guidance: - CIPC § 255 provides that each type of injunctions under CIPC § 254 (1) - (4) must accordingly satisfy each condition under CIPC § 255 (1) - (4). For example, the CIPC § 254 (1) injunction -- seizure of the property in dispute-- can be guaranteed by the circumstantial evidence prescribed in CIPC § 255 (1) that the defendant intends to

remove, transfer or sell the property in order to delay or obstruct the future execution of the court decision. CIPC § 255 (2) (a) and (b) provides conditions to restrain a repeat of the illegal act and hence to ensure a discontinuation of plaintiff loss.

The 'sufficient ground' is satisfactory if a defendant intends to repeat or continue the infringement or if the plaintiff's damage continues because of the defendant's act. The CIPC § 254 'sufficient ground' term can be interpreted in the same fashion as CA 2015 § 32/3 'necessary' term. Indeed, the Thai Supreme Court has used the term 'necessary' in place of 'sufficient' in a breach of contract case.

In Supreme Court case no. 1868/B.E.2548 (2005), a plaintiff Bank of Ayuthaya Plc., Ltd. filed an eviction lawsuit against C. Co., Ltd. and other defendants on the ground that the defendants broke the letting contract by sub-renting the building to others without the plaintiff's permission. During the trial, the plaintiff motioned for a preliminary injunction to forbid defendants from sub-renting the premises until the court rendered its decision. The court granted the requested injunction. It ruled that the order prohibiting defendants, as requested, was of 'necessary' extent to protect the plaintiff from damage incurred by the repeat breach of contract under CIPC § 254(2) and 255.

The Supreme Court directly applied the term 'sufficient' as prescribed in CIPC § 255 paragraph one. In so doing, it used the word 'necessary' instead of 'sufficient'. This case is not the only case where the Supreme Court interchanged the two terms. Case no.1868/B.E. 2548 (2005) used the 'necessary' term in certifying the injunction where it was proved that the defendants continued in breach of contract. This case applies the term 'necessary' to both circumstances and injunctive extent. In another case along these lines, Supreme Court case no.704/B.E.2545 (2003), the Court also used 'sufficient' and 'necessary' in slightly different circumstances.

In Supreme Court case no.704/B.E.2545 (2003), plaintiffs had contracted to buy land from defendants no.1-20 but they did not yet transfer the land with the registrar. The plaintiffs advanced that defendants no.1-20 fraudulently sold and registered the land to defendant no.21. During the trial the plaintiffs moved for a motion to prevent defendant no.21 from transferring the land to a third party. The Court entertained the plaintiffs' motion. As the plaintiffs claimed that the land was sold to them and requested for its transfer, defendant no.21 would damage the request if he transferred the land to a third party, in which case had the plaintiffs won the case, they would not have been able to

obtain the land; therefore, the court ruled that "it is necessary, sufficient and reasonable that the plaintiffs' request for the injunction under CIPC § 254(2) and 255 (2) be granted in order to prohibit defendant no. 21 from transferring the land under dispute to a third party until the court ordered otherwise".

The Court used both 'necessary' and 'sufficient' in its justification. These two cases indicate interchangeability between the two terms. Although the 1868/B.E.2548 and 704/B.E.2545 cases applied CIPC § 254(2) and 255 in a contract default case, there would be no difference if it were a tort case. In 1868/B.E.2548, had the defendants without the let contract tortuously trespassed the premise, the Court would have ruled that the injunction was 'necessary' to stop the continued wrongful trespass. An intellectual property infringement is a kind of tort which can be subject to the same ruling. Here below, the Supreme Court applied CIPC § 254(2) and 255 in intellectual property cases.

In Supreme Court case no.3740/B.E.2549 (2006), plaintiffs, P. Co., Ltd. and others, brought a case against the Department of Intellectual Property (DIP) to the Central Court of Intellectual Property and International Trade (CIPIT). The plaintiffs urged the court to withhold a design patent issued to the third party, D. Co., Ltd. It was argued that the patent was erroneously issued. The plaintiffs motioned for an interlocutory injunction under CIPC § 254(2). The motion was aimed at obtaining court permission to allow them to legally produce, distribute and use the product under the D. Co., Ltd.'s patent. In denying the motion, the Supreme Court held that the injunction under CIPC § 254 (2) applied to prevent a defendant from damaging plaintiff's interests whilst the trial was in progress. The injunction, however, did not apply when the person who caused such damage or affliction was a third party. The injunction could not be granted to influence the third party, D. Co., Ltd., who did not contest in the case. D. Co., Ltd. was the patent holder who had exclusive rights to its patent. The Court did not grant any permission that conflicted with such rights conferred by the law. The permission requested was not the injunction prescribed in the Act Establishing the Intellectual Property and International Trade Court B.E.2539 (1996) § 26 and the CIPC § 254 (2).[54]

[54] Supreme Court case no.873/2544 is another patent case which had essentially the same factual pattern. The Court held that the petitioner could not request for an injunction which prohibited the defendant from proceeding with the criminal action which he had already initiated.

According to the above ruling, it is clear that CIPC § 254 (2) is a provision that applies to intellectual property infringement. The CIPC § 254 (2) and CA 32/3 injunction aims at stopping the defendant's on-going contract default or tort, in effect, alleviating the plaintiff's on-going damage. It is true that Supreme Court case nos. 1868/B.E.2548, 704/B.E.2545 and 3740/B.E.2549 came before the CA 2015 enactment. However, these cases are positive precedents as there is no definition of 'necessary' provided by the law.

In copyright infringement cases, the 'necessary' ground is established if an infringer intends to repeat the infringement or continue to breach a licensing contract; or if there is a continuation of the right holder's damage. In online copyright infringement, continual availability of content over the internet is the repeat or continued breach of copyright. Uploading client/server users expose the content to reproduction, adaptation and distribution without time limit; hence, indicating intention of the users in continuing the infringement.[55] This infringement continually damages right holder's legitimate copyright and it would be unabated if nothing was done about it. This situation warrants the 'sufficient' cause and a court order is then 'necessary' to protect copyright through the prohibition of the online infringement.

In conclusion, the 'necessity' is to be interpreted in the same tradition as 'sufficiency'. Moreover, such interpretation also suggests that the terms 'sufficient' and 'necessary' cover likewise gravity of circumstance as well as scope of injunction. The 'necessary' factor signifies the circumstances whereas such circumstances demarcate the extent of injunction. Supreme Court precedents permit this conclusion even if the 'necessary' term is not stated in CIPC §255 but it is used to replace the 'sufficient' term stated therein.

The next question though is what kind of measures fit the online copyright infringement and how such a measure justifies the 'reasonable' threshold. These issues are discussed below.

[55]Actual access is not prerequisite under Thai court precedence. (*See* chapter 3: 3.2.1 Can Client/Server and Peer-to-Peer User Activities be Primary Infringement and What Are the Exclusive Rights Affected?)

4.3.3 What Constitutes a 'Reasonable' Court Order for Online Copyright Protection?

'Necessary' is not the only word the court used to adjudicate to the motion; 'reasonableness' is another word in CA 2015. The language of CA 2015 § 32/3 paragraph four seems to invite ambiguity as to the interpretation of 'reasonable'. Does it focus on circumstances, measures, or both?[56] This section examines the answer. It discusses the circumstances under which the court injunction is warranted and how the court finds if the requested measure is 'reasonable', and in which way, e.g., proportionality, cost effectiveness or ISP burden. As will be seen below, the Supreme Court reasoning seems to mix 'sufficiency' and 'necessity' with 'reasonableness' in examining the requested injunction.

In Supreme Court case no.704/B.E.2545 (2002) above, the court ruled that "it is necessary, sufficient and reasonable that the plaintiffs' request for the injunction under CIPC § 254(2) and 255 (2) be granted in order to prohibit defendant no. 21 from transferring the land under dispute to a third party until the court ordered otherwise". The Court incorporated 'necessary', 'sufficient' and 'reasonable' in the same judgement. It did not clearly differentiate that the circumstance was 'necessary' to protect the plaintiff's interest (the land transfer); and that the transfer prohibition injunction under CIPC § 254(2) ("not to […] sell or transfer the property in dispute until the court orders otherwise") was a 'reasonable' measure to achieve the goal. The decision blurs the intended clarity of terminology.

It can be inferred from the ruling of the case no.704/B.E.2545 that when circumstance satisfies the 'sufficient' condition and necessitates the prohibition of the defendant's act, the Supreme Court will grant the injunction by reasoning that the injunction is 'reasonable'. On the contrary, if the 'sufficient' ground is disproved or the injunction is not necessary, the Supreme Court will refuse the motion by holding that it is not 'reasonable' to grant the injunction.

In Supreme Court case no.1415/2499 (1956), a plaintiff requested to have a property attached. The property was the same as the property that had been attached in the previous case of which the two parties were the same in both cases. The Court

[56] CA 2015 § 32/3 paragraph four: "[…] If it [the court] finds that […] there is a necessary ground and reasonable to grant the requested order, it shall impose upon service providers to cease the alleged infringing acts, or to remove alleged infringing work from the service provider's system, […]"

refused to grant the attachment injunction by declaring that such an injunction was not 'reasonable'.

There are many other occasions where the Supreme Court used the term 'reasonable' as its justification for the term 'sufficient' under CIPC § 255(2).[57] Case no. 1868/B.E.2548 above also used the term 'necessary' as the tool to examine the extent of the injunction. The three terms rely on each other. Therefore, it can be concluded that the term 'reasonable' applies likewise to circumstances as it does to measures. It has wide array in that even though it is 'necessary', the court can negate the order. If granted, the order can be a type of injunction as provided by the law.

The court has two options when granting the order: to remove the material from the ISP system and to cease the infringement by other means.[58] The order to remove material is easily comprehensible. For client/server technology, the court can impose upon IHP and ICP service providers 'to remove alleged infringing work from the service providers' system'.[59] However, the order to 'cease the infringement' is not easily comprehensible. There is no definition or guidance as to what characterises 'ceasing the infringing acts'.[60] The term seems to accommodate all requested applications whether or not they target the supply (business operators) or the demand (users) side, or commercial or private use, or intentional or unintentional infringement. It follows that the court can instruct extensive orders, e.g., access disabling, traffic shaping or bandwidth shaping, website blocking (IP Address, URL), as well as content identification and filtering[61], provided that these approaches lead to "the cessation of the alleged infringing acts". The phrase 'cease the infringing acts' can benefit and damage Thailand copyright protection.

---

[57] For example, Supreme Court case nos. 2149/B.E.2516, 970/2519, 2574/2519, 1479/2520, 6/2534, 1343/2538, 1714/2539, 5294/2540, 753/2541, 4746/2541, 9028/2542, 7221/2544, 704/2545, 5273/2546, 7024/2546 and 1366/2553.

[58] CA 2015 § 32/3 paragraph four

[59] CA 2015 § 32/3 paragraph four

[60] Without guidance, litigants and the court seem to navigate into an uncharted sea. Among questions raised are: To what extent can a right owner request and the court permit; Can the order deter the infringement partly, not completely, or could it be gradually, not completely; What if the order places too much of a burden on an ISP; What if it is overly complicated and staggered (e.g., Graduated Response); What if it has an adverse effect on ISP expenses and free and fair competition; Can the court take these factors into consideration and refuse some or all of the requests. Regarding the discussion of a measure involving with P2P, *see* chapter 5 -- 5.3.2 Specific Characteristics of Reasonable Measure in P2P Circumstances.

[61] *See* available measures in chapter 2: Technological Aspects of Protection of Copyright on the Internet: 2.3. Legal Copyright Enforcement Techniques and Measures.

The court may interpret 'to cease the infringement' narrowly or widely on a case by case basis. Website blocking and access disabling is discussed below as method examples of the order to cease the infringement.

4.3.3.1 Website blocking and Disabling Access to Content

If the phrase 'cease the infringing acts' is interpreted narrowly, it is not clear whether the blocking and disabling methods are of the 'cessation' injunctions which is available to the court to order. 'To cease the infringing acts' could literally mean to stop the act which may be different from website blocking and content access disabling. Under Section 27-30 of CA 1994, infringing acts are essentially reproduction, adaptation and communication to the public.[62] To cease the infringing acts is to stop reproduction, adaptation and communication. A wrongdoer reproduces, adapts and communicates to the public when he posts a material on a public website.[63] Website blocking and content access disabling cannot stop reproduction and adaptation because those acts are already completed. It merely prevents users in Thailand from logging onto the site but the infringing act does not actually stop. For example, Facebook can be blocked to Thai people while Singaporean or other countries' networks can still use it.[64] The same is true with the access disabling. The material posted still resides in the website but users are disabled from access to it. However, cessation can restrict on-going communication to the public. Other users are barred from viewing. Therefore, the narrow interpretation of *to cease infringing acts* should encompass only the infringing act of communication to the public.

If the phrase 'cease the infringing acts' is given a wider interpretation, it can mean inhibition of any reproduction and adaptation by anyone. It can certainly mean the stopping of any communication to the public by the poster. When the phrase 'cease the infringing acts' is to be executed by ISP operations, it is likely that the connotation is to stop the 'on-going availability of the material' as it is impossible to stop the infringement at the moment of initial reproduction/adaptation such as in a bricks and mortar tradition.

---

[62] *See* chapter 3: 3.2.1 Can Client/Server and Peer-to-Peer User Activities be Primary Infringement and What Are the Exclusive Rights Affected? *and* chapter 2: 2.2 Current Trends in the Field of Digital Infringement.

[63] *Ibid.*

[64] Many other websites were blocked during the recent military coup in Thailand. (Sakawee, S., 2014. "Thailand's coup spreads from streets to the web, 219 sites blocked so far." [Online] Available at: https://www.techinasia.com/thailands-coup-spreads-streets-web-219-sites-blocked/ [Accessed: 24 Aug. 2015])

As the material is publicly viewable, the reproduction, adaptation and communication to the public persist because members of the public reproduce, adapt and view the work on their devices when they click to watch the content.[65] Indeed, this widest sense of interpretation serves the purpose of the law to deter infringement on the internet. The right holders need to stop impermissible public viewing. Moreover, CA2015 Section 33/2 paragraph three (6) states that a motioning party may request the cessation of the infringement 'by other methods'. Even though 'by other methods' is not clearly provided in paragraph four for the court to order, the paragraph infers that any 'method' can be granted if it ceases the infringing acts.

Access disabling can be done in at least two ways-- (1) access to specific content in a server or website and (2) access to the website itself.

Disabling access to the specific content is similar to N&T in that instead of removing the content from a system, an ICP and IHP disable the access to such content. The difference is that with access disabled the content is still in the server and/or can be accessed in different part of the world, e.g., Thailand King *lèse-majesté* content can be viewed in other countries but not in Thailand. Content removal completely deletes the content from the server; hence, no access is left available at all. Disabling an access to allegedly infringing content in effect prohibits the content from being viewed. Therefore, the measure is likely to be found 'reasonable'.

As regards website blocking, IAPs can block domestic users from accessing banned websites residing abroad. For example, on one occasion the Thai authorities blocked access to YouTube when the website refused to withdraw a film showing graffiti over the Thailand King's face.[66] *Lèse-majesté*[67] is considered a serious criminal charge so that the Minister of Information and Communication Technology banned the site. The ban occurred after issuance of the Office of the Council of State's opinion that an ISP can be

[65] For a discussion of digital infringement of the rights to reproduction, adaptation and communication to the public, *see* chapter 3 -- 3.2 Can Client/Server and Peer-to-Peer User Activities be Classed as Civil Offences under Copyright Act B.E.2537 (1994)?

[66] BBC, 2007. "Thailand blocks access to YouTube". [Online] Available at: http://news.bbc.co.uk/1/hi/world/asia-pacific/6528303.stm [Accessed: 17 February 2015]

[67] The insulting of a monarch or other ruler; treason. (Translation from Oxford Dictionary website at http://www.oxforddictionaries.com/definition/american_english/l%C3%A8se-majest%C3%A9)

prosecuted as an accomplice if it declines to block an illegal website.[68] There was no attempt to criminalise the declining website, YouTube. This may indicate a difference between black letter law and practice. With regard to copyright infringement, it is unlikely that an ISP will be prosecuted because it refuses to block an infringing website.

Domestic IHPs can also block websites by disabling access to the websites they host. By doing this, IHPs inhibit users worldwide from accessing the website. Right holders can apply this request to the court arguing that this is one of the methods that can be utilized to cease infringement under CA 2015 § 32/3. The question is what constitutes infringing websites. The Singaporean law offers a good example of guidance involving website blocking factors.[69] Similar to Thailand, Singapore website blocking measures can be achieved through the court. Singapore is Thailand's neighbour country, in the same region.[70] Studying the system in brief is interesting and relevant.

Recently in 2014, Singapore introduced the website blocking mechanism to its Copyright (Amendment) Act. The law inserted a "flagrantly infringing online location" definition to mean "an online location which is determined by the High Court under Section 193DDA to have been or is being used to flagrantly commit or facilitate infringement of copyright in materials."[71] The High Court determines (1) whether the service provider is used to access the online location in question,[72] and (2) whether the location is flagrantly infringing.[73] In determining whether the location is flagrantly infringing, the Court shall take into account the factors provided by the law, such as, the primary purpose of the website, activities the website provides, or court orders from other countries. These factors are not exhaustive. The court is allowed to introduce other reasons why it prefers or declines to block, the website. The court discretion effectively helps the law to keep up to date in its operation and hence counter any future

---

[68] Thailand, Office of the Council of State, Opinion No.343/B.E.2549 (2006)[Thai] Available: http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=cmd&year=2549&lawPath=c2_0343_2549 [Accessed: 23 December 2012.] Thai government organizations such as ministries, bureaus or departments which consult the Office of the Council of State are bound by the Office's opinion under the cabinet resolution on the 28th February 2482 (B.E.) (1939).

[69] Singapore Copyright (Amendment) Act 2014 Section 193DDA (2)

[70] According to the Global Intellectual Property Center (GIPC) International IP Index 2014, Singapore is the best IP environment of Asia. (Available at: http://www.theglobalipcenter.com/charting-the-course-the-gipc-international-ip-index-2nd-edition/ [Accessed: 22 September 2014])

[71] Singapore Copyright (Amendment) Act 2014 Section 193A (1)

[72] Singapore Copyright (Amendment) Act 2014Section 193DDA (1)(a)

[73] Singapore Copyright (Amendment) Act 2014 Section 193DDA (1)(b)

evolvement of threats. The next question is whether website blocking can deter user infringement in client/server.

For client/server user deterrence, it must be said that blocking of websites is an extreme measure. Blocking usually targets the whole website, not a specific page or content.[74] Rights holders who wish to remove or disable access to such a page or content need to rely on the current N&T mechanism.[75] Indeed, a website, flagrantly infringing or not, can consist of all the uploaded end-user content uninitiated by the website operator. Website blocking and access disabling are optional measures in client/server user infringement. The measures limit the possible location for user content placement. A website is certainly a place where infringement has 'taken place' in the service provider's system. 'To cease the infringement' can be materialised by blocking the website or disabling its access. CA 2015, however, does not have factors for consideration such as Singapore's copyright law. It is left to the court to decide if the measures are necessary in the circumstances and that there are 'sufficient' grounds to show that a user intends to continue his infringement by leaving content on the internet and causing the right holder to suffer financially. Blocking produces a cessation of the infringement which is of the CA 2015 § 32/3 injunctions. Many factors seem to be satisfied. The question though is if it is

---

[74] Rajah S.C., I., n.d. "Supporting the Digital Environment: the Copyright (Amendment) Bill 2014 "[Online] Available at: http://www.scca.org.sg/images/resources/Announcements/SMS%20Note%20on%20Copyright%20Bill.pdf [Accessed: 5 June 2015]

[75] Singapore Copyright Act 2014 Section 193D provides safe harbours for storage ISPs. Section 193D stipulates:

"(1) The court shall not grant any monetary relief or, except as provided for in section 193DB, make any order against a network service provider for any infringement of copyright in any material that occurs by reason of

(a) the storage, at the direction of a user of the network service provider's primary network, of an electronic copy of the material on the primary network, if the network service provider satisfies the conditions referred to in subsection (2); or

…

(2) The conditions referred to in subsection (1)(a) are that

…

(b) if the network service provider

…

(iii) is furnished in the prescribed manner with a notice in, or substantially in accordance with, the prescribed form relating to the electronic copy of the material on the primary network

(A) purportedly made by the owner of the copyright in the material or under the owner's authority; and

(B) stating the prescribed matters, the network service provider expeditiously takes reasonable steps to remove or disable access to the copy of the material on the primary network; and

…"

'reasonable' to grant such an order. In a UGC website, such as YouTube or Facebook, the blocking of websites because of illegal posts can be disproportionate because it also refuses access to a large amount of legal content. Website blocking is an option for a court order but is likely to be found out of proportion and not reasonable.

In conclusion, the order can be granted if the court finds it 'necessary'. The word ‘necessary’ in CA 2015 can be of the same criterion as the word ‘sufficient ground’ in CIPC 1934 § 255. The order is issued to stop the defendant’s on-going infringement and relieve the plaintiff’s on-going damage. The ‘necessary’, ‘sufficient ground’ and ‘cease the infringement’ requirements are not all inclusive factors. The court has discretion to consider if the requested measures are ‘reasonable’. The terms ‘necessary’ and ‘sufficient’ incorporated with ‘reasonable’ criterion are the ground to examine whether the situation warrants the order and whether the extent of order is justifiable. However, with all these criteria, it is still hard to demarcate the magnitude of a court order 'to cease the infringement'. Unlike the Singapore Copyright Act, the Thailand court has no factors for consideration in laying down the extent of ‘cessation’ order. Proportionality can be one of the ‘reasonable’ considerations but not clearly. Website blocking or website access disabling may not be proportionate in end-user deterrence because it denies access to the whole website and all usable content as opposed to taking down specific content or acts. This aspect can be just one of other Thai CA 2015 § 32/3 constraints shown below.

4.3.4 Limitations of the Thailand CA 2015 § 32/3 Court Procedure and Remedy

The court judgement has to be obeyed or the disobeying party can be disciplined. This makes the court system more effective than the US’ N&T arrangement. Whether the court system is an efficient means is another question. From a practical point of view, it is argued that the CA 2015 § 32/3 court system is not suitable in current situations because of a number of limitations, described as follows:

First, there is a limitation with regard to case preparation. The last part of CA 2015 § 33/2 paragraph four stipulates that “the right holders shall file the lawsuit against infringers within the time designated by the court for such cessation or removal”. The right holders may need to prepare the main case at the same time or before they file the motion or they might not be able to bring the infringement case in the time designated. Having to prepare the main case would cause considerable delay to the constraint of the on-going infringing activities. Such a delay could be financially damaging to right holders.

In total there are two litigations, the first occasion being the motion under Section 32/3 and the second being the main case. These litigations incur considerable cost but may not yield a good return.

According to one Thai right holder, damage calculation is a problem.[76] Under CA 2015 § 32/3 paragraph three (5), right holders have to provide 'potential damage incurred by the alleged infringing acts'. It is not easy to calculate the damage, i.e., what is the financial damage cost of one song posted for free use? Or what is the financial damage cost resulting from a posted movie? Whether or not the infringing song and movie affect sales volumes and the blockbuster effect is also hard to determine.

There is a general rule that the court shall not grant anything that is not requested by a party.[77] The strict application is that if a right holder motions for access disabling only, the court cannot render an order for content removal. As a consequence, this rule invites litigants to make as many requests as possible in order to assure one or another court order. To determine all the requests can retard the trial progress. The more requests, the more time and resources for which relevant institutions must be compensated. Moreover, if it is proved that all the requests will result in the cessation of the infringing acts, then the court can award all the methods or only just one method which it characterises as more appropriate than all the others.

Secondly, a limitation is encountered during the court examination/hearing. CA 2015 § 33/2 paragraph four requires that "when the court receives the motion under the first paragraph, it shall hold an examination". The present situation is that internet infringement is so widespread throughout the world and the law does not seem to realise that if right holders decide to file every single internet case then the court will be bombarded with a large number of examinations, a situation which is virtually impossible to handle. On the other hand, for economic reasons, the number of cases might be small. Right holders wanting to sue an individual user are conceivably not able to guarantee proper redress. They are forced by the law to bring only strong, high impact cases to the

[76] Thailand, Electronic Transactions Development Agency (Public Organization) (ETDA), 2015. "ICT Law Center Forum: Open Forum for Public No. 3: How the Draft Copyright Act that has just been passed by National Legislative Assembly Benefits Digital Economy", (Seminar) [Thai] Available at: https://www.youtube.com/watch?v=Od3O9kVHSYc [Accessed: 23 June 2015].

[77] CIPC 1934 Section 142 paragraph one provides that "The court decree or order shall decide all claims in the complaint but it shall not decide or grant something beyond or not requested in the complaint…"

attention of the court, leaving the majority aside. It is not good for copyright protection to have either very large or very small numbers of cases. Such situations are unlikely to reduce the amount of user infringement.

On the surface, a court system offers a guarantee of justice because it gives equal chances of presentation to the competing parties. The CA 2015 § 32/3 court system is different. The information required by CA 2015 § 32/3 paragraph three does not include alleged direct infringer identity. This means that there cannot be a serving of the motion to the infringer and hence the infringer will not be able to enter into the motion hearing. The law does not give the infringer a rightful chance to defend himself. A plea of fair use or any other legitimate plea cannot be advanced at this stage.

A court applies the preponderance of evidence principle.[78] The principle requires a relatively high standard of proof in order to guarantee a court decision. The petitioner needs to prove whether the work is copyrighted and whether the use of the work is not licensed. This principle is too much of a requirement in online situations which could render it impractical to pursue all alleged infringers.

Thirdly, there is limitation in the court order. The language of CA 2015 § 32/3 such as 'necessary' and 'cease the infringement' seems to protect copyright only. Such expressions do not connote arguments against copyright. Fair use, freedom of speech and other fundamental rights are not given appropriate consideration. Such rights are not required factors for consideration. It can be argued that the motion hearing does not present a comprehensive infringement case where these arguments can be shown. As the law does not allow the alleged infringer to enter into the case, it is hardly possible that anyone can present these issues from an alleged infringer's point of view.[79] It can also be argued that the court has discretion to refuse the order if the motion is not 'reasonable'.[80] In other words, if the request conflicts with freedom of speech, the court is able to dismiss

[78] CIPC § 104 paragraph one stipulates: "The court has the whole authority to consider whether evidence delivered by parties relates to the facts in the case and is sufficient, and adjudicate accordingly"

[79] Although the court has authority to invite evidence on account of its own deliberations, this authority is rarely used. CIPC 1934 § 87(2) provides: "The court shall not admit evidence unless:

...

(2) The party who delivers the evidence follows the rules in Section 88 and 90, but if, in the interests of justice, the court deems it needs to hear important evidence which it admits in conflict with this subsection, the court has the authority to do so.

..."

[80] CA 2015 § 32/3 paragraph four

it because it is not 'reasonable'. However, the right to freedom of speech expression is not clearly provided; hence, not guaranteed by the ‘reasonable’ ruling.

The ‘reasonable’ and ‘cease the infringement’ criteria are in a legal area. There are other areas that need to be observed. Technical constraints, economic concerns and market competition are such areas. These areas are not currently a legal requirement for the court to contemplate. This is especially so if an ISP does not enter into the case to protect itself.[81] The right holder and the court may not know about an ISP's limitations. Information about an ISP’s functions and facilities is inherent to the ISP itself. For example, if a party makes a request for content identification or filtering, an ISP has to have the systems in place to do it. It may not be possible to fulfil such requests if the ISP does not have such systems. Even if it is realistically possible, the ISP may struggle to install those facilities. Some measures incur considerable cost and yet they prove to be ineffective because they can be easily circumvented. Some measures can be disproportionate. Website blocking will completely prevent the website from offering non-infringing services or content. The court can order measures that can cause difficulty for an ISP and restrict a legitimate user's right. From an economic perspective, the cost of investment needed by an ISP for compliance could severely jeopardize its free market competition. The general rule is that the court has to rely on the information provided by both parties.[82] The court cannot rely on evidence that the parties do not present in the hearing.[83] The decision is based solely on the facts delivered by the parties. The court may not grant appropriate measures if both parties are not present in court. As to litigation techniques, the party who has knowledge of information against his interests may still ignore it and does not have to disclose it in the hearing as the onus is on his opponent to present the information. Nevertheless, the court again has the 'reasonable' factor[84] to dismiss the motion if it finds that the request is impossible under the present ISP's facility. The law should indicate these areas as factors to consider in granting the court order.

---

[81] There are many reasons why the ISP may not want to be involved in the trial; *inter alia*, avoiding the cost of litigation, unwilling to disclose internal information because this might encroach on the ISP’s private trade information, competitive capacity, system completion, taxation, etc.

[82] CIPC 1934 § 87(1) provides: “The court shall not admit any evidence unless:
(1) The evidence relates to the facts in the case that a party must prove, and;
...”

[83] The court has discretion to admit evidence in addition to that presented by parties under CIPC 1934 § 86 paragraph three but it does not normally do.

[84] CA 2015 § 32/3 paragraph four

In conclusion, CA 2015 § 32/3 has limitations concerning the preparation of the motion, the court examinations process and the granting of the court order. The limitation prior to the motion is due to the legal requirement that the right holders have to bring the infringement case to the court within a time limit. The motion and the infringement case preparation must be accomplished at the same time which prolongs the motion process and in effect, delays copyright infringement deterrence. To configure the requested amount of potential damage is a problem as it is not easy to compute. It could be that the law unnecessarily invites weighty, comprehensive requests on the part of litigants as it is not easy to anticipate the methods and the extent of the methods granted. The second limitation encountered concerns the required court examination. The examination creates resource difficulties for the right holder. The number of cases brought is very likely to be small because many cases cannot yield an appropriate return. The examination is between a right holder and an ISP and does not have a direct infringer represented in the case. The court system standard of proof can be too high regarding the internet user's infringing circumstance. The third limitation concerns court order aspects other than legal aspects. Indeed, it is the legal aspect that is ambiguous as to whether it allows the court to consider other aspects when granting the order. An ISP's presence before the court can be helpful to the court in its application of the 'reasonable' criterion.

As is shown above, the drawbacks of the Thailand court system under CA 2015 § 32/3 do not encourage a right holder to use it. In comparison with the US, the US right holders use their system more. The effectiveness of the US N&T function can be shown by the large number of notices sent to ISPs.[85] A large number of motions to the court is very unlikely in the system of Thailand. The above objects of comparison, where relevant, will be presented in the next section.

4.4. Functionality of the US Notice and Takedown

In comparison with the Thai system, this section will demonstrate some aspects of the US N&T system functionality. Firstly, as in Thailand, website hosts (IHPs) and websites (ICPs) play a key role; thus, targeted by a right holder in client/server. This section will explain if the US IHPs and ICPs play the same role and are the target of right holder’s

[85] *See* 4.4.2.1 Voluminous Notices Issued below.

notification. Secondly, in order to compare efficacy, the next section will also show the limitations of N&T. A comparison will be made at the end of this chapter.

4.4.1 Legal Definitions of Internet Service Providers (ISPs) for the purposes of Notice and Takedown Procedures

With respect to client/server technology, the question is whether 'Information Residing on Systems' under 17 U.S.C. § 512(c) covers both websites themselves (ICPs) and website hosting services (IHPs). 'Service Provider' is defined by 17 U.S.C. § 512 (k) (1) (B) as follows:

''(B) As used in this section, other than subsection (a), the term 'service provider' means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)."

The case of *Perfect 10, Inc. v. Ccbill Llc*[86] is used to illustrate the issue of how an ISP is defined and the types of service provider. In this case, CWIE, one of the defendants, hosts websites and provides necessary internet connectivity services to the owners of various websites. It monitors the operation and power of the "box" or server, as well as its connection to the internet. The Circuit Court did not discuss the issue directly, namely, that CWIE, by providing website hosting service, is a 'service provider' under § 512 (c). However, it ultimately determined that CWIE is entitled to § 512 (c) limitation if CWIE does not gain monetary benefit directly from the website infringement. Therefore, it could be said that the entities that provide cyber space to websites are protected by safe harbour because they are an information residing on systems at direction of users who are, in this case, the website owners under § 512 (c).

Another question is if a website is an ISP that can be subject to notification. User-generated content (UGC) websites or applications such as YouTube, Facebook, Instagram are the important platforms within client/server technology. The websites allow users to upload their own created content to the websites. The content can be infringing where a right owner can seek to stop the public viewing it. In *UMG Recording, Inc. v. Shelter Capital Partners LLC*,[87] Veoh Networks (Veoh), very much like YouTube, runs a website

[86] 488 F. 3d 1102 (9th Cir. 2007)
[87] 718 F. 3d 1006 (9th Cir. 2013)

where users can furnish and share their videos to other users publicly.[88] Over the internet, users can view videos other users uploaded. Veoh gains revenue from advertisements viewed along with the videos.[89] The court 'assume[d] without deciding that Veoh qualifies as a "service provider" because UMG does not contend otherwise.'[90] The question was whether Veoh met a requirement to receive safe harbour protection. 17 U.S.C. § 512 (c) (1) stipulates:

> "(c) Information residing on systems or networks at direction of users.—
>
> (1) In general.—A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason *of the storage at the direction of a user* of material that resides on a system or network controlled or operated by or for the service provider, if the service provider…" [*Emphasis* added]

17 U.S.C. Section 512 (c) requires that the material stored on the service has to be furnished by users. Veoh's system provided storage for users' uploaded videos and access to them.[91] UMG argued that because Veoh not merely provided storage, it also facilitated access to the stored content. It is the latter facility that excludes Veoh from exemption. The Circuit court agreed with the district court that UMG interpreted the phrase "by reason of the storage at the direction of the user" too narrowly. It explained that the phrase 'clearly meant to cover more than mere electronic storage lockers'.[92] It ruled:

"[T]he language and structure of the statute, as well as the legislative intent that motivated its enactment, clarify that § 512 (c) encompasses the access-facilitating processes that automatically occur when a user uploads a video to Veoh."[93]

---

[88] *UMG Recording, Inc. v. Shelter Capital Partners LLC,* 718 F. 3d 1006, 1011 (9th Cir. 2013)

[89] *Ibid*.

[90] *Ibid.,* footnote 4.

[91] It is worth noting that Veoh has developed filters that identify the same infringing material where the material cannot be re-uploaded or accessed if it is recorded as infringing. (*UMG Recording, Inc. v. Shelter Capital Partners LLC*, 718 F. 3d 1006, 1012-13 (9th Cir. 2013)) The filters can be the supplementary measure which compensates N&T failure as described in 4.4.2.1. Voluminous Notices Issued below. (*See* recommendation in chapter 6.)

[92] *UMG Recording, Inc. v. Shelter Capital Partners LLC,* 718 F. 3d 1006, 1016 (9th Cir. 2013)

[93] *Ibid*.

The *Shelter* decision shows that websites that permit user's storage of content and facilitate access to such content are service providers or 'Information Residing on Systems or Networks at Direction of Users' under 17 U.S.C. § 512 (c).

The question whether web-hosting services or websites are the service providers under 17 U.S.C. § 512 (c) is not directly answered by the court. One reason might be because it is clear enough that both entities store content at the direction of users; thus no controversy. The other way to find a clearer answer is through the court precedents clarifying differences between 'Transitory Digital Network Communications' (mere conduit) and 'Information Residing on Systems'. The case law addresses the issue when it rules which kind of service providers are responsible for their users' identity disclosures. In essence, the service providers that simply transmit information have no obligation to reveal the identity of subscribers; it is those that store users' information that are obligated to do so.[94] The following case discussed the issue in detail.

Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C.Cir.2003) was the first case whereby the Record Industry Association of America (RIAA) attempted to serve a subpoena on internet service provider, Verizon Internet Service Inc., pursuant to the 17 U.S.C. § 512(h)(1).[95] RIAA sought to "identify an ISP subscriber whom it believed was infringing its members' copyrights by trading large numbers of digital .mp3 files of copyrighted music via 'peer-to-peer' (P2P) file sharing programs."[96] When Verizon refused to disclose its subscriber, RIAA applied for a motion to compel production.[97] The U.S. District of Columbia granted the motion. Verizon appealed. In deciding the case, the D.C. Court of Appeals first indicated that in order to request for the identity, a right holder needs to supply the clerk of the court with sufficient

---

[94] 17 U.S.C. § 512 (h) "Subpoena to Identify Infringer" sets forth:
"…[A] copyright owner… may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer […]. The request may be made by filing with the clerk …a copy of a notification described in subsection (c)(3)(A). […] The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner […] information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider. […] If the notification filed satisfies the provisions of subsection (c)(3)(A), […], the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider."

[95] *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, Inc.,* 351 F.3d 1229, 1229 (D.C.Cir.2003)

[96] *Ibid.*

[97] *Ibid.*

documentation.[98] One of the requisites is a copy of the notification described in subsection (c)(3)(A)(iii) which sets forth that a notification of claimed infringement must include identification of the material that is claimed to be infringing. The infringing material needs identification to enable its removal or the disabling of access to it.[99] Most importantly, the identifying information has to be sufficient to permit the service provider to locate the material.[100] However, RIAA's notice was disqualified as a valid notice. The notice did show the infringing material, but it did not sufficiently show the material's location for purpose of content removal or access disabling. The court explicated that the insufficiency was due to the P2P platform which hosted RIAA's works in individuals' computers, not in the ISP's server. Neither the right holder nor the ISP could possibly be able to locate exactly where the content came from. Moreover, even if content location identification were possible, an ISP could not remove the content, nor could ISPs disable access to users' computers because they had no right or ability to control such facilities. RIAA argued that even though ISPs could not disable access to the users' content, it could disconnect infringer access to the internet. The court held that such a disconnection request is invalidated by the statute because 17 U.S.C. § 512(c)(1)(C) allows ISPs to remove or disable access by others to the infringing material resident on the subscriber's computer, not to terminate a subscriber's account.[101]

Therefore, the court 'held that under the DMCA, a subpoena may be issued only to an ISP engaged in storing on its server material that is infringing or the subject of infringing activity'. The subpoena cannot be issued to an ISP acting only as a conduit for data transferred between two internet users, and so a subpoena may not be issued to an ISP acting as a conduit for P2P file sharing, which does not involve the storage of infringing material on the ISP's server.'[102]

---

[98] 17 U.S.C. § 512(h)(2)(A)

[99] 17 U.S.C. § 512(c)(3)(A)(iii)

[100] 17 U.S.C. § 512(c)(3)(A)(iii)

[101] *Recording Indus. v. Verizon*, 351 F.3d, 1235.

[102] *Ibid.* This case creates precedent which other courts from different circuits follow such as *In re: Charter Communication, Inc.*, 393 F.3d 771 (8th Cir. 2005), *Interscope Records v. Does*, 494 F.Supp.2d 388 (E.D. Va. 2007) and *Well Go USA, Inc. v. Unkown participants in filesharing swarm identified by Hash*, WL 4387420 (S.D.Tex. 2012).

This case has the following implications. Many service providers have multiple functions.[103] However, the law defines 'Information Residing on systems' to cover mere conduit. Section 512 (k) (1) (B) sets forth service providers as used in Section 512, other than subsection (a) ('Transitory Digital Network Communications' or mere conduit), to include an entity described in subsection (A). A service provider can fall into one or many ISP categories under 17 U.S.C. § 512. It is clear from *Verizon* that the definition of a service provider is determined by the acting of the role in question and not by roles it might otherwise perform. In other words, the law intends to create exceptions by 'types of ISP's activity', not by 'types of service providers' as such.[104] Indeed, Verizon serves both information transmission and content hosting.[105] It is the transmission that Verizon served in P2P file sharing which saved it from being regarded as 'Information Residing on Systems'.

In comparison between different ISP functions (or types) featured in the protection measures, the US principle is the same as that of Thailand. IAPs or 'Transitory Digital Network Communications' are not subject to a court order to remove or take down the infringing content. If the IAP hosts websites, IAPs then become IHPs. The IHPs and ICPs of Thailand, or 'Information Residing on Systems' of the US, can be exposed to a court order or a notice. The ISP different functions and classification are both a legal and technical matters. In practice, a litigant needs to understand these matters otherwise it affects his case. Litigants of both Thailand and the US have to be precise as to what court order/injunction they need. The litigants also need to target the correct type of ISP. In cases where ISPs have multiple functions, the litigant needs to stipulate clearly in the request which function the ISP performs in keeping with the injunctive request. However, a right holder who files a notice to the correct ISP may find the N&T system problematic for a current digital infringement situation. The next section will demonstrate N&T limitations.

---

[103] *See* 4.5.1 Types of Service Providers Receiving Notification and their Safe Harbours below.

[104] Opinion of Advocate General JÄÄSKINEN delivered on 9 December 2010 (1) Case C-324/09 *L'Oréal v. eBay* paragraph 147 Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=83750&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=420842#Footref33 [Accessed: 10 October 2014] [Emphasis original]

[105] Record of live chatting with Verizon's agent through "Chat Now" on Verizon website at: http://www.verizon.com/smallbusiness/fiosInternetOverview.jsp?smbReferenceValue=SMBFIOSInternetPackageRef [conducted on 24 Oct 2014 at 14:45-14:51 (UK time)]

4.4.2. Limitations of Notice and Takedown

N&T has been in existence in the US and other countries such as EU countries for more than 15 years. [106] The scenario that was faced in the 1990s could be solved using N&T. However, new types of infringement now exist for which there does not appear to be adequate legal protection. Technology allows reproduction of works and makes posting much easier than in the past. It makes a large amount of internet copyright violation possible. This section considers limitations regarding the application of N&T.

4.4.2.1. Voluminous Notices Issued

The large volume of notices arises, for the most part, on account of the reappearance of the same infringing content.[107] Even so, there is no actual concrete evidence to show that the reappearance is the same infringing content. Right owners and telecommunication industries all accept the statistics as proof of the large number of notices.[108] "[F]or the six-month period ending last August[2013], member companies of the Motion Picture Association of America sent takedown notices for nearly 12 million files to search engines, and over 13 million directly to site operators."[109] This could be proof of either the system's effectiveness or ineffectiveness.[110] It is effective because right owners are interested in using the system, implying that the system works well. It is ineffective because notices were extremely excessive, suggesting that the current system does not deter infringement. From the right holders' perspective, the great quantity of notices certainly indicates that infringement on the internet is very widespread. This creates problems for right holders, ISPs and the public alike. Right holders' resources are stretched to produce notices while succeeding in the removal of only one location seems to be irreparable.[111] This could also be a problem for ISP resources. The cost borne by

---

[106] In EU via Directive 2000/31/EC of the European Parliament and of the Council on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (E-Commerce Directive))

[107] US House of Representatives, the Committee on the Judiciary, Subcommittee on Courts, Intellectual Property and the Internet, 2014. *Hearing 113th second session*, [Online] p.4-5. Available at: http://judiciary.house.gov/_cache/files/22c3acda-551c-41ba-b330-8dd251dd15fd/113-86-87151.pdf [Accessed: 10 November 2014]

[108] *Ibid*, p.4.

[109] Boyden, *op.cit*.

[110] US House of Representatives, *op.cit*., p.4.

[111] In *Cindy Lee Garcia v. Google, Inc.*, Slip. Op. No. 12–57302, p.17 (9th Cir. 2014), Google asserted that the content was so widespread that removing it from YouTube would have no effect.

artists and ISPs will no doubt be passed on to the public. These problems need a solution if digital copyright is to be honoured.

4.4.2.2 Does a Notice and Takedown System Adequately Protect P2P?

P2P technology did not exist at the time N&T emerged. P2P employs technology which gives rise to another type of infringement. The unique decentralized P2P characteristic makes it impossible to shut down the system "either by order of a court or technologically, unless the client P2P software is removed from each and every file trader's computer".[112] This characteristic means that P2P is at present beyond the reach of the N&T system which relies on information storage servers. So how can the US' N&T be used to protect P2P infringement?

DMCA has been used by right holders in two ways. Firstly, right holders sued the services and websites that engaged in third parties file exchange through the use of P2P protocol.[113] Secondly, right holders filed cases against ISPs to disclose P2P user's identification in order to later pursue a case against the users.[114] Apart from these means, N&T does not offer any legal measure that can be used for infringement deterrence within P2P technology.

When N&T is applied to P2P indexing services, it can only be done with the centralised indexing server, not the localised and distributed index.[115] For the localised and distributed index, it is not possible to send a notice to all users in a swarm. For the centralised server, a notice which includes a list shown on the indexing servers does not constitute a valid notice under DMCA § 512 (c). In *Perfect 10, Inc. v. Giganews, Inc.*, a notice that points to the results of a search performed on a specific date at a specific time

---

[112] The U.S. Congressional Record Vol. 148-Part 11: Proceedings and Debates of the 107th, Second Session, 2002 Available at: https://www.congress.gov/crec/2002/07/25/CREC-2002-07-25-bk2.pdf [Accessed: 2 June 2015] p.E1395.

[113] *See,* e.g., *Metro–Goldwyn–Mayer Studios, Inc. v. Grokster, Ltd*., 545 U.S. 913, *A & M Records v. Napster, Inc.*, 239 F.3d 1004 (9th Cir.2001) and *Columbia Pictures Industries, Inc., et al. v. Gary Fung, et al*., Case No. 10-55946 (9th Cir. 2013).

[114] *See*, e.g., *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, Inc.,* 351 F.3d 1229 (D.C.Cir.2003) This case creates a precedent which other courts from different circuits follow such as *In re: Charter Communication, Inc.*, 393 F.3d 771 (8th Cir. 2005), *Interscope Records v. Does*, 494 F.Supp.2d 388 (E.D. Va. 2007) and *Well Go USA, Inc. v. Unkown participants in filesharing swarm identified by Hash*, WL 4387420 (S.D.Tex. 2012).

[115] Napster is the classic example of the indexing server. (Buford, J.F., Yu, H. & Lua, E.K. 2009, "Chapter 7 - Search" in: J.F. Buford, H. Yu & E.K. Lua, Morgan Kaufmann, eds. *P2P Networking and Applications*. Boston, 2009, p. 164.)

on a specific newsreader, and attaching thumbnail images and screen shots did not amount to identification of the infringing material under § 512(c)(3)(A)(iii).[116] The list as such is not of infringing materials nor can each item on the list. The list and directories are merely the link to the potential infringing item. The notice that indicates the P2P file-searching results and asks the searching tools to take down the result is thus not identification of infringing material by the *Perfect 10* rule.[117] Indeed, N&T evidently only offers a means of protection from infringement other than P2P file sharing.[118] In addition, P2P applications do not fall under any of the four categories to which DMCA safe harbours apply.[119] Before being entitled to safe harbours, an ISP needs to have a policy about the termination of subscribers who are repeat infringers. The policy does not work with the P2P infringers. The following section explains reasons.

4.4.2.3 Policy towards the Termination of Repeat Subscribers and Account Holders

To be eligible for immunity, an ISP has to fulfil certain conditions. Section 512(i)(1)(A) stipulates:

An ISP "adopts and reasonably implements, and informs subscribers and account holders of the service provider's system or network of, *a policy* that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers." [Emphasis added]

An ISP is required to adopt, implement and inform its subscribers of a policy about N&T procedure and about termination of repeating infringers' accounts. The language of § 512 (i)(1)(A) may give the impression that 'the policy' is that if an internet access subscriber is a repeatedly infringing person, his internet access can be terminated by the IAP. As N&T procedure is only applicable to ICPs and IHPs, the 'policy' under this Section does not apply to IAPs.[120] "A conduit ISP is not required to have in place these notice and

---

[116] 993 F.Supp.2d 1192, 1200

[117] The information location tools under § 512 (d) are the kind of ISPs that can encompass P2P torrent websites. (*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020 (9th Cir. 2013). But study of the information location tool ISPs are not within the remit of this thesis.

[118] *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, Inc*., 351 F.3d 1229, 1236 (D.C.Cir.2003)

[119] Helman, L.2010. "Pull Too Hard and the Rope May Break: On the Secondary Liability of Technology Providers for Copyright Infringement." *Texas Intellectual Property Law Journal*. 19, 111, p.134 [Internal Citation omitted]

[120] Examples of policy can be found in various ICP's website, e.g., Social Science Research Network (SSRN) at http://www.ssrn.com/en/index.cfm/dmca-notice-policy/

takedown policies because it does not store material and, therefore, cannot be required to remove it."[121] IAPs cannot disconnect their subscriber's accounts if such accounts have been used in online infringement. Section 512(i)(1)(A) is not relevant to P2P application. A subscriber means a website's subscriber[122] or a website-hosting's subscriber[123]. Section 512 Legislative history and the courts make it clear that ICPs and IHPs are service providers that practice the policy.[124] Courts have interpreted the policy as a valid N&T system.[125] Implementation of the policy is merely to have the N&T system in place.[126] Therefore, the policy cannot be the ground for an IAP to disconnect P2P subscribers from internet access.

The limitations described above are known by the US. The problem of voluminous notices is being dealt with by the US Congress. The next section shows how the US Congress is making progress towards solving the problem. It also shows the solution to P2P infringement elsewhere.

4.4.3 Proposed Solution to Notice and Takedown Limitations

Recently, there has been an attempt to improve the 17 U.S.C. N&T system by the US Congress. The focal point directed is to reduce the amount of notification. In doing so, it is proposed that a notification should not only take down an allegedly violating content, but should also stay down the content. Moreover, the proposed 17 U.S.C. amendment attempts to change the actual knowledge standard in that in a specified circumstance such knowledge can and must be drawn, in which case ISPs have a duty to take action.

---

[121] Storie, M. N., n.d., "Best Practices for Wireless Access Providers to Avoid Copyright Infringement Liability" [Online] Available at: http://www.stoel.com/files/BestPractices_WirelessAccessProviders.pdf p. 9 [Accessed: 1 October 2015]

[122] E.g., Amazon (*Corbis Corp. v. Amazon.com, Inc.*, 351 F.Supp. 2d 1090 (W.D. Wash.2004)

[123] E.g., Ccbill (*Perfect 10, Inc. v. Ccbill Llc*, 488 F. 3d 1102 (9th Cir. 2007))

[124] *Ellison v. Robertson*, 189 F.Supp.2d 1051 (C.D. Cal. 2002), 1065.

[125] *Perfect 10, Inc. v. Ccbill Llc*, 488 F. 3d at 1109 (holding that "a service provider *implements* a policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications".) [Emphasis original] and *Ellison v. Robertson*, 357 F. 3d 1072, 1080 (9th Cir. 2004) (ruling that a service provider did not implement the policy to terminate a subscriber's account because its agent's contact for N&T notification is invalid.)

[126] The implementation does not need to be the actual action of terminating an ISP subscriber account. §512(i) does not require an ISP "to actually terminate repeat infringers" but rather requires an ISP "to put its users on notice that they face a realistic threat of having their Internet access terminated if they repeatedly violate intellectual property rights." (*Ellison v. Robertson*, 189 F.Supp.2d 1051 (C.D. Cal. 2002), 1065-66.)

This section discusses the development of copyright measures in two different areas--client/server and P2P technology.

4.4.3.1 In Client/Server Technology

The purpose of the current discussion is to reduce the amount of ubiquitous illegal posting on client/server whether the posting is the recurrence of the same infringing content or not. One of the proposed US N&T amendments offers a method to purge reposting of the same infringing content.

Professor Sean M. O'Connor proposed before the US Congress Subcommittee that there could be two solutions. First, Notice and Staydown (N&S) could be employed to deter the content that is already noticed from being reposted on the same site. There are two ways to use N&S. Service providers should establish voluntary best practices to monitor for, and immediately remove, reposted works. If such practices are unattainable, it is proposed that the US Congress should step in and amend the current N&T to N&S. The extreme position is that ISPs cannot enjoy safe harbour if they do not have, and implement, a policy to monitor and remove the same infringing content previously noticed.[127]

Then there is a proposal to amend the knowledge standard. IHPs could be exempted if they have no actual knowledge, no awareness that infringement is apparent but expeditiously remove content upon noticed. Current safe harbour exemptions inadvertently support IHPs in turning a blind eye to infringement. This is so even when significant quantities of material on the ISPs' websites are infringing.[128] Therefore it is argued that the current actual knowledge or red flag system does not work well and needs to be strengthened. "Wilful blindness could be defined to include any institutionalised policy prohibiting monitoring of content or consistently discouraging employee monitoring or investigation of content posts."[129]

---

[127] US House of Representatives, *op.cit.,* pp.14-15.

[128] In *Viacom Int'l Inc. v. YouTube, Inc.*, 679 F.3d 19, 33 (2d Cir. 2012), plaintiff, Viacom, cited evidence that "YouTube employees conducted website surveys and estimated that 75–80% of all YouTube streams contained copyrighted material." Moreover, an entity acting as financial advisor to Google estimated that "more than 60% of YouTube's content was 'premium' copyrighted content and that only 10% of the premium content was authorized." The 2nd Circuit Court remanded the District court to find if defendant, YouTube, can be found wilful blindness because of this fact and others.

[129] US House of Representatives, *op.cit.,* p.15.

The proposed new N&S could result in significant change. Currently, there is evidence showing that the volume of counter notices is low.[130] According to MPAA, of more than 10 million URLs sent to sites during March-August 2013, less than 10 URLs countered the noticed claims.[131] The lack of counter notices could be because content is actually infringing; therefore, posters have no defence. Another reason could be that users disregard the counter-notice because they know they can repost the content. Further, "[m]any posters are legally unsophisticated and don't know that they have this right or how to exercise it."[132] The situation is that there exists a lot of infringing content with just a few counter notices. N&S can deter the same infringing content from re-emerging. This can form a part, possibly major, of the solution. It is true that the same content can be posted illegally by one person but legally by another, if the latter is authorised or fair use. If the use of content is authorized but a right owner mistakenly takes down the content, then it is the right owner's responsibility to the licensees under the terms of the licence agreement. If the use is unauthorized but it is legitimate under the fair use/dealing principle, prohibition of use could jeopardise the public right. In this situation, DMCA has a provision regarding notice misrepresentation.[133] A misrepresenting notice is one where the right owner's agent knowingly materially misrepresents the case to show that material or activity is infringing. The agent can be held responsible. To strengthen this provision through N&S the legislators may need to clearly prescribe investigative duties. The duties concern right holder's investigation to determine if such use is legislative fair use/dealing before issuing a notice. Failing to do so could make a right holder liable for damage incurred by users or ISPs. By providing such duties, the amendment proposal could balance both parties interests.

---

[130] Urban, J. M. and Quilter, L., 2006, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act", *Santa Clara Computer and High Technology Law Journal*, 22, 621, Available via SSRN: http://ssrn.com/abstract=2210935 p.679.

[131] Boyden, *op.cit*., p.3

[132] Lemley, M.A., 2007, "Rationalizing Internet Safe Harbors.", *Journal on Telecommunications & High Technology Law*, 6(1) 101, p. 115.

[133] 17 U.S.C. § 512 (f) states:

"MISREPRESENTATIONS.—Any person who knowingly materially misrepresents under this section—

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it."

Furthermore, technology can play a part in solving the problem of recurring infringing content. A filter has already been developed to this end. It identifies previously recorded infringing material and prevents it from being re-uploaded or accessed.[134] In some platforms, e.g., YouTube, the so-called Content ID technology is used for the detection of legal content. It can be used to record infringing data too. The filter can be an effective mechanism for N&S.

4.4.3.2 In P2P Technology

Section 512 has caused a large amount of litigation, particularly with respect to P2P.[135] According to *Verizon*, DMCA is unable to deter P2P.[136] There is a system dealing with P2P elsewhere. France has developed a legal mechanism which has been running since 2009 and is aimed at controlling infringement on P2P. The resulting development is the so-called Graduated Response system. This system targets P2P users. The French legislation will be discussed in Chapter 5.

In conclusion, an ISP can be 'Transitory Digital Network Communications' and 'Information Residing on Systems'. Web-hosting services or website services can operate both information transmission and storage. Infringement can take place in an ISP's facility. Client/server technology might store infringing information on an ISP's server. This makes the 'Information Residing on Systems' susceptible to receipt of a notice. P2P needs an internet connection but no storage facility. 'Information Residing on Systems' can escape the receipt of a P2P notice. 'Transitory Digital Network Communications' might be obliged to disclose user identities. P2P user disclosure cases against 'Transitory Digital Network Communications' indicate that user identity may not be obtained because there are no valid notices produced. A policy directed towards the termination of repeat infringers' accounts is a prerequisite for ISPs. They needs to have N&T system in place and to inform subscribers of N&T system. The policy, however, does not apply to P2P users. All these elements render DMCA ineffective for the P2P enforcement. Apart from the P2P application, DMCA has other limitations. A large amount of notices has caused problems for both right holders and ISPs, particularly when the same infringing content reappears.

---

[134] *UMG Recording, Inc. v. Shelter Capital Partners LLC*, 718 F. 3d 1006, 1012-13 (9th Cir. 2013)
[135] US House of Representatives, *op.cit*., p.6.
[136] *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, Inc*., 351 F.3d 1229, 1238 (D.C.Cir.2003)

The recent attempt to correct the situation by the US Congress offers some solution. Any suggested solutions concern a reduction in the number of notices. Here a solution could possibly be a stayed down request by right holders. Up until now they have not addressed the P2P problem. The next section concerns DMCA N&T provisions. It shows relevant DMCA sections with their stipulated procedures.

4.5. The US Notice and Takedown Provisions under 17 U.S.C. § 512

In general, the Digital Millennium Copyright Act 1998 (DMCA) aimed to modernise Copyright Act 1976, which is initially codified in 1947, in order to meet the requirements of technological advancement. It has three titles. Title I implements two WIPO treaties which are the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). Title II amends 17 U.S.C. to address copyright infringement liability of online and other service providers. Title III deals with distance learning support and exemptions for libraries and archives when attempting to preserve deteriorating works. Title II has the purpose to "provide for limitations on copyright infringement liability for on-line and other service providers"[137], hence being the subject of the study here.

Title II has its origin in cases that right holders brought in an attempt to stop online user piracy through the ISP medium. The U.S. courts have developed over time what is known as copyright secondary liability.[138] The courts were inconsistent in their principle rulings. This was because the scope of online intermediary liability was a problematic and controversial issue that instigated a need for the US legislature to take action.[139] Title II provides the § 512 (a) - (d) addition to 17 U.S.C. The beginning of subsection (a) - (d) therefore demonstrates the liability limitations of each type of ISP. Such limitations clearly exempt an ISP's normal operation from incurring litigation but the ISP's cooperation is required. The limitations permit an ISP to enjoy a so-called safe harbour, obviously aiming to limit rather than to increase the liability of an ISP. The limitations encompass threats

---

[137] U.S. House of Representatives, 1998. *Report to the House of Representatives on Digital Millennium Copyright Act of 1998 for the 105th Congress, 2nd Session (105-551)*, p. 21. Available at: http://digital-law-online.info/misc/HRep105-551pt2.pdf [Accessed: 4 October 2014]

[138] Ginsburg, J. C. and Ricketson, S. 2006, "Inducers and Authorisers: A Comparison of the US Supreme Court's Grokster Decision and the Australian Federal Court's Kazaa Ruling.", *Media & Arts Law Review*,11, 1, Available via SSRN: http://ssrn.com/abstract=888928 pp.3-10 [Accessed: 18 June 2016]

[139] *Ouellette v. Viacom International, Inc.*, 2012 WL 850921 (Citing *Ellison v. Robertson,* 357 F.3d 1072, 1076 (9th Cir. 2004))

from both internet users and right holders.[140] ISPs which in their operation proceed in accordance with the law are not liable to copyright holders, primary or secondary. For example, they are not liable to their users if the N&T move was mistaken and interfered with their user's statutory fair use/dealing and subscriber contract. However, if an ISP decides not to follow and enjoy safe harbour, it will lose the immunities the provisions confer but that doesn't infer its liability. The affected parties need to prove that the ISP has performed in a manner which is attributable to direct, vicarious or contributory infringement.

At the time of its enactment, DMCA appropriately balanced the interests of content owners, online service providers, and information users.[141] The balance fostered the continued progress of electronic commerce and the growth of the Internet.[142] It served content owners' goals by requiring service providers and copyright owners to cooperate to detect and deal with infringing sites before the content was circulated too widely.[143] The measure was more immediate, but perhaps temporary, relieving the owners from going into court and getting a provisional injunctive order.[144]

The limitations offer exemption to liability within the following four categories of conduct by a service provider: 1. Transitory Digital Network Communications; 2. System caching; 3. Storage of information on systems or networks at direction of users; and 4. Information location tools (17 U.S.C. § 512 subsections (a)-(d) accordingly).[145] Subsections (a) through (d) exempt qualifying service providers from liability to pay any monetary relief for direct, vicarious and contributory infringement.[146] The subsections also confer

---

[140] *See*, e.g., *Ouellette v. Viacom International Inc.*, No. CV 10-133-M-DWM-JCL, 2012 WL 1435703 (D.Mont. 2012) and *Lenz v. Universal Music Corp.,* 572 F. Supp. 2d 1150 (N.D. Cal. 2008)

[141] U.S. House of Representatives, *op.cit.,* p. 21

[142] *Ibid.*

[143] Boyden, *op.cit*., p.1

[144] *Ibid.*

[145] Copyright Office, the U.S., 1998. *Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary*, Available at: http://www.copyright.gov/legislation/dmca.pdf p.8 [Accessed: 7 October 2014].

Under section 512(k)(1)(A), "service provider" in subsection (a) is defined as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." Under section 512(k)(1)(B), the same term "service provider" in subsection (b)-(d) is more broadly defined as "a provider of online services or network access, or the operator of facilities therefor."

[146] Under 17 U.S.C. §512 (k)(2), monetary relief means damages, costs, attorneys' fees, and any other form of monetary payment. Interestingly, liability limitation of the DMCA is wider than that of the EU

---

injunctive relief to the extent specified in § 512 (j).[147] ISPs are the key players in digital copyright protection. It is vital to know the different types of ISP.

4.5.1 Types of Service Providers Receiving Notification and their Safe Harbours

ISPs under 17 U.S.C. § 512 are classified into four types -- Transitory Digital Network Communications, System Caching, Information Residing on Systems and Information Location Tools (subsection (a)-(d) respectively). The provision confers safe harbour on ISPs provided they meet the conditions set forth in subsection (h). Moreover, as an ISP can fall into any of several types its activities at issue must involve a function described in subsection (a), (b), (c) or (d).[148] Everything considered, all conducts involve the transfer of information on the internet. This section investigates what ISP's exemptions are and how the exemptions operate in data interchange.

'Transitory Digital Network Communication'[149] is the first category under DMCA § 512 (a).[150] By using a 'Transitory Digital Network Communication' service, a subscriber is able to enter into the internet (via an IAP) and online networks (via an NP). "[I]Aps [Transitory Digital Network Communication] provide technical infrastructures for digital communication between each subscriber and anyone else connected to the internet."[151] 'Transitory Digital Network Communication' may be for the operating system networks or

---

E-Commerce Directive. The EU Directive leaves damages liability to the Member States. (Opinion of Advocate General, *op.cit*., para. 149)

[147] *Viacom International Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 520. (S.D.N.Y. 2010)

[148] U.S. Senate, Committee on Judiciary, 1998. *Report to the Senate on Digital Millennium Copyright Act of 1998 for the 105th Congress, 2nd Session (105-109)*, p. 41. Available at: http://digital-law-online.info/misc/SRep105-190.pdf [Accessed: 19 February 2015]

[149] Internet Access Provider (IAP) and Network Provider (NP) are among examples. A website (IHP or ICP) may serve as 'Transitory Digital Network Communication'. (*See* note 100 above) A torrent website can be 'Information Residing on Systems' and 'Transitory Digital Network Communication' depending on if the website does store copyrighted materials on the website. Normally, the website stores torrent files which are not infringing material and matches a requesting user with a source user. With these functions, it can be regarded as 'Transitory Digital Network Communications'. (*Columbia Pictures Industries, Inc., et al. v. Fung, et al.*, Case No. 10-55946 (9th Cir. 2013)) They are sometimes collectively called IAP.

[150] Under DMCA § 512 (k)(1)(A), 'transitory digital network communications' is a service provider that "offer[s] the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

Under DMCA § 512 (a): "Transitory Digital Network Communications.- A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections…"

[151] Jacobsen, S.S. and Petersen, C.S. 2011. "Injunction against Mere Conduit of Information Protected by Copyright: A Scandinavian Perspective." *International Review of Intellectual Property and Competition Law*, 42(2), 151, p.152.

for other networks (NP) which means that all IAPs that operate transmitting and routing material through their systems or networks are regarded as 'Transitory digital network communications' under DMCA § 512(a).[152] An IAP can also operate parts of, or an entire, system or network for another ISP as a subcontractor.[153] An entitled IAP in the first safe harbour is not liable for monetary or equitable relief provided it acts within its normal course. In the normal operation, 'Transitory Digital Network Communications' is that of transmits, routes or provides connection through its systems[154] and an automaton reproduces user-directed content in a short time before delivery to a destination. The ISP needs to ensure that the transmission of the material is not initiated or directed by itself, that the automaton keeps the reproduced content no longer than necessary for transmission, and that an automaton carries out submission without being involved in the selection of the material and the recipients.[155] § 512 (a) exempts 'Transitory Digital Network Communications' from liability for the reproduction of copyright material provided it is temporarily stored in ISP systems. In some technology such as USENET, the technology operator may store posts from its users; this is described as reasonably necessary for transmission, routing or provision of connections, and still be shielded from liability even if the posts are infringing copyright.[156] This is not to be confused with a caching system.

In practice, an ISP has a caching system. The system temporarily stores transmitted information automatically. This is necessary for reducing traffic congestion whenever the information is subsequently requested by its subscribers. "The difference between caching and transitory storage is whether the material is stored on the servers at the user's request (transitory storage) or through an automated process of the ISP (caching)."[157]

When an IAP offers server capacity for its customers for free or for hire by business, education institutes, email services, websites, the IAP becomes 'Information

---

[152] *Viacom v. YouTube*, 718 F. Supp. 2d, at 520.

[153] *Ibid.*

[154] 17 U.S.C. § 512 (a) paragraph one.

[155] 17 U.S.C. § 512 (a) (1)-(4)

[156] Storing of copyright infringer's posts on USENET servers for fourteen days constituted "intermediate and transient storage" within the meaning of the Digital Millennium Copyright Act's safe-harbour provision section 512(a). (*Ellison v. Robertson,* 357 F.3d 1072 (C.A.Cal. 2004))

[157] Storie, *op.cit.,* p.5.

Residing on Systems or Networks at Direction of Users' under 17 U.S.C. § 512(c) because it is 'a provider of online service or network access' or because it is the 'operator of facilities therefor'.[158] By the same reasons, when an ICP offer a space for their subscribers to post their own created content on the website, the ICP can become the 17 U.S.C. § 512(c) ISP.[159] "A provider of online services storing data on its own servers at its own discretion would not qualify as an ISP under this section […]."[160] 'Information Residing on Systems at Direction of Users', as the name suggests, have to provide information storage for users and, because of this, they are the ISPs that are subject to notice and are therefore required to process the taking down of the information.[161] Apart from N&T procedural requirements, ISPs would also qualify for limitation of liability provided they do not have "actual knowledge of infringing materials or activities".[162] In the absence of such knowledge, they are not "aware of the fact that such activities are apparent".[163] Finally, they must not have directly financially benefited from the infringing activity in cases where they have a right to control such activity.[164]

Information Location Tools under 17 U.S.C. § 512 (d) can be simply explained as linking or search engines. This section attempts to stop site locating service which directs users to an illegal content or supports infringing activities as culpable even when the site itself is not responsible for the provision of the content or activities. It also attempts to invalidate any infringing results to which a search engine directory might refer. N&T under 17 U.S.C. § 512 (d) is applicable to a cataloguing ISP.[165] If 'Information Location Tool' service providers remove requested links or results, they are exempt from liability. Like the information storage safe harbour in § 512(c), an Information Location Tool ISP qualifies for liability limitations if the following criteria are met: knowledge standard, no actual awareness of facts and circumstances, and no financial attribution.[166]

---

[158] 17 U.S.C. § 512 (k) (1) (B)
[159] *Viacom v. YouTube*, 718 F. Supp. 2d, at 520.
[160] Storie, *op.cit.,* p.6.
[161] *See* 4.4.1 Legal Definitions of Internet Service Providers (ISPs) for the purposes of Notice and Takedown Procedures above.
[162] 17 U.S.C. § 512 (c) (1) (A) (i)
[163] 17 U.S.C. § 512 (c) (1) (A) (ii)
[164] 17 U.S.C. § 512 (c) (1) (B)
[165] U.S. Senate, *op.cit*., p. 47.
[166] 17 U.S.C. § 512 (d) (1) (A) (B) and (C)

In summary, end-users are able to publish infringing materials stored in 'Information Residing on Systems'. The materials infringe copyright and hence right holders can request the cessation of the infringement. 'Information Residing on Systems' ISPs receive notices and process the taking down of the content. Right holders need to liaise with such ISPs. The next question is how the N&T procedure works and how 'Information Residing on Systems' can deter client/server users from infringing activities.

4.5.2 Notice and Takedown Procedure and Online Infringement

As to infringement on the internet, right holders are responsible for detecting potential infringing acts. Right holders can serve notice to an agent to ask 'Information Residing on Systems' to take down the alleged infringing content. The agent designated by 'Information Residing on Systems' is responsible for receiving notice and taking down the content. The N&T procedure is as follows:

(1) Information Residing on Systems receive a notice from a rights holder[167]

(2) Information Residing on Systems respond expeditiously to take down the material claimed to be infringing[168]and notify the subscriber accordingly[169]

(3) Upon receipt of a counter notification, 'Information Residing on Systems' replace the taken down material and notify the rights holder and resume the content within 10-14 days following the receipt of the counter notification [170]

(4) If the rights holder has filed a court action, 'Information Residing on Systems' will take down the material again[171] and there will be no further action until the court decision has been rendered.

N&T procedure has more details than those in (1)-(4) above. The details, such as elements of notification[172] and of counter notification[173], time frame for taking down and filing legal action and so on, are provided. For example, under section 512(c)(3)(B)(ii), the notification has to comply substantially with requirements of provisions under §

[167] 17 U.S.C. § 512 (c) (1) (A) (iii)
[168] 17 U.S.C. § 512 (c) (1) (C)
[169] 17 U.S.C. § 512 (g) (2) (A)
[170] 17 U.S.C. § 512 (g) (2) (B) and (C)
[171] 17 U.S.C. § 512 (g) (2) (C)
[172] 17 U.S.C. § 512 (c) (3)
[173] 17 U.S.C. § 512 (g) (3)

512(c)(3)(A) or it is not deemed to be a valid notification.[174] The notice is not enforceable if it complies with only some of the requirements.[175] A notice to ISPs indicates necessary information such as infringed and infringing works along with an accurate notice statement.[176] The US notice does not need any proof in asserting the facts. The complaining party has to provide a statement that he believes in good faith that the work is being used without permission and that, under penalty of perjury, he has authority from the owner of the exclusive right.[177]

'Information Residing on Systems' can deter client/server user infringement in two ways – (1) removing infringing content; (2) disabling access to the content.[178] There are no other measures that right holders can request. Right holders in Thailand have more options available in connection with the court order. However, as shown in (3) and (4) above, the US system provides end-users with a form of self-defence where they can rebut the notice with a counter-notice. Such a defence is not available in the Thai system. Moreover, N&T is appreciated as a procedure that is relatively quick and economical because it circumvents the court system. The right holder does not need to initiate every single infringement case and the notice will not be examined by the court unless it is countered by the user in which case the right holder needs to file the infringement lawsuit to maintain the taking down status. These aspects are objects of the discussion below which compares and contrasts with how Thailand's court system deals with similar infringing activity.

4.6 Comparative Analysis

This section compares similarities and differences regarding the definitions, operations, exemptions and procedures for enforcing digital copyright online. Other topics such as system limitations and website blocking are also discussed. In addition, these elements will be critically analysed to show the efficacy/efficiency and benefits/drawbacks of the US and Thailand legislation. Preliminary recommendations will be provided in brief following the outcome of the comparative discussion.

---

[174] *Perfect 10, Inc. v. Ccbill Llc*, 488 F. 3d at 1112
[175] *Ibid.*
[176] 17 U.S.C. § 512 (c)(3)(A)(i) - (vi)
[177] 17 U.S.C. § 512 (c)(3)(A)(v) and (vi)
[178] 17 U.S.C. § 512 (c)(1)(A)(iii)

4.6.1 ISPs Affected by the Digital Copyright Protection Measures

The US and Thai SP definitions do not seem to be different in legislative terms. The two jurisdictions have two ISP defined categories. The categories are classified widely by ISPs' functions -- telecommunication access and information storage. The US 17 U.S.C. § 512 (k) (1)[179] has two subsections -- 17 U.S.C. § 512 (k) (1) (A) defines the term as used in § 512 (a) which suggests IAPs, and 17 U.S.C. § 512 (k) (1) (B) as used in § 512 (c) which suggests IHPs.[180] Similarly, Thailand CA 2015 § 32/3 paragraph two defines SP in two subsections -- CA 2015 § 32/3 paragraph two (1) suggests IAPs, and CA 2015 § 32/3 paragraph two (2) suggests IHPs.[181] These CA 2015 SP definitions are literally exactly the same as that of CROA 2003. Thai MICT Notification No. 5, implemented the CROA 2003, detailed definitions of all the IAP, IHP and ICP service providers alluded to by CA 2015.[182] The Notification shows Thailand and the US definitions to be similar. Both jurisdictions incorporate IHPs with IAPs definitions. MICT Notification No. 5 embraces IAPs with IHPs.[183] The last sentence of 17 U.S.C. § 512 (k) (1) (B) clarifies that the IHP definition includes "an entity described in subparagraph (A)" which is IAPs. These similarities do not have much implication in terms of application; it is the functional aspects of an ISP which do.

CA 2015 § 32/3 paragraph two SP definitions can also be taken as ISP functional classifications. Thailand ISP functional classifications are different from those of the US. They are different because MICT Notification No.5 does not place ICPs in the same classification as IHPs but the US ICPs and IHPs are both covered in the same 17 U.S.C. § 512 (c) classification. CA 2015 § 32/3 paragraph two has two classifications whereas the

---

[179] 17 U.S.C. § 512 (k) (1) provides definitions to "Service Provider" as followings:

(A) As used in subsection (a), the term 'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

(B) As used in this section, other than subsection (a), the term 'service provider' means a provider of online services or network access, or the operator of facilities therefor, and *includes an entity described in subparagraph (A)*.

[*Italic* emphasis added]

[180] 17 U.S.C. § 512 (a) (b), (c) and (d) are 'Transitory Digital Network Communications', 'Information Residing on System', 'System Caching', and 'Information Location Tools' accordingly.

[181] CA 2015 § 32/3 paragraph two subsection (1) "A person who provides service to the public with respect to access to the internet … ", and subsection (2) "A person who provides services with respect to the storage of computer data for the benefit of another person."

[182] Trivially different, MICT Notification No. 5 (1) uses the term 'Telecommunication Access Service Provider' instead on IAPs and No. 5 (2) uses 'Content Service Provider'. (*See* 4.2.2 Clarification of meaning and classification of service providers under CA 2015 § 32/3 and the other relevant regulations above.)

[183] *See* Table 1 above.

US DMCA § 512 has four (subsections (a) - (d)). IHPs and ICPs are ISPs that play key roles in client/server infringement protection. The difference in ISP functional classifications between the two jurisdictions has considerable implications in practice. The Thailand system does not particularly specify which kind of service providers will carry out which procedures (e.g., remove content and/or cease the infringement).[184] The US system, however, makes it clear that the service providers specified in § 512 (b), (c) and (d) have specific ISP functions. These functions, those of Information Residing on Systems in particular, must expeditiously remove content or disable access upon being notified.[185] This comparison should not be considered as an attempt to change the Thai legislation but rather as a clarified understanding of the US legislation by way of the technical explanation in accordance with good practice in order to suggest recommendations for Thailand.

To comply with good practice, a party requesting a motion will supply with it information regarding the specific functions of the ISP. In the motion to the court, the party supplies pertinent functional details of the infringing activities and presents such details at the trial. The injunction requested relates to the ISP's capacity. The court hears the case, confirms the facts and ultimately grants a suitable order. Such good practice assumes an understanding of the technical issues involved. All players in the case need to be thoroughly conversant with the associated technical issues. A party's failure to provide appropriate factual details may lead to a dismissal of the case, or put another way, if the court misunderstands, this can lead to a decision based on untrue, irrelevant facts. For example, a party who seeks to remove content from the ISP's system needs to know that such ISP offers the storage function in its system. The court has the power to impose an order for content removal on an IHP rather than a mere conduit IAP. It is recommended that Thai institutions and practitioners need to be educated with regard to the technical

[184] CA 2015 § 32/3 paragraph four: " … it [the court] shall impose service providers [telecommunication and content storage] to cease the alleged infringing acts, or to remove alleged infringing work from the service provider's system … "

[185] 17 U.S.C. § 512 (b) (2) (E): "if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c) (3)…"

17 U.S.C. § 512 (c) (3): "upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing…"

17 U.S.C. § 512 (d) (3): "upon notification of claimed infringement as described in subsection (c) (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing…"

issues concerned. Chapter 6: Conclusions and Recommendations will provide more detailed recommendation. Without a proper understanding of ISP definitions and functions, it would be a waste of resources for all those involved parties in a trial in which both copyright protection and fundamental rights would not be guaranteed.

4.6.2 The US and Thailand Legal Proceedings and Their Limitations

US N&T proceedings are simpler than Thailand court proceedings. Following US N&T proceedings, a right holder submits and an IHP receives a notice of alleged infringement, the IHP responds expeditiously by taking down the material claimed to be infringing and notify the subscriber accordingly. There will be no further action if no counter notification is produced. With regard to court proceedings, upon detection of infringement, the right holder can initiate a case by filing a motion to the Central Intellectual Property and International Trade Court (CIPIT). The motion needs information about service providers, infringed and infringing work, investigating data, any damage suffered, and the requested court order. After receipt of the motion, the court will then summon the other party, namely an SP, to enter into the case and will hold an examination. If granted, the order shall be in force instantly and the right holders will have to initiate the infringement case within the time fixed therein or the order will be invalid.

As each jurisdiction has its own approach, it has its own unique limitations. The problems experienced in the Thai court system are not in any way related to the US N&T system. Voluminous notifications are a problem in the US but are unlikely to be a problem in Thailand. A large number of end-user court cases are not possible in Thailand because of the burden on court resources. This limits the permissible number of cases being heard to the strongest cases only. Such a limitation restrains right holder usage of the Thai court system which is an access to justice issue beyond the scope of this paper. The DMCA was an attempt to construct an N&T system in order to circumvent the necessity of a court system. US right holders need to file a lawsuit if a counter notification is made. There, very few cases go to court because less than one per cent of notices generate a counter notice.[186] The magnitude of infringement on the internet necessitates a measure that offers a simple and quick response. In this respect, the US system is better placed to solve the problem of digital online copyright infringement. Measures against end-users need to

[186] *See* 4.4.3.1 In Client/Server Technology above.

be quicker and more cost effective than those afforded by the current Thai system. With these aims in mind, a recommendation relating to Thailand's adoption of the US N&T will be proposed in chapter 6: Conclusions and Recommendations.

4.6.3 A Comparison of Due Process

Due process of law guarantees citizen's rights to be notified and to be heard in a fair proceeding before their lives, property or liberty can be forfeited. In the author's opinion, the US system has a problem with the reverse burden of proof. The notice prompts implementation by taking down content. At this point, the requesting party has not yet proved that the content is infringing. Rather, the accused subscriber must demonstrate a belief in good faith before the content can be restored.[187] It is controversial whether the system is due process.[188] Without the examination, the user's right of expression can be forfeited.

On the other hand, it can be argued that the US legislation honours an end-user's right more than that of Thailand. Although the notice is not examined as to whether the content and the user are infringing as the right holders allege or not, the end-user can send a counter notification to the ISP where the ISP will replace the removed material or cease the disabling access to it.[189] N&T is of due process because notices and counter notices extend a right holder and an allegedly infringing user equal chances.[190] The Thai CA2015 does not supply an end-user with the right to defend himself. Nowhere in the CA 2015 §32/3 does it state that the court shall issue a summon to a user although a right holder and an end user, not an ISP, are the actual conflicting parties. The Thai court can hear the case without the user being present. After delivery of the order, there are no provisions that allow the user to contradict the order. The user may not even know the order is granted because there is no provision providing that the user shall be informed.

---

[187] 17 U.S.C.A. § 512 (g) (3) (C)

[188] A copyright opponent has tried to put a burden on the N&T system in that "copyright owners must consider fair use before sending a takedown notice, or face legal liability". (Electronic Frontier Foundation (EFF), 2015, "Tuesday Court Hearing Over Absurd Copyright Claim in Family Home Movie" [Online] Available at: https://www.eff.org/press/releases/tuesday-court-hearing-over-absurd-copyright-claim-family-home-movie [Accessed: 10 July 2015])

[189] 17 U.S.C. § 512 (g) (2) (B) and (C) (*See* 4.5.2 Notice and Takedown Procedure Concerning Online Infringement.)

[190] Still, it is argued that, in this situation, ISP resumes the content within 14 days during which a user is deprived of his freedom of speech. This issue will be present solution in chapter 6.

The user perhaps knows it if the right holder has filed an infringement case. In this regard, the US N&T proceedings are more justified.

4.6.4 The Extent of the Court Order and the Act of 'Taking Down' by the ISPs

Thai court orders, as well as US N&T practices, do adopt sound interlocutory injunction principles, the aim of which is to stop the defendant's continuing infringement and relieve the plaintiff's on-going damage. However, Thailand and the US employ different approaches. Under 17 U.S.C. § 512 (c) (1) (C), the US 'Information Residing on System' expeditiously: (1) removes the infringing content; or (2) disables access to the content.[191] US ISPs have clearer guidance than those in Thailand. There are no other measures on which a US notice can base a request.[192] In contrast, Thai legislation has two principal measures, namely: (1) cessation of the infringing acts; and (2) removal of the infringing content.[193]

Thai and the US removal of content are both straightforward; ISPs merely eliminate the content from their systems. The term 'to cease infringement' in the Thai jurisdiction has wider implications than does the term 'disabling of access' of the US. The wider implications are of benefit to copyright holders because they offer a huge range of potentials orders a court can issue. The implication is that the court can order any measures that cease the alleged infringing acts which is very powerful. This aspect makes the Thai legislation more flexible than the US system in functional terms. The Thai flexibility could also feature strongly when encountering different forms of future online threats with a variety of potential measures. However, a high degree of flexibility may also cause misuse of an order because any measure is permitted even though it might only operate partly, temporarily, or not proportionately. For example, website blocking, as discussed earlier, can disproportionately deny access to the whole website merely because specific infringing content was published by any particular user.[194]

---

[191] The right holder can otherwise motion for an injunction where the court may grant an order to restrain an ISP from providing access to infringing material or activity, or from giving access to an infringing subscriber of an ISP's system and for other injunctive relief necessary to restrain infringement. (17 U.S.C. § 512 (j) (1) (A))

[192] *Recording Indus. v. Verizon*, 351 F.3d, at 1235.

[193] These measures have to be 'necessary' and the court must find them 'reasonable' in its discretion. (CA 2015 § 32/3 paragraph four)

[194] *See* 4.3.3.1 Website blocking and Disabling Access to Content .

It is true that the wide range of remedies can be delimited by the court's discretion under the term 'reasonable'. The court has discretion to demarcate the breadth of its order or even not to grant the order at all if it is not 'reasonable'. Thai legislation provides the 'reasonable' discretion which suffices somewhat as a legal tool for the court. However, the implications of the term 'reasonable' can be improved. Under the current terminology, it depends solely on the knowledge the court has at its disposal and on the information obtained in the case. To exercise 'reasonable' discretion, it is recommended that such a term be clarified by the inclusion of specific factors for consideration and the court participants be educated as to scholarships outside legal issues. This recommendation will be further expanded in Chapter 6: Conclusions and Recommendations.

4.6.5 Concluding Remarks

In order to simplify the comparison, Table 3 below summarises the discussions above.

Table 3: The US System and Thailand System Comparison

Country / Objects of Comparisons	The US	Thailand
1.Classifications of Service Providers (SPs)	Safe Harbours under 17 U.S.C. § 512 (a) - (d) accordingly 1) Transitory Digital Network Communications 2) Information residing on systems or networks 3) System Caching 4) Information Location Tools	Information Retention under MICT Notification No. 5 (1) - (2) accordingly 1) Telecommunication Access Service Providers A. Telecommunication and Broadcast Carrier B. Access Service Providers [IAPs, ISPs] C. Hosting Service Providers [IHPs, NSPs] D. Internet Café 2) Content and Application Service Providers, e.g., Web Board or Blog, Internet Banking and Electronic Payment Provider, Web Service, e-Commerce or e-Transactions

Country / Objects of Comparisons	The US	Thailand
2. SPs affected by Digital Copyright Protection Measures Against Client/Server Technology User Infringement	Notice and Takedown - Internet Hosting Service Providers (IHPs) under 17 U.S.C. § 512 (c) 'Information Residing on Systems or Networks at Direction of Users' - Internet Content Service Providers (ICPs) under 17 U.S.C. § 512 (c) 'Information Residing on Systems or Networks at Direction of Users'	Court Order - Internet Hosting Service Providers (IHPs) under MICT Notification No. 5 (1) (C); and - Internet Content Service Providers (ICPs) under MICT Notification No. 5 (2)
3. The Extent of the Measures	Notice and Takedown - Remove the content from the system - Disable access to the content	Court Order - Remove the content from the system - Cease the infringing acts
4. Advantages and Disadvantages	Notice and Takedown 1) Advantages - Users can counter notice. - Quick - Cheap 2) Disadvantages - Volume of Notice - Recurring Infringing Content - Unusable with P2P	Court Procedure and Order 1) Advantages - Flexible Range of Order ('Cease the infringing acts' and 'Reasonable') - Usable with the Future Threats 2) Disadvantages - No guidance of 'Cease the infringing acts' and 'Reasonable' interpretation provided - Slow - Costly - Users cannot be involved in court proceedings.

In conclusion, the above table briefly compares the Thailand and the US approaches to online copyright infringement. Thailand and the US have different classifications and definitions. These differences do not affect the efficacy of the Thai system. Copyright infringement can take place within all sorts of ISP classifications. Regarding client/server technology, in Thailand it is IHPs and ICPs that execute court orders rather than IAPs. Similarly, in the US it is IHPs and ICPs rather than IAPs that

process notices. An appropriate ISP function along with an appropriate request is required information within the motion application under CA 2015 § 32/3 paragraph four. Likewise, the US notice has to have substantial information in accordance with 17 U.S.C. Section 512(c)(3)(A) and (B)(i). If notice requirements are met, the US ISP who wishes to have protection by means of safe harbour will be required to take down the content. In comparison a Thai court holds examination and considers if it is 'necessary' to grant an order.[195] An injunctive order is 'necessary' to stop the on-going infringement and relieve the on-going damage.[196]

Knowledge of ISP functions should be acquired by means of education beyond the court rooms. Litigants are especially in need of appropriate knowledge in order to present facts in the trial. Court fact finding relies upon information presented by the parties concerned; therefore, litigants should be able to understand the meaning of any specialist technical language.

US measures are limited to 'remove the content' or 'disable access to the content'. The Thai court order has the same content removal but encompasses more by means of the term 'to cease the infringement by other means'. Though not specific, the term 'to cease the infringement by other means' still benefits Thailand. The phrase can be explained by providing certain examples, e.g., access disabling, traffic capping, website blocking, content identification and filtering, internet speed reduction and subscriber's account termination. Thailand could incorporate these examples by developing the 'reasonable' factor interpretation through the CA 2015 amendment. More favourably, the standards of such examples could be determined by agreement acquired from stakeholders.

Certainly, the Thai court order system is more powerful than the US notice. However, the court proceedings do not satisfy the needs of online copyright protection in many respects. Thailand's system is less efficient than that of the US. The CA 2015 court proceedings are slow, expensive, and do not protect end-user rights.[197] The Thai system

---

[195] CA 2015 § 32/3 paragraph four

[196] CIPC 1934 § 254 (2)

[197] An EU report concludes that the Thai court system is slow and costly. (European Commission, 2015. *Report on the protection and enforcement of intellectual property rights in third countries*. p.22. Available at:

---

does not encourage a right holder to use it and this is an access to justice issue. Because of its inefficacy, the volume of CA 2015 copyright infringement motions is expected to be low in contrast to the quantity of notices experienced in the US N&T system. Although the US N&T has the problems of voluminous notices and content reappearance to deal with, it is in the author's opinion still a better system.

As to the argument against N&T on freedom of speech invasion, chapter 2 has suggested that a notice that leads to taking down of allegedly infringing content secures end-user's freedom of speech even if the right holder does not reasonably investigate infringement before a notice is filed.

Chapter 6 of this thesis will recommend the adoption of N&T for Thailand with an additional mechanism to cope with the US N&T problems. Moreover, it will suggest potential reform concerning the balance between freedom of speech and copyright protection in Thailand as discussed in chapter 2.

Regarding P2P infringement, this chapter has already suggested that the US' N&T system fails to adequately protect copyright against digital infringement when it comes to P2P users because it was not originally designed for this task. The next chapter will reveal that Thailand's CA 2015 is also inadequate when applied to P2P technology. Chapter 5 will introduce current measures from France that have made progress in overcoming the P2P problem with a view to comparing them with Thailand's equivalent provisions to further develop CA 2015 deterrence measures to deal with P2P copyright infringement applications.

https://euipo.europa.eu/ohimportal/documents/11370/0/Report+on+the+protection+and+enforcement+of+intellectual+property+rights+in+third+countries [Accessed: 7 July 2016].)

Chapter 5: The Thailand and France Approaches to Graduated Response

5.1. Introduction

"While new forms of unauthorized distribution continue to grow, the majority of copyright infringement incidents on the Internet still occur through peer-to-peer (P2P) file-sharing."[1] In Chapter 4 the conclusion was drawn that the US Notice and Takedown (N&T) was created for client/server and has proved to be inappropriate for P2P. This chapter analyses a measure, so-called 'Graduated Response' (GR), which directly targets P2P. It examines and compares CA 2015 with GR in application to P2P file sharing infringement by end users.

In 2006, France transposed the EU Directive 2001/29/EC of 22 May 2001 (EU Directive 2001/29/EC) on the Harmonisation of Certain Aspects of Copyright and Neighbouring Rights in the Information Society.[2] The French initiative included GR with the technological protection measures (TPM) provided in EU Directive 2001/29/EC in the Act for Copyright and Neighbouring Rights in the Information Society (DADVSI) (French: *Loi sur le Droit d'Auteur et les Droits Voisins dans la Société de l'Information*).[3] Essentially, DADVSI introduced the concept of internet users' obligation to monitor their own internet usage.[4] Based on this concept, the French Parliament later passed the Act Promoting the Distribution of Works and the Protection of Rights on the Internet (French: "*Haute Autorité pour la Diffusion des œuvres et la Protection des droits d'auteur sur Internet*") which reaffirmed the internet subscriber obligation principle.[5] HADOPI also

---

[1] BitTorrent is one kind of P2P file sharing programme which is extremely popular. IFPI states that fifty-seven percent of all Internet traffic in Eastern Europe is made up of BitTorrent transfers. (Boardman, M. 2011. "Digital Copyright Protection and Graduated Response: A Global Perspective*" Loyola of Los Angeles International and Comparative Law Review*, 33, 223, [Online] Available at: http://digitalcommons.lmu.edu/ilr/vol33/iss2/1 p.224 and note 15 [Internal Citation omitted] [Accessed: 31 May 2015]. For more information about how BitTorrent works please see Chapter 2 of this thesis.

[2] France, Hadopi, 2011. *Annual Report 2011*, Available at: http://hadopi.fr/sites/default/files/page/pdf/Hadopi_Rapportannuel_ENG.pdf p.14 [Accessed: 30 April 2015] Throughout this thesis HADOPI stands for the HADOPI Act and Hadopi for the Hadopi organization.

[3] *Ibid.*

[4] *Ibid.*

[5] In this thesis "HADOPI" stands for the Act (the High Authority for the Dissemination of Works and the Protection of Rights on the Internet Act or France Intellectual Property Act (FIPC) 2009), and "Hadopi"

provided GR with a warning system, a presumption of guilt and an automatic fine for breach of the obligation. Internet disconnection was also introduced into the HADOPI as complementary to criminal sanction.

Importantly, the recent Thai CA 2015 employs a court procedure to counteract online copyright infringement on all platforms, including P2P.[6] Thailand's online copyright protection provisions for Peer-to-Peer (P2P) copyright infringement will be explored in the following section.

5.2 Thailand Online Copyright Protection Provisions for Peer-to-Peer (P2P) Copyright Infringement

The court proceedings in application to client/server as described in chapter 4 apply in their entirety to this chapter.[7] In other words, the proceedings are not different between client/server and P2P applications. This section will explore service providers that are affected by the court order in its application to P2P under CA 2015 § 32/3. It will also explore whether Thailand laws facilitate P2P user enforcement by having an internet subscriber duty like that of France. With the lack of such a duty, the section will determine if a court motion application requires real infringer and/or subscriber identification. Finally, with the lack of such identification, this section will examine if Thailand's legislation has presumption of guilt for internet subscribers or if an online copyright infringement count can be classed as a minor offence for which the offender can be fined.

As in other jurisdictions, service providers play an important part in the court order execution. The following subsection will explore the classification(s) of service providers that are relevant to P2P technology. In other words, it searches for a service provider against which a right holder may file a motion to stop P2P users to implement the court order.

for the organization (the High Authority for the Dissemination of Works and the Protection of Rights on the Internet).

[6] For CA 2015's background, purposes and surface legislation see Chapter: 4 – 4.2. Thailand Copyright Act (No.2) B.E.2558 (2015) Provisions for Digital Copyright Protection.

[7] *See* 4.2.1 Thai Court System for Digital Copyright Protection.

5.2.1 Service Providers Affected by the Court Order in its Application to P2P under CA 2015 § 32/3

The definitions of service providers and their classifications as clarified in chapter 4[8] and the other relevant regulations are also applicable in this chapter. The difference between chapters 4 and 5 is that ISPs dealing with client/server technology may not be the same as ISPs in P2P. This subsection clarifies these issues.

Pursuant to section 32/3 paragraph one, a right holder can file a motion for a court injunction when it is reasonable to believe that copyright infringement has 'taken place' within a service provider's (SP's) system. A service provider, under CA 2015 Section 32/3 paragraph two, in the online environment is an internet service provider (ISP). CA 2015 Section 32/3 paragraph two states:

"For the purpose of this section, a service provider means:

(1) A person who provides service to the public with respect to access to the internet or other mutual communication via a computer system, whether on their own behalf, or in the name of, or for the benefit of, another person

(2) A person who provides services with respect to the storage of computer data for the benefit of the other person"

IAPs and IHPs are in the telecommunication access provider class under CA 2015 Section 32/3 paragraph two (1). On the other hand, Internet Content Service Providers (ICPs) are computer data/application providers under CA 2015 Section 32/3 paragraph two (2). As suggested in chapter 4, all of these ISPs are service providers that can be subject to a court order under CA 2015 Section 32/3 paragraph two.[9] The question is if P2P infringement has taken place within these ISP systems and, if so, how and through what class of ISP.

P2P protocol differs from client/server protocol. There is no need for a central computer server which stores information or software which inherently runs the server. "In peer-to-peer networks, every member, or peer, acts as both a client, by requesting

[8] *See* 4.2.2 Clarification of Meaning and Classification of Service Providers under CA 2015 § 32/3.

[9] This thesis studies user infringement and protection measures thereof; ISP liabilities and exemptions are not of concern in this thesis.

data from other peers, and as a server, by contributing a portion of one's computing resources to the network as a whole."[10] The data is kept in users' computers and is exchanged directly among users' computers.[11] The file exchanges conducted in a P2P platform can result in 'reproduction' and 'adaptation' of copyrighted works on other users' computers. They can also facilitate others in obtaining the copy; hence, 'communication to the public' of the works. These acts constitute copyright infringement.[12]

In these circumstances, users' information does not reside in a server owned by an IHP. ICPs provide a web board and blog, and web service for users' information. The IHP's server and ICP's web board are not the places where P2P users' information resides. Therefore, P2P file exchange infringement is not taking place within the IHPs' server communication systems nor is it within the ICP's web board. The question though is if it occurs in internet access providers' (IAPs') systems.

To download/upload content from/to another computer online through P2P, a connection must be established.[13] IAPs' computer systems offer connection and operate as a conduit by transmitting potentially illegal information. The systems receive information from a particular P2P user and send it to other P2P subscribers as recipients. These processes cannot be possible without IAP communication systems.

"As each user of the peer-to-peer network will potentially be liable for infringements to the making available right and, eventually, to the reproduction right, measures based on art. 8.3 of the InfoSoc Directive could be taken against the intermediaries whose services are used for the functioning of the peer-to-peer network (the peer-to-peer operator, the access providers of the users)."[14]

---

[10] Patel, A.R., 2010, "BitTorrent Beware: Legitimizing BitTorrent against Secondary Copyright Liability", *Appalachian Journal of Law*, 10, p. 119.

[11] Brown, M. 2009, "White Paper: How BitTorrent Works" [Online] Available at: http://www.maximumpc.com/article/features/white_paper_how_bittorrent_works [Accessed: 26 June 2014]

[12] They can generate an act of criminal and/or civil liability. (*See* chapter 3: 3.2 Can Client/Server and Peer-to-Peer User Activities be classed as Civil Offences under Copyright Act B.E.2537 (1994)?) *and* 3.3 Are Client/Server and Peer-to-Peer User Activities Criminal Offences under Copyright Act B.E.2537 (1994)?)

[13] Borland, J., 2004, "Covering tracks: New privacy hope for P2P", [Online]. Available: http://news.cnet.com/2100-1027-5164413.html [Accessed: 24 July 2014].

[14] Depreeuw, S. and Hubin, J., 2014. *Study on the Making Available Right and its Relationship with the Reproduction Right in Cross-Border Digital Transmissions*, [Online] Available at:

IAPs contribute to violations to copyright of reproduction, adaptation and communication to the public via their systems whether or not they can be held responsible.[15] Therefore, it can be concluded that these infringing activities do 'take place' in the IAP's systems under CA 2015 section 32/3 paragraph one. Hence IAPs can be subject to a right holder motion.

5.2.2 Do Thailand Laws have Internet Subscriber Obligations and Does a CA 2015 Motion Need to identify the Subscriber?

This section considers the relevant provisions of Thailand such as the Penal Code B.E.2499 (1956) (hereinafter 'PC 1956') and the Criminal Procedure Code B.E.2477 (1934) (hereinafter 'CRPC 1934') which could be considered as comparable to the internet subscriber duty of HADOPI Act. In case that Thailand does not have such a duty, this section analyses if subscriber identification is necessary in court motion under CA 2015. In this regard, the French HADOPI Act creates such a duty to monitor internet usage for P2P protection. The monitoring of internet account usage on the part of the account subscriber well compensates for the difficulty of identifying an actual copyright infringer.

In Thailand, there is no obligation for internet use monitoring prescribed by the law. *Prima Facie*, an internet account owner is not responsible for infringing act undertaken by using his account merely because he is the account owner. Even if the account owner knows there is the infringement taken place by using his account, there will have to be determined whether he is liable as a principal, instigator, abettor or contributor of the infringement in both civil and criminal cases.[16]

The question is whether an IP address is enough and whether a CA 2015 motion needs to identify the illegal P2P user or subscriber. These questions can be answered by the required information of a motion under CA 2015 § 32/3 paragraph three, which states:

---

http://ec.europa.eu/internal_market/copyright/docs/studies/141219-study_en.pdf p.29 [Accessed: 3 December 2015]

[15] One commentator argued that the Thai courts cannot 'hold an ISP liable for secondary infringement on the basis of illegal file sharing'. (Khopuangklang, K. 2011, "Should ISPs in Thailand act at the behest of the entertainment industry to control P2P file sharing?" *European Intellectual Property Review*, 33(10), 632.)

[16] Beside substantive law, there are problems with procedural law in the legal action against a subscriber. (*See* 5.3.6 Taking Legal Action against infringers Subsequent to the Court Order and Problems of Proof in the Trial without Actual Infringer Identification below.)

"The motion in paragraph one shall have apparent details about information, evidence and request as follows:

(1) Name and address of the service provider;

(2) Allegedly infringed copyrighted work;

(3) Work allegedly made by infringement;

(4) Process of investigating time and date of detection, and infringing acts or circumstance as well as infringement evidence;

(5) Potential damage incurred by the alleged infringing acts;

(6) Request to the service provider to remove the alleged infringing content from service providers' computer systems or to cease infringement by other means"

None of (1) - (6) requires identification in a motion. Subsection (4) requires 'infringing act' or 'circumstances' information. A petitioner can satisfy subsection (4) by demonstrating the 'circumstances' of how P2P architecture works and how a specific IP address participates in file swap without permission from a right holder which attracts 'infringing act'.[17] To this point the right holder can investigate to know the fact that the IP address is attached to a specific IAP.[18] The right holder does not know who actually used the IP address.[19] Such an IAP is the only one who can tell which account is assigned the IP address and identify the account owner (not the real infringer). Therefore, it can be concluded that a motion is valid even though it does not identify an account holder or an infringer. If granted, a court order could potentially affect the account holder and the whole household, irrespective of whether or not the holder is the infringer. The next subsection will explore if Thailand has a presumption of guilt that can infer that the account holder is culpable of the alleged copyright infringement.

---

[17] Details of how P2P architecture attracts infringing act can be found in chapter 3 -- : 3.2 Can Client/Server and Peer-to-Peer User Activities be classed as Civil Offences under Copyright Act B.E.2537 (1994)?.

[18] Ryan, J. 2010, "Internet access controls: Three Strikes 'Graduated Response' Initiatives" [Online] Available at: http://www.iiea.com/documents/draft-overview-of-three-strikes-measures-nlm-study p. 7 [Accessed: 2 December 2015] Citing *EMI Records & Ors v. Eircom Ltd*, [2010] IEHC 108.

[19] *Ibid.*

5.2.3 Does Thailand Law have a Presumption of Guilt and Are Copyright Infringement Charges Minor Offences?

This section considers if copyright infringement is a minor offence and whether there is a presumption of guilt in digital copyright enforcement due process. In this area, France's onus on an internet account subscriber to monitor internet usage is underpinned by a presumption of guilt. The actual infringer does not need to be identified. This reverse burden of proof is only acceptable because the breach of duty is classed as a minor offence.[20]

Currently, CA 1994 has no such a presumption of guilt provision. CA 1994 used to have a presumption of guilt in section 74.[21] A manager of a legal entity was presumed guilty for the illegal actions of that entity unless he could prove that the actions were accomplished without his knowledge. The Thailand Constitutional Court ruled that § 74 placed a burden on a manager and the legal entity to prove his innocence. Such a burden conflicted with the 'presumption of innocence' under the Constitution of Thailand section 39 paragraph two. The Constitutional Court, therefore, held that section 74 was unconstitutional.[22] It did not rule out the possibility of a reverse burden of proof in other circumstances, e.g., minor or petty offences.

In Thailand, a minor offence can be explained as a petty offence. Petty offences are the those that have penalties of no more than 1 month imprisonment and/or 10,000 baht in fines (approximately £200 GBP).[23] Under CRPC 1934 § 37, minor offences can be settled by a fine imposed by authorities without criminal indictment provided the accused willingly pays the fine. In general, offences that are settled at the inquiry stage must only be punishable by a fine.[24] Offences can also be settled when other laws are supportive of such a fine.[25] CRPC 1934 § 37 states:

---

[20] The French Constitutional Council Decision no. 2009-580 of June 10th 2009, Available at: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf p. 5 [Accessed: 19 September 2015])

[21] The then section 74 provided: "If a legal person commits an offense under this Act, all the directors or managers of the legal person shall be considered joint offenders with the legal person unless they can prove that the legal person has committed the offense without their knowledge or consent."

[22] Thailand Constitutional Court Case no.5/B.E.2556 (2013) [Thai] Available at: http://www.constitutionalcourt.or.th/index.php?option=com_docman&task=cat_view&gid=542&Itemid=94&lang=th&limitstart=10 [Accessed: 20 September 2015]

[23] Thailand PC 1956sections 102 and 367-398

[24] CRPC 1934 § 37(1)-(3)

[25] CRPC 1934 § 37(4)

"Criminal cases may be dismissed as follows:

(1) In the case of offences *having a fine as the only penalty*; by the accused voluntarily paying to the incumbent official, prior to a hearing, the maximum fine prescribed for the offence;

(2) In the case of petty offences, offences having a fine not exceeding the petty offence fine, or any other offences *having a fine as the only penalty* and not exceeding ten thousand baht, or offences against revenue law having a maximum fine not exceeding ten thousand baht, by the accused paying the fine as stipulated by the inquiry official;

(3) In the case of petty offences, offences having a fine not exceeding the petty offence fine, or any other offences *having a fine as the only penalty* and the fine is not exceeding ten thousand baht and the offence having taken place in Bangkok, by the accused paying the fine as nominated by the local police officer, ranked inspector upwards, or by the commissioned police officer in charge;

(4) In any other case subject to *any other laws*, by the accused paying the fine as stipulated by the competent officials." [Emphasis added]

Copyright offences penalty under CA 1994 § 69 paragraph one (primary infringement) and 70 paragraph one (secondary infringement) *have a fine as the only penalty*. However, penalty under CA 1994 § 69 paragraph two and 70 paragraph two carry both a fine and imprisonment. Copyright offences penalty under CA 1994 § 69 and § 70 provides:

Section 69: "Any person who infringes copyright or performers' rights under Section 27, 29, 30 or 52 shall be liable to a fine of between 20,000 baht and 200,000 baht.

If the offense referred to in the first paragraph is committed by way of trade, the offender shall be liable to imprisonment of between six months and four years or a fine of between 100,000 baht and 800,000 baht or both imprisonment and fine."

Section 70: "Any person who commits a copyright infringement under Section 31 shall be liable to a fine of between 10,000 baht and 100,000 baht.

If the offense referred to in the first paragraph is committed by way of trade, the offender shall be liable to imprisonment of between three months and two years or a fine of between 50,000 baht and 400,000 baht or both imprisonment and fine."

Copyright offences under CA 1994 § 69 paragraph one and 70 paragraph one are fallen into CRPC § 37(1) above because these offences *have a fine as the only penalty*. Therefore, at any stage of the prosecution prior to the court hearing, an alleged infringer may plead guilty and pays the maximum fine prescribed for these offences. This puts an end to the prosecution.[26] In this circumstance, it can be said that P2P copyright infringement offences allow a presumption of guilt although the fine penalty is much higher than typical minor offences. However, the very high maximum fines would rather attract innocence plea, especially when an internet account holder, not the real infringer, is accused of the infringement. Indeed, the problem of infringer identification for the purpose of fining here can be the same as the fining under CRPC § 37(4) which will be discussed below.

On the contrary, copyright offences under CA 1994 § 69 paragraph two and 70 paragraph two have penalty of both a fine and imprisonment; they are not classed as those in CRPC 1934 § 37 (1) above. Moreover, they are also not classed as offences under § 37 (2) and (3) because the provisions have fines from 10,000 to 800,000 baht (approximately £200 to £16,000) exceeding that of petty offences which is not exceeding 10,000 baht (approximately £200).[27]

CA 1994 is one of *other laws* under CRPC 1934 § 37 (4). It has a provision that allows settlement of criminal prosecutions. CA 1994 allows an accused infringer to pay the fine as nominated by the competent official -- the Director General of Department of Intellectual Property (DIP). Under CA 1994 § 77, the Director General is authorized to stipulate the fine for copyright offences. CA 1994 § 77 (as amended by CA 2015) states:

"The Director General shall be authorized to lay down the fine for offences under the first paragraphs of section 69, of section 70 and of section 70/1."

CA 1994 § 77 does not fit squarely with the nature of P2P infringement. The fine has to be assigned to a copyright offender. The Director General will not assign it to an allegedly infringing internet account holder in the cases where identification of the infringer cannot be produced. In computer-related crime cases an investigator can only

[26] The maximum fines are 200,000 baht (§69 paragraph one) (approximately £4,000) and 100,000 baht (§70 paragraph one) (approximately £2,000).

[27] PC 1956 § 102

search for an IP Address and seek for internet traffic data from an ISP.[28] The data supply leads to the telephone number used for the internet connection (by an internet account holder).[29] The investigator will then apply for a search warrant to the property.[30] There is normally no eyewitness who saw the incident in such a case.[31] Assigning the fine to an internet account holder can conflict with the presumption of innocence. So far, the Director General has never assigned a fine under this provision.[32]

In consequence, it must be concluded that presumption of guilt is available for copyright infringement offences but is not practical for authorities to impose a fine against an internet account holder, as opposed to the actual infringer who is not yet identified at the stage of the imposition.[33] Entitled to be settled by fines, copyright infringement charges, however, are not a minor offence because the fine is so high that guilty plea is unlikely to be gained. A right holder who needs to enforce his right has to resort to traditional prosecution or the CA 2015 mechanism.

5.2.4 Is Internet Suspension Criminal Penalty or Administrative Sanction in Thailand?

In Thailand, internet suspension has never been a criminal penalty. A person can be punished only by the penalties provided by the law. PC 1956 § 18 states:

"Punishments for inflicting upon the offenders are as follows:

1. Death;

2. Imprisonment;

3. Confinement;

4. Fine;

5. Forfeiture of property."

---

[28] Thailand, High-Tech Crime Unit, Royal Thai Police, n.d., "Guidance on Criminal Investigation of Technological Case" [Online]. Available at: http://www.hightechcrime.org/inv [Thai] [Accessed: 5 December 2015]

[29] *Ibid.*

[30] *Ibid.*

[31] Thailand, Office of Attorney General, n.d., *Criminal Proceeding Handbook for Computer-Related Crime*, p.39 [Thai].

[32] It should be noted that there is no Act, Ministerial Regulation, Notification or other regulation implementing the Director General's authority under CA 1994 section 77. (*See* Department of Intellectual Property, Thailand, website at: http://www.ipthailand.go.th/en/index.php?option=com_docman&view=docman&Itemid=272 [Thai] [Accessed: 4 December 2015])

[33] *See* 5.3.6 Taking Legal Action against infringers Subsequent to the Court Order and Problems of Proof in the Trial without Actual Infringer Identification below.

In principle, strict interpretation must apply in criminal cases. A person can be criminally liable and punished only if the offence and punishment are provided by the law.[34] There is no legislation providing internet suspension as a criminal penalty. The criminal court is not authorised to sentence any other punishments than (1) - (5) above. Therefore, the criminal court is not allowed to impose internet suspension. This principle applies similarly to administrative sanctions.

Administrative sanctions can be legalised to be supplemented to the traditional criminal punishments. Certain laws can state particular sanctions in their own legislation. For example, the Local Representative and Administrator Election Act B.E.2545 (2002) sections 118 and 119 stipulate the election right ban. Upon found guilty, a politician can be sentenced to prohibition of being an elective candidate for 5 or 10 years in addition to a fine and imprisonment. In order for internet suspension to be such a sanction, it has to be prescribed by the law. As CA 1994 and any other Thai laws do not have internet suspension as a sanction; therefore, it cannot be used as an administrative sanction by any institutions.

Internet suspension is therefore neither a criminal penalty nor administrative sanction any institution can inflict to a defendant. Whether it is an available option for the court injunctive order under CA 2015 § 32/3 is questionable. This issue will be discussed in section 5.3.5 The Court Order Relating to Internet Traffic and Connection below.

In this section, it can be concluded that internet access providers (IAPs) are the service providers responsible for the implementation of the court order because P2P copyright infringement takes place in their system. Thailand does not have legal mechanism to facilitate P2P online copyright enforcement such as internet subscriber duty and presumption of guilt. A court motion does not require real infringer and/or subscriber identification. An online copyright infringement count can be settled prior to the indictment only if an infringer is known. Finally, internet suspension and disconnection is not a criminal or administrative sanction in Thailand. Table 4 below summarises the findings of this section.

[34] PC 1956 § 2 paragraph one: "A person shall be criminally punished only when the act done by such person is provided to be an offence and the punishment is defined by the law in force at the time of doing of such act, and the punishment to be inflicted upon the offender shall be that provided by the law."

Table 4: Thailand's Online Copyright Protection Legal Mechanism for Peer-to-Peer Copyright Infringement

Country / Objects of Discussion	Thailand
1. Affected ISPs	- Access Service Provider[IAP] a kind of service providers under CA 2015 § 32/3 paragraph two (1)
2. Subscriber Duty to Monitor Internet Use	- No.
3. Presumption of Guilt	- Yes, for copyright infringement offences under CRPC 1934 §37(1)
4. Minor Offences	- No. A copyright infringer can be fined £400-4,000 under CA 1994 § 69 paragraph one (primary infringement), and £200-2,000 under CA 1994 § 70 paragraph one (secondary infringement), but minor offences generally carry a fine of £200 under the PC 1956.
5. Fine Imposed by Judges or Administrative Authorities	- Theoretically yes, by Director of DIP on breach of copyright ground. - Practically no, because the fine has to be imposed to the real infringer who is not identifiable.
6. Internet Suspension and Disconnection as a Criminal Penalty or an Administrative Sanction	- No.

Under the current CA 2015 mechanism, if it is reasonable to believe that the infringement has taken place within a service provider's computer systems, a right holder can file a motion to the court. The next section will discuss functional aspects of the Thailand CA 2015 in its application to P2P technology.

5.3. Functionality and Limitations of the Thailand Court Remedy in P2P Technology[35]

This section will interpret the 'necessary' and 'reasonable' criteria requisite to grant a court order in P2P matter. It will explore characteristics of 'reasonable' measures and will discuss how the 'reasonable' term is interpreted if the measures and method provided by the GR three strikes, e.g., mail warnings, criminal cases reference, internet traffic connection, are requested within the Thai context. Finally, the problems that arise when bringing legal action against infringers, if the court actually grants an order without actual infringer identification will be analysed. As we will see, the Thai court order can be even less effective and less efficient in P2P matters than when dealing with the client/server technology discussed in chapter 4.

5.3.1 Is a Court Order 'Necessary' in P2P Protection?

In chapter 4, this thesis concludes that interpretation of the word 'necessary' in CA 2015 can refer to the interpretation of 'sufficient' in traditional civil interim injunction provisions in the CIPC 1934 § 254-255.[36] The 'sufficient' ground under CIPC 1934 § 254, 255 and 'necessary' ground under CA 2015 § 32/3 paragraph four is interchangeable although CA 2015 § 32/3 does not explicitly state the 'sufficient' term.[37] These grounds are satisfied if a defendant intends to repeat or continue the infringement and the plaintiff's damage will continue.[38]

In chapter 3, this thesis concludes that P2P file sharing can constitute primary and secondary infringement by reproduction, adaptation and communication to the public of copyrighted works. P2P continual share of content, within a swarm, without permission, is the repeat or continued breach of copyright. Every user in the swarm intends to repeat and continue the infringement by making available exchanged bits of the content. Such acts of exchange damage copyright owners' interests and would continue unabated if no action were taken. This situation warrants the 'sufficient' cause and a court order is then

[35] At the time of this writing in 2015, CA 2015 has only been in effect for a few months. As yet there are no institutions interpreting the law in practice which might be of help in the study of this aspect. This section is an author's attempt to discuss the law functionality when it applies to P2P technologies.

[36] *See* Chapter 4 -- 4.3.2 Is a Court Order 'Necessary' in Online Copyright Infringement Especially in the Client/Server Platform?

[37] *Ibid.*

[38] CIPC 1934 § 255 (2) (a) and (b)

'necessary' for the prohibition of the sharing. The next question though is what measures fit the P2P infringement which are 'reasonable' and 'cease' the infringement? These issues will be addressed further below.

5.3.2 Specific Characteristics of 'Reasonable' Measures in P2P Circumstances

The 'reasonable' term is prescribed in CA 2015 but not in CIPC § 254 and § 255. However, in its application, the Supreme Court is consistent in using 'reasonableness' in its deliberations for permitting or negating an injunction under CIPC § 254 and 255.[39] CIPC §254 injunctions are straightforward. The Court applies them simply in accordance with the plaintiff's claims, e.g., to prohibit the sub-letting act, to stop transfer of the property to the third party, etc.[40] CA 2015 § 32/3 injunctions embody removal of the content and cessation of infringement. A P2P injunction falls within the cessation of infringement method. Reasonable cessation injunctions are very similar to the CIPC §254 injunctions but are relatively more complicated in many respects.

Under the CA 2015 §32/3, to successfully apply for an injunction requires appropriate technical knowledge, e.g., how P2P technology works, where content is reproduced, adapted or made available, what functions of ISPs are, how an injunction stops P2P distribution.[41] Chapter 4 concluded that the words 'cease the infringement' can be associated with any method that stops an on-going piracy. The Thailand Supreme Court precedents confirm that the injunctions and the circumstances have to be 'reasonable'. For online copyright infringement, the 'reasonable' injunctive measures ought to accommodate factors such as proportionality, freedom of speech, right to privacy and balance of public right and copyright. P2P has similar problem to client/server as discussed in chapter 4 in that it is likely but unclear as to whether or not the court can take these factors into consideration before granting the order.[42]

---

[39] Also used within the same reason are 'sufficiency' and 'necessary' terms. (*See* Supreme Court case nos.704/B.E.2545 (2002) 1415/2499 (1956) 1868/B.E.2548 (2005) in chapter 4 -- 4.3.2 Is a Court Order 'Necessary' in Online Copyright Infringement Especially in the Client/Server Platform?)

[40] *Ibid.*

[41] *See* chapter 4 -- 4.3.4 Limitations of the Thailand CA 2015 § 32/3 Court Procedure and Remedy.

[42] This thesis suggests that the word 'reasonable' should be followed by examples for consideration by the court in its deliberations. (*See* chapter 6 -- 6.4.4 Recommendations Regarding Thailand Court Proceedings.)

Moreover, a court measure can be granted even if the real infringer is not identifiable.[43] The question is how these characteristics can be assembled to be a 'reasonable' measure in a P2P situation. Indeed, a 'reasonable' measure has to be defined individually, measure by measure. For comparative purpose, measures and methods provided in GR are raised as examples in analysing whether or not a court order containing GR measures 'ceases the infringement' and is 'reasonable'.

5.3.3 The Court Order Measures for Graduated Response's Three Strikes

At present, Thailand does not have a duty to monitor internet use or the establishment of a presumption of guilt in minor offences.[44] A measure is imposed upon an ISP, who is then directed to an account holder. However, a request similar to GR's three strikes system is of interest. The first strike is an email, the second a registered mail. The mailing notices contain useful information about internet fraud.[45] They simultaneously educate subscribers. These notices can be followed by a third strike -- case reference to authorities. GR increases sanctions gradually, and hence seems to satisfy the 'reasonable' criterion.

For the first and second strikes, if a right holder files a motion and requests an informative email followed by a registered mail, the court can rule on the motion in different ways. The court may find that P2P infringement is replete and widespread. Educative and informative notices can be helpful in raising P2P user awareness. This possibly triggers an improvement in users' morale, decreases subsequent infringing acts and screens hard core infringing users from intermittent users. In effect, the mailings could ultimately reduce the number of online infringements and of infringement cases. On account of all these aspects, orders can be granted as they satisfy both 'cessation' and 'reasonableness' criteria.

On the other hand, the court may find that notices do not 'cease' the infringement. They cannot be described as a straightforward measure that bans P2P users from committing file sharing. P2P users are warned of potential P2P file sharing infringement.

---

[43] *See* discussion in 5.2.3 Does Thailand Law have Presumption of Guilt and Do Copyright Infringement Charges Constitute Minor Offences? above.

[44] *See* 5.2.2 Does Thailand Law have Internet Subscriber Obligation and Does the CA 2015 Motion Need to identify the Subscriber? above.

[45] *See* 5.5.3 HADOPI Act Procedure in P2P Deterrence below.

They may or may not follow the mail's instruction. Right holders have no way to prove if the mails effectively control users until an order is granted. Regarding these points, the court is unlikely to rule that the notices 'cease' the infringement and are 'reasonable'; hence there may be a refusal of a first and second strike request.

Indeed, it is uncertain that the request merely to send mails and emails to subscribers will result in the cessation of infringement. Raising awareness is actually a long term solution which a right holder may not welcome when filing a motion. A measure that instantly stops online sharing is more likely to be suitable for the fight against on-going infringing activities. The request accompanied by information that the third strike or criminal prosecution can follow may yield improved results. A petitioner can advance the idea that the notices themselves are not the deterring factor but that the subsequent prosecution is. Users afraid of it may stop doing their illegal activities at the warning stage. In effect, this brings about the cessation of the infringement. In addition, in cases where the court allows warning mails to be processed, but the warning mails prove unsuccessful, the right holder can then lodge a complaint to the authorities. As a result, the subsequent prosecution can also lead to the cessation of infringement. If a description of this method is given, the court may rely on it and find the method 'reasonable'. However, filing a court order which incorporates GR measures is not compatible with the current practice in a Thailand context. The next subsection will analyse this issue.

5.3.4 The Practical Aspect of Graduated Response's Three Strikes in the Context of Thailand Proceedings

Granting a court order which incorporates the requirements of GR is theoretically possible, though ambiguous. From a practical point of view, the proceedings seem complicated under the current Thai digital copyright enforcement system.

For the first and second strikes, normal practice teaches us that a creditor does not need any permission via a court to send a notice to a debtor. Hence right holders are fully entitled to send 'cease and desist' letters to anyone who they find infringing their rights. To send the letters, a court subpoena is needed to reveal suspected users in civil cases. However, under the Thai court procedure, a claimant cannot file the subpoena until he

files the claim.[46] It is possible that a court motion under CA 2015 § 32/3 can also be used as a tool to reveal a subscriber. A wise right holder can file a § 32/3 motion without having to identify the user. In the same motion, the right holder can also request the subpoena claiming that she must institute the main infringement legal action if the order is granted. Under the current Thai system, a right holder cannot avoid entering into a lawsuit even if she only wants to send a cease and desist letter to the allegedly infringing account holder.

With regard to the third strike, currently in Thailand a right holder does not need a court order to refer the case to the criminal authorities. The right holder does not need to ask any institution to pursue a criminal case. Copyright charges are a compoundable offence.[47] In pursuing public prosecution, a right holder is an injured person who can initiate criminal action by lodging a complaint with the inquiry official. The inquiry official investigates to find who the actual infringer is, interrogates witnesses and collects evidence in support of the allegation. The dossier and evidence will later be handed to a public prosecutor. The right holder does not need to do much at all. In view of this a right holder is unlikely to file a court motion requesting a GR third strike.

It can be concluded that all the GR's three strikes are theoretically possible, but in the author's opinion, not functionally practical in a Thailand context. Thai right holders are likely to prefer using public prosecution than the CA 2015 § 32/3 regime because criminal proceeding on part of an injured person is clearly simpler than that of CA 2015 motion litigation. The HADOPI Act offers another sanction, namely, internet suspension on an account holder. It is important to examine if such a choice is available in a CA 2015 § 32/3 motion.

5.3.5 The Court Order Relating to Internet Traffic and Connection

This subsection discusses whether internet traffic management, internet disconnection and suspension is an available option for the court injunctive order under CA 2015 § 32/3 in the circumstance where a real infringer is not identifiable. In other words, it discusses if these measures 'cease' the infringement and are 'reasonable' under

[46] CIPC 1934 § 123

[47] CA 1994 Section 66: "An offense under this Act may be subject to settlement."

CA 2015 § 32/3. Traffic management, internet disconnection and suspension of internet use are different in certain aspects.[48]

Traffic management (internet speed reduction or traffic shaping) is a way IAPs prioritise one type of traffic over others.[49] It is argued that the court order for internet traffic management 'ceases' the infringement and is 'reasonable'. If so requested and ordered, a subscriber is unable to use P2P file sharing. This definitely 'ceases' the infringement. Alternatively, a subscriber is able to use it in a delayed mode. This does not directly 'cease' the use of P2P file sharing. It dramatically discourages such use which is in effect the cessation of it. Either disabling P2P completely or reducing its P2P does not disturb other internet activities, e.g., emailing, browsing, internet phone calls.[50] An exercise of freedom of speech does not affect. Therefore, traffic management can pass the 'reasonable' threshold.

Internet disconnection is a possible court order. Internet disconnection is practiced by an ISP in certain circumstances and is part of the terms of subscription.[51] Disconnection unquestionably 'ceases' P2P application. It is argued that disconnection is also a 'reasonable' order. Copyright infringement is a similar ground for disconnection to other grounds, e.g., one-month non-payment of subscription fee. A household account, as opposed to company or institution accounts, is limited in its number of users. The disconnection court order affects only members of the household, not many people. Furthermore, even if disconnected by a current ISP, an internet account holder or other member of the household can apply for another subscription. Therefore, disconnection injunctions can be held proportionate and is likely to be found 'reasonable'.

Whether internet suspension is an available option for the court order is questionable. Suspension injunction does not only disconnect an account from accessing the internet but it also disallows new subscribing for a certain period. These affect fundamental rights offered by internet access in a long term. Had CA 2015 § 32/3

---

[48] *See* Chapter 2: -- 2.3.2 Suspension and De-subscription of an Internet Account *and* 2.3.3 Traffic Management.)

[49] Broadband Stakeholder Group, 2013, "Broadband providers launch new traffic management transparency code" [Online] Available at: http://www.broadbanduk.org/2011/03/14/broadband-providers-launch-new-traffic-management-transparency-code/ [Accessed: 2 July 2014]

[50] Wisegeek, n.d., "What is Traffic Shaping?" [Online] Available at: http://www.wisegeek.com/what-is-traffic-shaping.htm [Accessed: 4 July 2014]

[51] *See* Chapter 2: -- 2.3.2 Suspension and De-subscription of an Internet Account *and* 2.3.3 Traffic Management.)

provided factors for consideration, suspension injunctions would have been held disproportionate and unlikely to be found 'reasonable'.[52] Be it as it may, the 'reasonable' factor is likely to exclude internet suspension order.

In conclusion, internet traffic management and internet disconnection orders are potentially granted but the internet suspension order is not. Even if the court grants an order for the sending of the two mails followed by prosecution and internet traffic management, there will still be a main infringement court case according to CA 2015 §32/3 paragraph four. The next subsection will analyse the court order status, the situation after the order is granted and proof of online infringement cases.

5.3.6 Taking Legal Action against infringers Subsequent to the Court Order and Problems of Proof in the Trial without Actual Infringer Identification

The last sentence of CA 2015 § 32/3 paragraph four states: 'After the court order, the right holders shall take legal action against the infringer within the time designated by the court for such cessation or removal.' This implies that failing to do so, the order lapses.

The words 'take legal action' do not specifically state whether the legal action is civil or criminal action. This means that the 'legal action' can be any type of action. To take legal action in a civil case, a right holder may file a lawsuit against an internet account owner alleging that the owner infringes copyright. For a criminal case, a right holder may lodge a complaint to an inquiry official.[53] These actions satisfy the term 'taking legal action'. What seems to be the problem is the proof of actual infringer identification. CA 2015 § 32/3 paragraph four uses the word 'the infringer' where it really means an alleged infringer as the infringer at this stage is yet to be proved as such.

In civil cases, the alleged infringer is presumably an internet account holder because infringement is found using the internet account. Even so, a lawsuit against an internet account holder is not easily successful. The court will decide on the

---

[52] The factors are, e.g., freedom of speech and other fundamental human rights. (*See* chapter 4 -- 4.3.4 Limitations of the Thailand CA 2015 § 32/3 Court Procedure and Remedy.)

[53] The inquiry official will then have a duty to investigate, collect evidence and submit the case for prosecution. Alternatively, a right holder can initiate private criminal prosecution by filing the indictment to the court directly under Criminal Procedure Code B.E.2477 (1934) (CRPC 1934) section 28 provides:

"The following persons are entitled to institute criminal prosecution in Court:
(1) the public prosecutor;
(2) the injured person."

preponderance of evidence (or balance of probability) whether it believes such holder is actually the infringer.[54] As far as the right holder can prove, evidence at hand may simply assert that infringement took place by using the internet account holder. This evidence may be sufficient to win the case unless the account holder proves otherwise, e.g., he was not using the internet, not using the identified device, or not in the house at the time of infringement. The account holder can counter the claim in various ways. It is not certain that the right holder will win the case.

In criminal cases, the standard of proof is higher than that of civil cases. The 'proof beyond reasonable doubt' standard tends to thwart an criminal prosecution in a computer-related offence.[55] Proof of a wrong doer is difficult when the offence is committed in a private property. It is the fact that even members of the property may not know. A litigant can only secure an IP address or an internet account holder information.[56] In online copyright offence, an account holder and an infringer can easily escape from the conviction if the proof is merely that infringement is found using his internet account. In a computer-related crime case below, the Supreme Court ruled that mere proof of an IP address attached to an identified account holder does not prove beyond reasonable doubt.

In Supreme Court case no. 2492/B.E.2558 (2015), a defendant was prosecuted on a *lese majeste* count.[57] She allegedly posted and disseminated insulting and defamatory comment about Thailand's Queen on a news web board. The Court of the First Instance dismissed the count because there was no witness who actually saw her posted the comments. The judgment was reversed in the Court of Appeal. The defendant petitioned to the Supreme Court. The Supreme Court agreed with the Court of the First Instance in

---

[54] CIPC § 104 paragraph one stipulates: "The court has the whole authority to consider whether evidence delivered by parties relates to the facts in the case and is sufficient, and adjudicate accordingly"

[55] CRPC § 227 provides:

"The Court shall exercise its discretion in considering and weighing all the evidence taken. No judgment of conviction shall be delivered unless and until the Court is fully satisfied that an offence has actually taken place and that the accused has committed that offence.

Where any *reasonable doubt* exists as to whether or not the accused has committed the offence, the benefit of doubt shall be given to him." [*Emphasis* added]

[56] *See* chapter 2 -- 2.4 Infringement Detection and Identification.

[57] *Lese majeste* is a criminal charge for insulting the Thai royal family as enshrined in the Thailand Constitution and PC. PC section 112 states:

"Whoever, defames, insults or threatens the King, the Queen, the Heir-apparent or the Regent, shall be punished with imprisonment of three to fifteen years."

dismissing the case reasoning that an IP Address alone could not prove that the defendant posted the comment.[58]

The case above discussed the importance of IP address which also needs to be supported by other evidence. This case sets the precedent of computer-related crime cases including online intellectual property infringement cases. Where there is no eye witness and there are other people who can use the computer in question, the prosecutor has to prove that there is an illegally-reproduced musical file in a defendant's computer.[59] Moreover, it was the defendant, not someone else, who reproduced the file onto the computer.[60] It is common to this computer crime where eye witness cannot be found. In this circumstance, concrete circumstantial evidence needs to be adduced, e.g., a user name registered in a website, the owner of a telephone number and computer forensic. Fingerprint, DNA and other forms of biotechnology proof may infer.[61] These facts must support each other.[62] All of these complicate the criminal proceedings and are not practical in a user prosecution. Without these, conviction cannot be secured.

In consequence, there will be problems with taking legal action against an infringer subsequent to the court order. The problems involved are less with the constitution of the legal action but more with the proof of actual infringer identification. Without such proof or concrete circumstantial evidence, the defendant-liable judgments of both civil and criminal cases cannot be held.

In this section, it can be concluded that the Thai court order is 'necessary' in P2P file sharing because of continuation of content availability and right holder damage. A P2P injunctive request falls into the 'cessation of infringement' category. The 'reasonable' extent of the order that ceases the infringement requires knowledge of P2P technology. CA 2015 § 32/3 does not provide factors for 'reasonable' consideration, e.g.,

---

[58] *See also*, ILaw Freedom, 2015. "October 2015: Famous people and police arrested for *lese majeste* case, giving flowers charged for sedition and journalists were summoned." [Online] Available at: http://freedom.ilaw.or.th/en/report/october-2015-famous-people-and-police-arrested-lese-majeste-case-giving-flowers-charged-sedit [Accessed: 16 February 2016].

[59] Supreme Court case no.3054/B.E. 2548 (2003)

[60] Supreme Court case nos. 3054/B.E. 2548 (2003), 3882/B.E.2553(2010) and 2492/B.E.2558(2015)

[61] "DNA, or deoxyribonucleic acid, is the hereditary material in humans and almost all other organisms. Nearly every cell in a person's body has the same DNA." (US, National Library of Medicine, 2016, "What is DNA?" [Online] Available at: https://ghr.nlm.nih.gov/primer/basics/dna [Accessed 1 September 2016].

[62] Supreme Court case no. 2492/B.E.2558(2015)

proportionality, freedom of speech. A motion requesting for GR-type first and second strikes (mail notifications) is not certain to be granted but a motion associating the first two strikes with the third strike (criminal prosecution) is more certain. These three strikes are unlikely to have practical application in the Thailand context because criminal proceeding is simpler. Internet traffic management and internet disconnection injunctive orders are potentially granted but the internet suspension order is not. Finally, there is the problem of taking legal action, as required by the law, against an alleged infringer and of proof in such a legal action. The problems exist in both civil and criminal cases. Table 5 summarises the CA 2015 functionality in application to P2P user infringement.

Table 5: Thailand Functional Remedy and Limitation in Application to P2P Technology

Country / Objects of Discussion	Thailand
1. Warning Notifications	1. By a right holder herself: -Theoretically, yes. - Practically, no, because the account holder is unknown. - a court subpoena is needed to reveal the internet subscriber identity. 2. By the court order - Not certain (the 'cessation' ground) - Notification and then criminal prosecution request is possible, but not practical
2.Internet Traffic Management/Suspension/ Disconnection	-The court order for internet traffic management and disconnection potentially satisfies 'reasonable' (proportionality) grounds. - Internet suspension is disproportionate.

The above table summarises functionality and limitations of the Thailand court remedy in P2P technology. The analysis and conclusion made in chapter 4 -- 4.3.4 Limitations of the Thailand CA 2015 § 32/3 Court Procedure and Remedy can contribute to this section as functionality and limitations of the Thailand court remedy in general. The court procedure for P2P protection has limitations similar to those of client/server and other online infringement. The limitations are inherent in the three stages of any case --

the case preparation of the motion, the case trial and the case decision.[63] In consequence, it is predictable that the Thai court procedure will rarely be chosen as an option by right holders. GR employs measures which circumvent the use of the court. It introduces a new regime which is desirable for Thailand's digital copyright enforcement framework in many respects. The advantages of GR will be discussed in the next section.

5.4. Functionality of the Graduated Response System of France

The purpose of the Graduated Response (GR) system of France is both educational and suppressive.[64] Professor Geiger commented in his work:

"The systems[GR] known as the 'graduated response' are amongst the means that have been frequently presented by legislators and copyright industries as being the most effective for combating illegal file sharing."[65]

This section will discuss functional aspects of GR. It will begin with ISP involvement in the GR processes. GR's desirable aspects include subscriber duty, informative and educative notices and graduated sanctions which this section will discuss. The court interpretation of the other aspects such as reverse burden of proof and termination of internet access will also be critically analysed. These discussions will be prefaced by an analysis of ISP involvement in the GR system below.

5.4.1 ISPs Are Less Involved in the Graduated Response System

There are many kinds of ISPs that implement a P2P application. IHPs host the content and applications provided by ICPs. Napster provides a central register application in a website and Kazaa provides P2P software.[66] Both Napster and Kazaa are ICPs.[67] When

---

[63] *See* Chapter 4 -- 4.3.4 Limitations of the Thailand CA 2015 § 32/3 Court Procedure.

[64] Rambaud, S. 2010. "Illegal internet file downloads under HADOPI 1 and 2" [Online] Available at: http://www.twobirds.com/en/news/articles/2012/france-struggle-against-illegal-downloads-050510 [Accessed: 6 January 2016]

[65] Geiger, C. 2014, "Challenges for the Enforcement of Copyright in the Online World: Time for a New Approach," *Max Planck Institute for Innovation and Competition Research Paper No.14-01* [Online] Available at: https://www.researchgate.net/publication/260791463_CHALLENGES_FOR_THE_ENFORCEMENT_OF_COPYRIGHT_IN_THE_ONLINE_WORLD_TIME_FOR_A_NEW_APPROACH p.5 [Accessed: 28 October 2015]

[66] Conradi, M. 2003. "Liability of an ISP for allowing access to file sharing networks", *Computer Law & Security Report*, 19, 4, p.293.

[67] Shutting down websites, or ICPs, is not "a way to reduce consumption of pirated media content and increase licensed consumption." (Aguiar, L. et. al., 2015 "Online Copyright Enforcement, Consumer Behavior, and Market Structure" [Online] Available at:

---

the copyright content is actually exchanged, ICPs and IHPs are not involved because the exchanged content is stored in users' computers and is delivered directly from those computers. These ISPs are not affected by the GR procedure. On the contrary, IAPs are involved in GR because they offer subscribers an internet access. IAPs are required to process notifications by the HADOPI Act.[68] However, IAPs are not responsible for their subscriber copyright infringement. An internationally accepted standard is that mere conduit IAPs are not responsible for transmitting information if the information is not initiated, directed, or modified by IAPs.[69] The safe harbour concept does not apply in GR. GR measures are based on another concept, the so-called internet subscriber duty. The question is to what extent a subscriber's default of such duty can be proven and/or sanctioned. It is the burden of proof imposed on a subscriber and the sanctioning authority given to Hadopi that French courts did not approve.

5.4.2 Is a Subscriber's Reverse Burden of Proof Legitimate?

A criticism of GR is that it is insufficient due process.[70] In particular, the appeal process "looks like a guilty-until-proven-innocent schema".[71] Under HADOPI Act 1 article L. 331-38 paragraph two, Hadopi could impose criminal sanction on a subscriber if the said subscriber could not disprove.[72] HADOPI Act 1 article L. 331-38 paragraph two provided:

"Concerning measures pronounced by the committee for protection of rights in applying article L. 331-27, this decree specifies in particular the conditions under which the exercise of the rights of defence guarantees, in an effective way, respect for the principle of personal responsibility of the subscribers penalized. To this end it defines the conditions under which may be produced for use, at each stage of the procedure, all

---

http://druid8.sit.aau.dk/druid/acc_papers/khu2mchxelh7g4fvnc9pio6cdh71.pdf [Accessed: 16 September 2015]

[68] FIPA Article L. 331-26 paragraph one provides: "Where facts likely to constitute a breach of the obligation defined in Article are referred to the Rights Protection Commission, it may send to the subscriber, under its seal and on its own behalf, by email and through *the person whose activity is to offer access to public online communication services* and that has entered into a contract with the subscriber, …" [Emphasis added]

[69] Directive 2000/31/EC of the European Parliament and of the Council on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (E-Commerce Directive) § 12, and the US DMCA § 512 (a)

[70] Elton, S. 2014. "A Survey of Graduated Response Programs to Combat Online Piracy," *Journal of the Music & Entertainment Industry Educators Association.* 14(1), p.99. Available at: http://www.meiea.org/Journal/Vol.14/Elton-MEIEA_Journal_vol_14_no_1_2014-p89.pdf [Accessed: 6 July 2016]

[71] *Ibid.*

[72] For example, the subscriber has secured his access, the internet account was fraudulently accessed, force majeure. (HADOPI Act 1 Article L 336-3 paragraphs 2-5)

elements that may establish that he has put into use one of the methods of security on the list mentioned in the second paragraph of article L. 331-32, that the violation of the right of authorship or a related right is the act of a person who has fraudulently used access to the public on line communication service, or the existence of *force majeure*."

It was argued that article L. 331-38 paragraph two was against presumption of innocence because it assumed guilt on a subscriber who was repeatedly in default of his duty after the process of warning. The French constitutional court adjudicated the challenges. Constitution Tribunal Decision no. 2009-580 ruled against the burden put on a subscriber that the article reversed the burden of proof in criminal cases. Such reverse burden of proof was only acceptable in minor offences. A subscriber duty offence was not a minor offence because it incurred suspension of internet access. Internet access was crucial and was part of freedom of speech, a fundamental right guaranteed by the Constitution. Moreover, it was Hadopi, a regulating organization, not the Court, which imputed such sanction. Therefore, Article L. 331-38 paragraph two and Article 336-3 paragraphs 2-5 were held unconstitutional.[73]

The Constitutional Court rightly dismissed Article L. 331-38 paragraph two and confirmed the world-accepted presumption. "The general principle in civil law systems and common law is that the burden of proving the defendant's guilt should be on the prosecution and that guilt must be proven beyond reasonable doubt and not by a balance of probabilities."[74] The general principle has exception -- presumption of fact or of law -- which operates in every legal system.[75]

In Europe, the European Court of Human Rights held in *Salabiaku v. France, Publ.*, that the presumption of fact or of law is possible under the European Convention on Human Rights, Article 6 (The Right to Fair Trial) within certain limits regarding criminal

---

[73] The French Constitutional Council Decision no. 2009-580, *op.cit.*

[74] Durrieu, R.F, n.d, "Terrorism, organized crime, drug trafficking and due process", [Online] Available at: https://translate.google.co.uk/translate?hl=en&sl=es&u=http://www.estudiodurrieu.com.ar/articulo_2013_03_21.html&prev=search [Accessed: 10 October 2015]

[75] *Salabiaku v. France, Publ. ECHR*, Judgment of 7 October 1988, [Online] Available at: https://www.coe.int/t/dghl/cooperation/economiccrime/corruption/projects/car_serbia/ECtHR%20Judgements/English/SALABIAKU%20v%20FRANCE%20-%20ECHR%20Judgment%20_English_.pdf paragraph 28. [Accessed: 10 October 2015]

law.[76] The presumption of fact has to be exercised in such a way that allows an accused to disprove the presumption for particular exceptions such as *force majeure*.[77]

In the US, the US Supreme Court in *Morissette v. United States,* 342 U.S. 246, allowed an exception to general criminal due process guaranteed under the Fourteenth Amendment in the area of public welfare offences including traffic regulation.[78] A registered car owner whose car is illegally parked can be under the presumption of guilt as it is not practical for a state to prove the facts.[79] Moreover, offences which are not minor can introduce presumption of guilt if such offences are driven by political will. An offence of money laundering assumes that a convicted person of a main criminal case benefits from the proceeds of illegal activities.[80] The convicted person must prove that the proceeds were earned by legitimate business.

Minor offences and policy-focused offences can be applied to presume particular facts or guilt. The accused can reject the allegation, in which case he is given a chance to contest in court to disprove the presumed facts. It is certain that online copyright infringement and breach of subscriber duty can be made a policy-focused minor offence if a state so wishes. The question is how to characterise the offence.

Offences can be considered minor offences by their very nature.[81] Other offences which are not minor in themselves may be regarded as minor because of the particular facts of the case, for example, theft of low monetary value property.[82] Online copyright infringement can be classed as both minor and serious offences.[83] It will depend on the particular facts of the case, e.g., if infringement causes a lot of damage, if it is for commercial gains or for personal enjoyment, or if it is committed intentionally or out of negligence. Commercialization without permission can be a serious offence. It is

---

[76] *Ibid.*

[77] *Ibid.,* paragraph 29.

[78] *Commonwealth v. Rudinski,* 382 Pa. Super. 462, 464-465 (1989)

[79] Lippma, M., 2010. *Contemporary Criminal Law: Concepts, Cases, and Controversies*, Los Angeles: Sage Publications. pp.172-173.

[80] Stessens, G., 2004. *Money Laundering: A New International Law Enforcement Model*, Cambridge: Cambridge University press. pp.71-72.

[81] UK, The Crown Prosecution Service, "Minor Offences" [Online]. Available at: http://www.cps.gov.uk/legal/l_to_o/minor_offences/ [Accessed: 10 October 2015] (*See also* The French Constitutional Council Decision no. 2009-580, *op.cit.* p. 2.)

[82] *Ibid.*

[83] *See* chapter 3 -- 3.3 Are Client/Server and Peer-to-Peer User Activities Criminal Offences under Copyright Act B.E.2537 (1994)?

undoubtedly illegal exploitation of another's work. Under Thai and international standards, this act can lead to imprisonment or a high amount of indemnity in a civil case. Moreover, commercial file-sharing can result in a criminal court penalty of internet access blocking under the French Decree 2013-596 of 8 July 2013.[84] Therefore, in order for an online copyright infringement offence or a breach of internet monitoring duty offence (for online copyright protection purposes) to be characterized as a minor offence, it must not have an element of commercialisation. With this in mind, an offence can be subject to presumption of fact or of law which an amount of fine can be imposed by an administrative authority or by a single judge with a summary procedure.

On the 8th of July 2013, the French government amended FIPA by Decree 2013-596. According to the amendment, a file sharing with no-commercial aspect is a minor offence.[85] The offence does not have to have detailed proof and internet suspension is not an available penalty.[86] This situation is now considered to be a more favourable step in support of copyright. It states that upon detection, the offence of breach of internet monitoring duty is to be settled by an automatic fine of less than 1500 Euros.[87] The automatic fine is considered to be an adequate response to a minor offence. The offence allows the reverse burden of proof in accordance with the French Constitutional Council's ruling.

It can be concluded that the minor offence concept could be introduced into internet subscriber duty and/or online copyright protection. This approach can divert the lengthy court procedure by presumption of fact and a minimal amount of fine is implemented through an administration or a court summary procedure. A question is raised: should there be any warning prior to the imposition of a fine and would any other sanction followed be appropriate? There are two aspects of GR measures that can be considered as warning and sanctions: (1) mail notification; and (2) internet suspension as supplementary to criminal sanction. The latter aspect will be discussed later in this chapter. The former, a mail warning is not contentious. However, it was challenged

[84] Torremans, P., ed., 2014. *Research Handbook on Cross-border Enforcement of Intellectual Property*. Cheltenham: Edward Elgar. note 512 p.298.

[85] *Ibid.*

[86] *Ibid.*

[87] A fine can be made to be part of a copyright royalty fee as a commentator proposed. (Serbin, D. 2012. "The Graduated Response: Digital Guillotine or a Reasonable Plan for Combating Online Piracy?" *Intellectual Property Brief*, 3(3), 42.)

because it was considered unsupportive of the presumption of innocence principle. This aspect is discussed below.

5.4.3 Does Mail Notification Conflict with Presumption of Innocence?

There were challenges against mails notification made through the French administrative court -- the *Conseil d'Etat* (the Council of State).[88] In case N° 342405, French Data Network (FDN) filed a case to annul Decree no. 2010-236. It was argued that a mail sent to a subscriber alleging breach of duty on the part of such subscriber was against the presumption of innocence principle. The court essentially ruled against this challenge in two respects.[89]

Firstly, that a warning email/mail is neither a sanction nor an accusation. It gives information to users. It also reminds users of an obligation. Its purpose is "to state the factual record of certain data that could reveal a breach of the duty to secure its access to the internet covered by Article L. 336-3 of the Code of Intellectual Property".[90] Moreover, the warning informs the internet users concerned by merely reminding them of the law, of the obligations incumbent on them in the application of the provisions of the Intellectual Property Code.[91] The Council of State ruled that mere sending of notices to subscribers did not affect the presumption of innocence.[92]

Secondly, the third warning is to invite an alleged subscriber to rebut the accusation and warn him of possible prosecution. If illegal downloading practice is renewed and a subscriber is actually prosecuted, the system guarantees a fair trial before a judge.[93] Subsequent to such a prosecution, the facts noted in the warning letters can be

---

[88] The terms 'mails' in this section, unless otherwise indicated, represents the first and second mails which are an email and the registered mail accordingly. (*See* 5.5.3 The HADOPI Act Procedure in P2P Deterrence below.)

[89] The Council of State case No. 342405 Available at: https://translate.google.co.uk/translate?hl=en&sl=fr&u=http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-octobre-2011-French-Data-Network-n-342405&prev=search [Translated by Google Translation][Accessed: 5 October 2015]

[90] *Ibid.*

[91] Blocman, A. 2011. "State Council Confirms Legality of the HADOPI Decrees" [Online]. Available at: http://merlin.obs.coe.int/iris/2011/10/article15.en.html [Accessed: 1 July 2016].

[92] Graduatedresponse.org, n.d., "France"[Online] Available at: http://graduatedresponse.org/new/?page_id=24 [Accessed: 1 July 2016]

[93] France, The State Council, 2011. "The Council of State rejects requests from Apple Inc and French Data Network against the decrees *Hadopi*"[Online]. Availble (in English by google translation) at:

---

contested.[94] Therefore, the mail-warning system is not classed as a penalty and does not interfere with the right to a fair trial or with the presumption of innocence principle.

As established by the court, mails actually function as an informative and educative notice as well as a warning notice. The mails are informative because they give information about how to protect users from fraudulent internet use and how to legally acquire a source of copyrighted content.[95] Information about time and date of detected infringement is also mandatorily provided.[96] The mails are educative because they teach users what copyright is and how infringement of copyright affects the economy.[97] Lastly, the warning function reminds users of their obligations to secure their internet use and of the potential sanctions to follow.[98] These mails invite the recipients to respond to Hadopi regarding the accusations.[99] All these functions not only raise users' awareness, they also enhance the enforcement of online copyright.[100] The characteristics of GR mails can be

---

https://translate.google.co.uk/translate?hl=en&sl=fr&u=http://www.nancy.cour-administrative-appel.fr/Actualites/Communiques/Decrets-Hadopi&prev=search [Accessed: 1 July 2016].

[94] *Ibid.*

[95] Language of the first mail contains:

"Information

· You can consult the site of the Hadopi www[.]hadopi[.]fr to obtain information about its missions, the applicable mechanism, the legal offer and the methods of security.

· You can also ask for information about the methods of security to you [sic] Internet service provider."

(*See* translation of the first notice in Trillet, G.V.R. 2012, *Liability and Evidence in case of Infringement of copyright of the internet: A Legal Comparison between Belgium and France.* LL.M. thesis, Tilburg University, Appendix VII and VIII, Available at: http://arno.uvt.nl/show.cgi?fid=127512 [Accessed: 22 October 2015])

[96] Language of the first mail contains:

"· Sworn agents have noticed that on the xxxxx one or several copyrighted works were reproduced, consulted or offered for sharing from the Internet access matching the IP address No. xxxxxxxx.

· By that time, this address had been allocated to the company xxxxx, your Internet service provider, to: [name and address]" (*Ibid.*)

[97] Language of the first mail contains:

"Why protect the authors' right?

Under the seducing guise of gratuitousness, the practices that do not respect the copyright of the works deprive, indeed, the creators of their fair remuneration. They represent a grave danger for the economy of the cultural sector and the survival of the artistic creation relies on it, in all its form, which is at stake. To better conciliate the advantages of the Internet and the respect of creation, we remind you that today online services put forward legal offers that are attractive and respectful of the creators' rights." (*Ibid.*)

[98] The Council of State Case N° 342405

[99] UK, Intellectual Property Office, 2015. *International Comparison of Approaches to Online Copyright Infringement: Final Report,* [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/404429/International_Comparison_of_Approaches_to_Online_Copyright_Infringement.pdf p.48. [Accessed: 25 October 2015]

[100] Ofcom of the UK has advised its government that online piracy strategy can be effective if it has well-monitored educational enforcement measures and readily available legitimate digital services to consumers. (Hargreaves, I., 2011. *Digital Opportunity, A Review of Intellectual Property and Growth, An Independent Report*.[Online] Available at:

---

viewed as desirable elements which benefit copyright. France employs mail notification of a subscriber's duty which indirectly serves copyright protection purposes.

The next issue regards the second part of GR sanction which can be used in addition to a criminal fine. Internet suspension can be imposed in cases which are referred for prosecution. The sanction of internet suspension is controversial not only in France but also worldwide. This issue is discussed in the next section.

5.4.4 Should Termination of internet access be Supplementary to Minor Offences?

This subsection discusses if termination of internet access can be classed as proportionate under a copyright enforcement paradigm, if such termination can be imposed by law or by contractual obligation stated in subscriber-ISP agreements and if it can be supplemented to minor offences.

HADOPI Act 1 penalises P2P repeat infringers in the third warning.[101] It allows HADOPI to impose a sanction of internet suspension lasting from two months to one year and it includes the prohibition of a subscriber from contracting with other online access operators.[102] Constitution Tribunal Decision no. 2009- 580 ruled that internet access is part of fundamental rights and suspension of internet access can only be imposed by a court. The ruling stated:

"[I]n view of the freedom guaranteed by Article 11 of the Declaration of 1789, Parliament was not at liberty, irrespective of the guarantees accompanying the imposition of penalties, to vest an administrative authority with such powers [internet access suspension powers] for the purpose of protecting holders of copyright and related rights;"[103]

---

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/32563/ipreview-finalreport.pdf p.79. [Accessed: 21 December 2015].)

[101] HADOPI Act 1 Art. L. 331-27 paragraphs one and two state:

"When it is held that the subscriber has failed to recognize the obligation defined in article L 336-3 during the year following the reception of an injunction sent by the committee for protection of rights and accompanied by a receipted letter or any other method needed to establish proof of the date that the injunction was sent and that when the subscriber received it, the committee may, after a hearing, pronounce, as a result of the gravity of the violations and the use of access, one of the following sanctions:

1 The suspension of access to service for a duration of two months to one year accompanied by making it impossible for the subscriber to subscribe during that period to another contract giving access to a public on line communication service with any operator;"

[102] *Ibid.,* paragraph two.

[103] The Constitution Tribunal Decision no. 2009- 580, *op.cit.*, p.5.

The Court clearly stated that vesting an administrative agency with internet access suspension powers runs contrary to a fundamental right. Suspension can only be imposed by the court. The Court however did not clearly specify whether or not internet suspension sanction was proportionate to the offence of copyright infringement. After the French constitutional court had annulled Hadopi's internet suspension order, HADOPI Act 2 was enacted to incorporate the decision of the Constitutional Council (Decision no. 2009-580). HADOPI Act 2 keeps the option of internet suspension, but only to be used in the event that the true copyright infringer is found.[104] The suspension option was challenged again in the Constitutional Council. Members of the National Assembly contended, *inter alia*, that "the penalty of suspension of access to the Internet for a period of one year is disproportionate [...]."[105] The French Constitutional Council Decision no. 2009-590 considered the proportionate issue and held that:

"The introduction of a supplementary penalty designed to punish offences of infringement of copyright committed by the use of a public online communication service and consisting in suspending access to such a service for a maximum period of one year, together with a prohibition on entering into another contract for the same services with any other provider does not fail to comply with the principle of the necessity of punishments."[106]

According to the ruling, internet suspension is a proportionate criminal sanction which can be imposed on copyright infringement grounds.[107] Moreover, internet suspension needs to be sanctioned by the court because it affects freedom of speech for a period of time during which a subscriber cannot sign another internet access agreement. From a copyright holder's point of view, in order for a measure to be effective, it must

---

[104] Article L 335-7 paragraph one:

"When the offence has been committed by use of a public online communication service, persons guilty of the offences provided for in *Articles L 335-2, L 335-3 and L 335-4* may also be liable to imposition of a supplementary penalty of suspension of access to a public online communication service for a maximum period of one year, together with a prohibition on taking out any other contract of a similar nature with another online access provider for the same period."

(The French Constitutional Council Decision no. 2009-590 of October 22nd, 2009, Available at: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/en2009_590dc.pdf pp. 4-5 [Accessed: 20 September 2015]) [Emphasis added]

It should be noted that Articles L 335-2, L 335-3 and L 335-4 concern copyright infringement offences and penalty, as opposed to subscriber's duty default offences.

[105] *Ibid.*, p.5.

[106] *Ibid*., p.6.

[107] Moreover, the suspension case can be adjudicated by a single judge in summary court. (*Ibid.*)

circumvent the lengthy affair of court proceedings.[108] Internet disconnection, not the same as internet suspension, is the tool that circumvents court proceedings. Internet disconnection applies to a situation when an ISP disconnects a subscriber under certain circumstances. Internet disconnection can be done by an ISP alone. It is an alternative option to internet suspension.

Internet disconnection is practiced in ISP businesses. It is based on a contractual obligation or 'Terms of Use'. An ISP can terminate internet access if a subscriber is in breach of contract.[109] Certainly, if a subscriber does not pay the due subscription bill, he breaches the contract and is disconnected. Internet 'Terms of Use' include not using the internet for criminal activities.[110] Copyright infringement is of a criminal offence which could be a ground for disconnection.

In fact, internet disconnection is used as a tool for copyright deterrence elsewhere. In the US, internet disconnection is practiced by the private sector. Under the cooperative Memorandum of Understanding (MOU) signed by copyright content societies and telecommunication companies, the so-called Copyright Alert System (CAS) constitutes six warning strikes but an ISP can temporarily disconnect internet access from the fifth strike if it deems it to be appropriate.[111] Temporary internet disconnection by terms of contract is recommended for Thailand legislative framework in chapter 6.

---

[108] This thesis concluded earlier in Chapter 4 that court proceedings are considered expensive and time consuming and not practically suitable for online deterrence where end-user infringers are numerous. (*See* Chapter 4 -- 4.6.4 Concluding Remarks)

[109] See, e.g., Conditions for BT Wi-fi Service (including BT Openzone), "18. Breaches of this Contract", Available at: http://www.btwifi.com/terms-and-conditions/conditions-for-wifi-service.jsp#a18 (Accessed: 3 November 2015)

[110] See, e.g., Conditions for BT Wi-fi Service (including BT Openzone):

> "7 Use of the Service
> ...
> 7.2 The Service must not be used in any way that:
> …
> b. does not comply with the terms of any legislation or any licence applicable to the you *[sic]* or that is in any way unlawful;
> …"

Available at: http://www.btwifi.com/terms-and-conditions/conditions-for-wifi-service.jsp#a7 [Accessed: 3 November 2015]

[111] Bridy A., 2012, "Graduated Response American Style: *Six Strikes* Measured against Five Norms", *Fordham Intellectual Property, Media and Entertainment Law Journal*, 23, 1, Available at: http://www.fordhamiplj.org/wp-content/uploads/2013/01/C01_Bridy.pdf pp.32-33 [Accessed: 4 November 2015].

It can be concluded in this section that IAPs are less involved in, and not responsible for, their subscriber copyright infringement because they merely offer subscribers an internet access. The subscriber duty principle causes the burden of proof to be placed firmly on the shoulders of the subscriber where the court considers it to be legitimate. This principle also leads to the mail notification process where it was held compliant with presumption of innocence because the notification does not possess sanction, accusation or penalty characteristics, but supplies education and information. Finally, the citation of suspension of internet access under the authority of an administrative entity is disproportionate for copyright protection purposes. However, it is considered proportionate and legitimate if it is imposed by the court as a supplementary criminal penalty for copyright infringement in particular circumstances.

5.4.5 Effectiveness of Graduated Response

In this thesis, one objective is to propose effective legal measures for online copyright enforcement that reduce a number of infringing activities. It does not suggest that reducing the number of infringements is the proper aim of the copyright law - an argument often asserted by major global rights holders.[112] Assessing effective copyright law requires us to contemplate the question of what copyright actually seeks to achieve.[113] An effective enforcement legal measure that reduces infringements may or may not result in positive impacts on economic growth, technological advancement and cultural diversity. The relation between the enforcement and these impacts are other questions that depend on various factors, e.g., countries' administration regime, copyright systems, popularity of copyrighted works[114], availability and convenience of online content[115], different time and place of the new release creative works[116], market strategy,

---

[112] Giblin, R., 2014. "Evaluating Graduated Response." *Columbia Journal of Law & the Arts*, 37(2), 147. p.149.

[113] There are many ways in evaluating effective impact of GR, e.g., infringement reduction, enlargement of the legitimate market, encouragement of creation and dissemination. (*Ibid* at pp.149-150)

[114] Zhang, L. 2014. "Intellectual property strategy and the long tail: Evidence from the recorded music Industry." Available via SSRN at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2515581 [Accessed: 4 August 2017]

[115] Danaher, B. et.al., 2010. "Converting Pirates without Cannibalizing Purchasers: The Impact of Digital Distribution on Physical Sales and Internet Piracy," *Marketing Science*, Available at: http://www.heinz.cmu.edu/~rtelang/ms_nbc.pdf [Accessed: 4 August 2017]

prices of content from legal and illegal sources, etc. All of these require an extensive study which is not possible for this thesis to fulfil. This section aims to evaluate effectiveness of GR in P2P file sharing infringement reduction, a much narrower issue. Nevertheless, it is asserted that effective GR could also be a correct way to encourage artistic creation and dissemination of creative works.

In France, there are several indicators of the effectiveness of GR enforcement. Firstly, according to statistics collected by HADOPI, GR decreases the magnitude of P2P online infringement by gradually increasing degree of severity (discussed in more detail in section 5.6.4 below). Literally, a 'graduated response' to the repeat infringement is one of the successful characteristics of GR enforcement regime. Each time a warning is sent, the size of infringing users is shaped down leaving only a small number of prosecuted cases in the final stage. As a result, there one argument against the HADOPI system is it is too expensive as only a very small number of cases handed in to the prosecution.[117] It has been proposed that Hadopi organization should be shifted and its duty should be replaced by a telecommunication control agency.[118] This proposal could be taken forward and implement in any country where such an agency already exists.[119]

Secondly, a study conducted in France showed that iTunes music sales increased before and at the time the public became aware of the passage of HADOPI Act.[120] It asserted that HADOPI awareness caused reduction in internet piracy and caused pirates to become legitimate purchasers. This can be indicated by the fact that "French sales of heavily pirated genres rising higher than for less pirated genres, which suggests that this

---

[116] Ma, L. et.al, 2014. "An Empirical Analysis of the Impact of Pre-Release Movie Piracy on Box-Office Revenue," Available via SSRN at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1782924 [Accessed: 4 August 2017]

[117] McAllister, N. 2013. "France weighing 'culture tax' on phones, slabs, PCs, TVs" [Online] Available at: http://www.theregister.co.uk/2013/05/13/france_culture_tax_smartphones/ [Accessed: 12 August 2017]

[118] France Embassy to Canada website, 2016. "Culture-acte 2: 80 proposals regarding digital cultural content", [Online] Available at: https://ca.ambafrance.org/Culture-acte-2-80-proposals [Accessed: 12 August 2017]

[119] *See recommendation 2 in* 6.5.2 Recommendations for Thailand in Adopting the Principles of France and Graduated Response Remedy for Peer-to-Peer Online Copyright Protection.

[120] Danaher, B. et.al, 2014. "The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France." *The Journal of Industrial Economics,* 62(3), 541.

sales increase is causally related to a reduction in French piracy levels caused by HADOPI."[121]

Apart from the benefit of GR in impeding P2P infringement, GR was heavily critical of its negative impacts in other areas.

First, it is argued that enforcement should move the target from demand side, i.e., individual users, to supply side, i.e., commercial business or corporation entities.[122] As suggested earlier in the methodology section, the thesis focuses on end-user deterrence.[123] Commercial corporation enforcement can fulfil online copyright protection along with measures suggested in this thesis. A country does not need to pursue only one target.[124]

Secondly, in the previous section, GR arguably also impacts freedom of speech, resulting in parts of the law being repealed by French Constitutional Court. The Court ruled that internet access is part of fundamental rights and suspension of internet access can only be imposed by a court.[125] From the French Court's perspective, internet suspension, if properly ordered, is a possible sanction in relation to private rights protection. As suggested in section 2.3.2 Suspension and De-subscription of Internet Account**,** the temporary disconnection of internet access is a simple process and a less severe sanction than internet suspension which can be a measure of last resort.[126] Finally, if suspension

---

[121] *Ibid.,* p. 550.

[122] France, Hadopi, 2013. *Report on the prevention of unlawful streaming and direct downloading*, Available at: https://hadopi.fr/sites/default/files/page/pdf/Rapportstreaming_eng.pdf [Accessed: 7 October 2016]. (*See also* France, Minister of Culture and Communication, 2015. Press Release: *Government strategy on the fight against piracy of works on the Internet*, [Online] Available at: http://www.culturecommunication.gouv.fr/Presse/Communiques-de-presse/Lutte-contre-le-piratage [translated by Google Translate][Accessed: 7 October 2016].

[123] *See* chapter 1--1.5 Methodology.

[124] *Ibid.*

[125] *See* 5.4.4 Should Termination of internet access be Supplementary to Minor Offences?

[126] *See* 2.3.2 Suspension and De-subscription of Internet Account *and recommendation 5 in* 6.5.2 Recommendations for Thailand in Adopting the Principles of France and Graduated Response Remedy for Peer-to-Peer Online Copyright Protection.

and disconnection do not satisfy human rights champions, content filtering and traffic management can be an alternative.[127]

Thirdly, there is criticism that GR is ineffective when applied to platforms other than P2P. End-users resort to another platform such as cyber storage (or cyber locker) to avoid being observed by HADOPI.[128] With technology environment, there is no perfect system to address all potential threats. As far as legislation can do so, a legal system must be competently flexible in order to keep pace with fast technological change.[129]

Finally, another argument is that the GR system encroaches the right to privacy, an issue discussed earlier in justification section (2.1.2 The Graduated Response System (GR)) in chapter 2. The GR system correlates to users' IP addresses. In the EU context, the CJEU held that IP addresses can be personal information. It allowed revelation of users' IP addresses for civil and criminal proceedings according to the Member State's law, which must accommodate fundamental rights under the EU community laws and must be in accordance with other principles such as principle of proportionality.[130] Indeed, the CJEU threshold essentially accords the Universal Declaration of Human Rights which "was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A) as a common standard of achievements for all peoples and all nations."[131] Thailand is one of the countries where human rights are concerned. Thailand's copyright law must satisfy UN standards.

---

[127] *See* 2.3.3 Traffic Management, 2.3.5 Content Identification and Filtering *and recommendation 4 in* 6.5.2 Recommendations for Thailand in Adopting the Principles of France and Graduated Response Remedy for Peer-to-Peer Online Copyright Protection.

[128] Moody, G. 2013, "HADOPI May Be Succeeding -- In Driving French Customers To Dotcom's Mega" [Online] Available at: https://www.techdirt.com/articles/20130218/07195522015/hadopi-may-be-succeeding-driving-french-customers-to-dotcoms-mega.shtml [Accessed: 12 August 2017]

[129] *See recommendation 1 in* 6.5.2 Recommendations for Thailand in Adopting the Principles of France and Graduated Response Remedy for Peer-to-Peer Online Copyright Protection.

[130] *See* 2.1.2 The Graduated Response System (GR).

[131] United Nations, "Universal Declaration of Human Rights" [Online] Available at: http://www.un.org/en/universal-declaration-human-rights/ [Accessed: 13 August 2017]

There are other claims where effectiveness of GR is in doubt.[132] The thesis cannot cover all of them due to word constraints. Regarding the above areas, a state can rework the GR system so that is effective in deterring users' online infringing activities. Thailand must learn from France Constitutional Panel and the CJEU rulings to minimise any conflict between freedom of speech, the right to privacy and of other interests. Such a system should aim to correspond with dissemination of knowledge and encouragement of artistic creation and expression. In the Chapter 6: Conclusions and Recommendations, this thesis will inform the possible reforms to Thai law according to these findings.

5.5. The Graduated Response Rule of France

"[The Graduated Response system] seeks to strike the middle ground by providing sufficient warning to Internet users who might have engaged in illegal online file-sharing activities while at the same time protecting the interests of copyright holders, such as those in the publishing, recording, movie, software, and game industries."[133]

To achieve the above objectives, the HADOPI Act resorted to options available outside the court room. It created a new public duty, a new public organization, proceedings and sanctions. This law put a monitoring duty on an internet subscriber, instructed the informative and coercive proceedings and imposed sanctions on both pirates and internet access subscribers.[134] It has evolved over years and continues to do so. This section provides a history of the HADOPI Act and evolution of P2P deterrence. It explores the HADOPI Act which gave birth to the Hadopi organization. Under Article L. 331-13, Hadopi retained three missions: "protect works against copyright infringement on public online communications networks; promote the development of legal content services, and monitor the legal and illegal use of works and objects subject to a copyright or neighbouring right on digital communications networks."[135] The HADOPI Act required that ISPs inform their subscribers of their duty to monitor internet access as outlined in

---

[132] *See e.g.*, Giblin, R., 2014. "Evaluating Graduated Response." *Columbia Journal of Law & the Arts*, 37(2), 147, McKenzie, J. 2017. "Graduated response policies to digital piracy: Do they increase box office revenues of movies?", *Information Economics and Policy*, 38, 1., Danaher, B. et.al. 2017. "Copyright Enforcement in the Digital Age: Empirical Evidence and Policy Implications", *Communications of the ACM*, 60(2), 68.

[133] Yu, P.K., 2010. "The Graduated Response", *Florida Law Review*, 62, 1370, 1379

[134] Rambaud, *op.cit*.

[135] UK, Intellectual Property Office, *op.cit*., p.47. [Internal emphasis omitted].

their subscription contract, measures possibly taken by the Rights Protection Commission (RPC) in civil and criminal lawsuits, and security means to prevent breach of monitoring duty.[136] Having learned from the contract, a subscriber is required to monitor his internet use or he can be prosecuted. There are informative and educative proceedings before a potential prosecution. This section examines certain characteristics of subscriber duty and GR proceedings. A HADOPI Act history section immediately below discusses how subscriber duty and the associated proceedings emerged.

5.5.1 History of the HADOPI Act and of the Deterrence to P2P Illegal Use

In 2007, the French Minister of Culture and Communications brokered the agreement for the protection of cultural works signed by interested parties such as public authorities, right holders and service providers. The agreement set forth provisions to establish a warning and sanction mechanism (GR) and laid the foundation for the law that followed. On 13th of May, 2009, the HADOPI Act 1 was ratified. It reaffirmed the internet subscriber obligation principle under DADVSI and the agreement on GR procedure originally outlined in the DADVSI Act.[137] It established an administrative body that supervises internet copyright violation, the so-called High Authority for the Distribution of Works and the Protection of Rights on the Internet (Hadopi) (French: *Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet*). HADOPI Act 1 authorised Hadopi internet disconnection where the constitutionality of such authority was negated by the French Constitution Council in the same year.[138] Following the Council judgment, on October 28, 2009, the French government enacted HADOPI Act 2. This Act stipulated that copyright infringement can be imposed only by the Criminal Court for a maximum of one year.[139] It left most of the HADOPI Act 1 procedure for P2P deterrence unchanged.

The HADOPI Act was changed once again in July 2013. Decree N°2013-596 (HADOPI Act 3) Article 2 repealed the FIPC provision that allowed the court to suspend an account holder's internet access where evidence showed that such an account holder had been

---

[136] Vassenaix-Paxton, A.S., 2012. "The French Law *Hadopi # 1 & 2*", In: ALAI Meeting, slide 14. Available at: http://www.barrysookman.com/2012/10/10/the-french-hadopi-law-its-history-operation-and-effectiveness/ [Accessed: 26 December 2015]

[137] France, Hadopi, 2011. *Annual Report 2011*, Available at: http://hadopi.fr/sites/default/files/page/pdf/Hadopi_Rapportannuel_ENG.pdf p.14 [Accessed: 30 April 2015]

[138] Strowel, *op.cit*., p. 81.

[139] Vassenaix-Paxton, *op.cit.*, slide 17.

negligent in monitoring his internet access.[140] However, the option of a complementary suspension penalty still remains with the court if it finds that an actual copyright infringer, being the account holder or not, is found guilty.[141] This decree relieves the HADOPI Act from the controversial issue that internet suspension hampers the fundamental right to the access of information, especially as regards the account holder who may not be the actual infringer.[142] The account holder can still be punished by a fine of up to 1500 euros in the case of gross negligence.[143] The present state of GR is that it is a procedural system which raises the internet user's awareness through a series of notifications as well as fine sanctions directed towards an errant user if the notifications are ignored. Internet user duty and detailed procedure is analysed below.

5.5.2 The Creation of Internet Subscriber Obligation for Online Copyright Protection

The internet account holder's duty was conceived to assist online copyright infringement.[144] Section 11 of the HADOPI Act inserts Articles L 336-3 into Chapter IV of the French Intellectual Property Code (FIPC). Article L 336-3 prescribes internet subscriber duty to monitor internet use. The duty is that a subscriber has an obligation to monitor his internet usage, not to allow it to be used in a way that damages copyright. Article L336-3 paragraph one of FIPC stipulates:

"A person who has subscribed to internet access to online public communication services is under a duty to ensure that said access is not used for reproducing, showing, making available or communicating to the public works or property protected by copyright or a related right without the authorization of the copyright holders provided for in Books I and II when such authorization is required."

The subscriber is informed of such duty and GR measures by a mandatory clause in an internet subscription contract.[145] If a subscriber does not fulfil his duty and his account

---

[140] The 1709 Blog, 2013, "Three Strike Struck Out" [Online] Available at: http://the1709blog.blogspot.fr/2013/07/third-strike-struck-out.html [Accessed: 8 May 2015]

[141] *Ibid.*

[142] For a discussion on philosophical issues or the justification of GR measure *see* chapter 2 -- 2.1. Justification and Characteristics of Digital Copyright Protection Remedies.

[143] Andy, 2013. "Three Strikes and You're Still in- France Kills Piracy Disconnections" [Online] Available at: http://torrentfreak.com/three-strikes-and-youre-still-in-france-kills-piracy-disconnections-130709/ [Accessed: 8 May 2015])

[144] This duty also helps overcome the difficulty of proving the actual infringer in a subscriber's house.

[145] FIPC Article L. 331-35:

---

is used to infringe copyright, such subscriber can be subject to GR warning and sanctioning measures, no matter if he is the actual infringer or not. FIPC Article L.331-26 prescribes that the first warning is via email and the second warning is via a registered mail. After the process of warning, the third stage is a fine for a petty offence of up to EUR 1,500.[146] The monitoring duty is a separate distinct legal responsibility within the French copyright Act since breaching the duty is not the same as breaching copyright. The subscriber can be upheld as being in default of the duty although he himself might not necessarily have engaged in copyright infringement.[147] By no means does the subscriber's duty itself create a copyright infringement charge.

Whether using the subscriber duty principle for copyright protection is at all justified was a question already discussed by the French Constitutional Council.[148] In its Decision no. 2009-580 of June 10th 2009, the court ruled that the obligation is distinct from the offence of copyright infringement.[149] In imposing the obligation, the French Parliamentary proceedings were accessible and the legal content was intelligible.[150] The monitoring duty is now constitutional. Following France's initiation, other countries can create and impose a duty on a subscriber and presume guilt on the subscriber provided that the subscriber has the opportunity to prove otherwise in his defence and that the breach of such duty is only classed as a minor offence. The principle of subscriber duty is

---

"People whose business is to provide access to communication services to the public online are to include in contracts with their customers, the clear and readable mention of the provisions of Article L. 336-3 and measures that can be taken by the rights protection commission. They also include in their contracts with subscribers, the criminal and civil penalties incurred for breach of copyright and related rights.

In addition, the persons referred to in paragraph one of this article inform their new subscribers and those renewing their subscription agreement on the legal offer of cultural content online, on the existence of security means for preventing breaches of the obligation defined in Article L. 336-3 and the dangers for the renewal of artistic creation and the economy of the cultural sector if practices do not respect copyright and related rights."

[146] Berne, X., 2015. "Hadopi: several subscribers fined between 300 and 500 euros fine. The last sentence?" [Online] Available at: http://www.nextinpact.com/news/96525-hadopi-plusieurs-abonnes-condamnes-a-300-et-500-euros-d-amende.htm [French translated by Google Translation] [Accessed: 8 January 2016]

[147] Geiger, C., 2014. "Challenges for the Enforcement of Copyright in the Online World: Time for a New Approach," *Max Planck Institute for Innovation and Competition Research Paper*, 14, 1 [Online] Available at: https://www.researchgate.net/publication/260791463_CHALLENGES_FOR_THE_ENFORCEMENT_OF_COPYRIGHT_IN_THE_ONLINE_WORLD_TIME_FOR_A_NEW_APPROACH p.6 [Accessed: 28 October 2015]

[148] The French Constitutional Council Decision no. 2009-580, *op.cit.* p. 2.

[149] *Ibid.*

[150] The court ruled: "Contrary to what is claimed by the parties making the referral, the definition of this duty is distinct from that of the offence of infringing copyright. It is defined in sufficiently clear and precise terms. When imposing this duty Parliament neither failed to exercise fully the powers vested in it by Article 34 of the Constitution nor failed to comply with the constitutional objective of intelligibility and accessibility of the law." (*Ibid*.)

followed by the procedure to identify the account owner, send mails and impose a fine. The procedure is examined below.

5.5.3 The HADOPI Act Procedure in P2P Deterrence

From the beginning, a subscriber acknowledges monitoring duty, and measures and sanctions following failure of such duty by a clause in an internet subscriber contract.[151] An ISP does not monitor P2P used by its subscribers.[152] Hadopi is the main regulator. A subordinate unit of Hadopi, the so-called Rights Protection Committee (RPC), is in charge of implementing the warning mechanism.[153] It is comprised of official professional organisations, collecting societies or any other right holder representatives. These representatives "use a variety of measures, including anonymously venturing onto peer-to-peer websites and using third party monitoring companies, such as Dtechnet, to detect any illegal sharing".[154] Upon detecting copyright infringement, the right holders collect IP addresses of suspected subscribers and notify Hadopi. "Hadopi may then request that the relevant ISP provides the contact details of the subscriber whose IP address is under investigation."[155] The subscribers can be individual users or an organisation such as a university which is not directly infringing a copyright.[156] The RPC can then initiate the GR by sending the first online warning email to users.[157] IAPs

---

[151] FIPC Art. L. 331-35 paragraph one – Persons whose activity is to offer access to public online communication services shall include, in contracts entered into with their subscribers, a clear and understandable reference to the provisions of Article L. 336-3 and the measures that may be taken by the Rights Protection Commission. They shall also include, in contracts entered into with their subscribers, the criminal and civil sanctions incurred in the event of copyright and related rights being violated."

[152] Elton, S. 2013. "Graduated responses to online piracy: Approaches taken in the United States and around the world" In Deflem, M., ed. *Music and Law (Sociology of Crime, Law and Deviance, Volume 18)* Emerald Group Publishing Limited, p.44. Available via Emerald: http://dx.doi.org/10.1108/S1521-6136(2013)0000018005 [Accessed: 16 October 2015].

[153] Aroba, N., 2013. Implementation and Success Analysis of Various Global Graduated Response Programs for Piracy with Special Focus on the "Six Strikes" Policy. Bachelor Degree. Thesis, University of Arizona. pp.16-17.

[154] Elton, 2013. *op.cit.*

[155] Rambaud, *op.cit.*

[156] Strowel, *op.cit*., p.80.

[157] FIPC Art. L. 331-26 paragraph one provides:

"When entering facts that could constitute a breach of the obligation under Article L. 336-3, the Rights Protection Commission may send to the subscriber, under its tone and for its account, electronically and through the person whose business is to provide access to communication services to the public online under contract with the subscriber, a recommendation reminding him of the provisions of Article L . 336-3, requiring it to comply with the obligation that they define [Provisions declared non-compliant with the Constitution by the Constitutional Council decision No. 2009-580 DC of June 10, 2009]. This recommendation also contains information for the subscriber on the legal offer of cultural content online, on the existence of security means for preventing breaches of the obligation under Article L. 336-3, and on

---

cooperate by forwarding the warnings to their clients.[158] The first email, the so-called "recommendation", contains information about:

(a) the offence of which he is alleged to be guilty,

(b) his monitoring obligation

(c) legal alternatives to acquire copyrighted works

(d) ways to secure their Internet access[159]

The email raises awareness by stressing the threats of copyright infringement to the cultural industry and to creativity.[160] If another breach of the obligation is identified within six months, there will be a second warning by both an email and a registered postal mail.[161] The two 'recommendations' contain the same information (a)-(d) above. They must include the date and time of breach of monitoring obligation and contact information but "they do not disclose the content of protected works or objects affected by the breach".[162] ISPs are responsible for contacting their subscriber regarding the notice issued by Hadopi or they can be fined up to 7500 Euros.[163] The subscriber is given a chance to acquire additional information from Hadopi on protected works in order to prepare his defence.[164]

In case of a third detection within one year of the second recommendation sent, the third notification is conducted by letter against signature on receipt.[165] Hadopi can notify account holders that their file can be transferred to the judicial authorities for

---

hazards to the renewal of artistic creation and the economy of the cultural sector if practices do not respect copyright and related rights."

[158] Strowel, *op.cit*., p. 80

[159] FIPC Art. L. 331-26 paragraph one.

[160] Meyer, T. and Van Audenhove, L. 2012, "Surveillance and Regulating Code: An Analysis of Graduated Response in France" *Surveillance & Society,* 9(4), 365. p.369 Available at: http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/reg_code/reg_code

[Access: 29 April 2015]

[161] FIPC Art. L. 331-26 paragraph two provides:

"In case of renewal, within six months from the sending of the recommendation referred to in the first paragraph of facts that could constitute a breach of the obligation under Article L. 336-3, the Commission may make a new recommendation with the same information previously provided electronically in the first paragraph. It may attach to the recommendation a letter delivered against a signature or other appropriate means of establishing proof of the mailing date of this recommendation."

[162] FIPC Article L. 331-26 paragraph three

[163] Decree no. 2010-1202 of 12 October 2010 modifying Article R. 331-37 of the Intellectual Property Code (France, Hadopi, *op.cit*., p.23)

[164] Strowel, *op.cit*., p. 80

[165] FIPC Art. L. 331-27 paragraph one.

criminal proceedings.[166] After due deliberation by Hadopi, individual case files may be forwarded to the French Penal Courts.[167] The third strike is fulfilled by an automatic fining system. A single judge may render a decision without the need to inform the account owner and without trial.[168] However, the account owner, on receipt of the judge's decision, may challenge it within 45 days to defend his case through the traditional procedure.[169] The maximum penalty incurred by the account owner is a EUR 1,500 fine.[170] The fine is for a failure to secure the internet connection.[171] Suspension of the subscriber's internet access is not sanctioned but that option is available in the case of the real infringer, if and when apprehended. Before HADOPI Act 2 was ratified, infringers were punishable by a fine of up to EUR 300,000 and imprisonment of up to three years.[172] Under HADOPI Act 2, the infringer's internet access may also be suspended for a period not exceeding one year.[173] During this suspension, infringers must not subscribe to another ISP or "they may be punished by a further fine of up to EUR 30,000 and imprisonment of up to two years".[174]

It is said that the GR measure is based on a contractual obligation, not a copyright charge. The reason for this is that the subscriber agreement states subscriber duty and the measures to follow in case of duty default. However, the whole process is actually prescribed in law. The agreement merely enhances subscriber knowledge. Were it not mandatory in law to include such duty in the agreement, the GR system could otherwise be enforced through the law. Table 6 below summarises functional aspects of HADOPI of France in application to P2P.

Table 6: Functional Aspects of HADOPI of France in Application to P2P

[166] Meyer, *op.cit*., p.369.
[167] UK, Intellectual Property Office, *op.cit*., p.47.
[168] Rambaud, *op.cit*.
[169] *Ibid.*
[170] Konstantinou, I., 2013. The compatibility of a Graduated Response System at EU level with the fundamental human rights to privacy, data protection and freedom of expression. LL.M.thesis, Tilburg University. p.22.
[171] *Ibid.*
[172] Rambaud, *op.cit.*
[173] *Ibid.*
[174] *Ibid.*

Country / Objects of Discussion	France
1. Affected ISPs	-Internet Access Providers (IAPs) under FIPC Article L. 331-35
2. Subscriber Duty to Monitor Internet Use	-Yes, under FIPC Article L. 336-3
3. Warning Notifications	-Yes, the notification directed to a detected subscriber
4. Presumption of Guilt	-Yes, on breach of subscriber duty grounds
5. Minor Offences	-Yes with an offence of breach of a subscriber duty
6. Fine Imposed by Judges	- Yes, by a single judge on breach of subscriber duty (summary procedure) -The subscriber may refuse the allegation in which case the court trial follows.
7.Internet Suspension/ Disconnection	-Internet suspension is possible, if a subscriber is proved guilty of copyright infringement.

5.6 Comparative Analysis: Conclusion

In this section, the two systems will be compared in many areas. Thailand and France service providers concerned will be compared how they can be affected by their own countries legislation applicable to P2P user copyright violation. As Thailand lacks a monitoring duty on part of internet account subscribers, this section will discuss how this affects its civil and criminal procedure in a case against a P2P user. This section will compare the case outcome of the country which has presumption of guilt and minor offence with the other country which does not have. In terms of procedure, a comparison is made between GR and court proceedings. Lastly, internet access restriction is analysed if it can be part of an alternative or supplement measure.

5.6.1 Thailand and France Service Providers Affected by the Court Order and Graduated Response in Application to P2P

For Thailand, IAPs are service providers that can be subject to a court order under CA 2015 Section 32/3 paragraph two. P2P infringement has 'taken place' within IAPs' systems because the systems transmit P2P file exchange. Therefore, copyright infringement -- reproduction, adaptation and communication to the public -- is committed in IAPs' systems. Another prerequisite criterion for a motion is that the order must be 'necessary' under CA 2015 § 32/3 paragraph four. The term 'necessary' can be interpreted by, or interchanged with, the term 'sufficient' under CIPC § 255 (2).[175] The 'sufficient' ground is established if infringement and plaintiff damage continues.[176] In the P2P scenario, the infringement and damage continue whilst the P2P programme is running. A measure needs to be implemented by an IAP with respects to connection to the internet. Therefore, an IAP is a service provider under CA 2015 paragraph two which can be subject to a motion.

France is similar to Thailand in that P2P infringement takes place in an IAP's system. IAPs are involved in GR because they offer subscribers an internet access. Because of this, French IAPs need to assist Hadopi in GR measures in cases where illegal file sharing is found being committed by a user of their systems.

Both Thai and French IAPs are subject to their own laws. French ISPs are required to state in the subscriber contract the subscriber duty along with the GR process, and then to process GR legal measures accordingly. Thai ISPs have no such requirement nor do they have an out-of-court legal process. French IAPs are clearer about the process because the HADOPI Act expressly prescribes what an IAP must do, e.g., notify an alleged subscriber of

---

[175] CIPC § 255 (2) stipulates: "The court shall grant any application filed under Section 254, when it is satisfied that the complaint is *prima facie* and has sufficient ground for applying the protective measures requested according to the following rules:

(2) In case of an application for any order provided in Section 254(2), the court must be satisfied that:

(a) The defendant intends to repeat or continue the wrongful act, the breach of contract or the conduct complained of,

(b) The plaintiff will henceforward sustain trouble and injury because of the defendant's act,

(c) The property in dispute or the defendant's property is in circumstances to be wasted, injured or transferred, or

(d) There is any ground provided in (1) (a) or (b);

... "

[176] CIPC § 255 (2) (a) and (b)

the matter by emails and registered mails, revealing the subscriber identity. Thai IAPs are obliged to execute the court order of which the extent is unclear as to whether the court applies email warnings, disconnection, or any other measure.

5.6.2 Thailand's Lack of Monitoring Duty on the Part of Internet Account Subscribers in P2P Technology

French subscriber duty is intended to be a regime to protect copyright online. A subscriber is criminally liable for online copyright infringement which has taken place by use of his internet account. Thailand does not have such a duty in its legislation. A subscriber is not liable to copyright infringement occurred in his account merely because he is the account holder. A subscriber who is not involved in such infringement is not necessarily liable the third party infringement criminally or civilly. The lack of monitoring duty in substantive law including the lack of presumption of guilt and minor offence worsens the P2P enforcement situation in Thailand.

5.6.3 Thailand's Lack of Presumption of Guilt and Minor Offences for P2P Infringement Protection Purposes.

The presumption of guilt in minor offences is well accepted in developed countries. That presumption dispels the difficulty of proving the identity of actual infringer in a subscriber's household. France legalises the presumption of guilt in such a way that it does not conflict with the presumption of innocence. It characterises the unfulfilled subscriber's monitoring duty as a minor offence. The subscriber bears the burden of proving that he is innocent of not fulfilling his monitoring duty. This is so whether or not the subscriber is actually the real infringer. A summary prosecution proceeds in such a case. A single judge can impose a fine according to the evidence of an infringement persistence record and the non-compliance with prior notifications.[177]

CA 1994 prescribes that a copyright infringement, though not of the minor offences, has a presumption of fact because it is a fineable offence. CA 1994 § 77 authorizes the Director General of DIP to impose the amount of fine. The Director cannot impose a fine on a subscriber because the subscriber may not be the infringer. The

[177] Berne, X. 2015. "Hadopi: several sentenced to 300 subscribers and 500 euro fine. The last Judgement ?" [Online] Available at: http://www.nextinpact.com/news/96525-hadopi-plusieurs-abonnes-condamnes-a-300-et-500-euros-d-amende.htm [French][translated by Google Translation]

Director also cannot impose a fine on an infringer because the infringer is unidentifiable. Therefore, presumption of guilt and minor offence are not available legal mechanism for P2P user infringers under the current CA 1994. In light of this, success in online copyright infringement litigation is not guaranteed.

In civil cases, although a CA 2015 motion does not need identification of the illegal P2P user or subscriber but a right holder needs to identify an account holder or an infringer in order to pursue redress. In the identification process, a right holder needs a court subpoena to reveal the personal identity of the IP address. The acquired identity is not necessarily revelation of the real infringer. There are various strong arguments an account holder can advance to counter to an infringement claim. As a result, the civil case is likely to be unsuccessful. These problems can arise in a § 32/3 motion and in the main infringement case.

In criminal cases, the problems are similarly embedded in both process and outcome. In prosecution process, the inquiry official has to investigate to determine the real infringer. The investigation is very demanding process even if a search warrant for the property is acquired because it involves gathering of computer forensic and biological evidence, or other circumstantial evidence. Merely having an IP address and an account holder identity without a witness or the aforementioned evidence is insufficient to satisfy the standard of proof in a criminal case.

The situation in Thailand outlined above likely persuades a right holder to opt for the criminal process because it is much simpler than the civil and requires less resource. However, this option suffers bad publicity and requires much resource on a state whereas the outcome is not ensured. The introduction of subscriber duty as a minor offence incorporated with the presumption of guilt is a potential way to overcome these drawbacks. Moreover, there is a warning system before a subscriber is exposed to the prosecution. The nature of the warning system will be evaluated next.

5.6.4 Mail Notification Followed by Prosecution in Comparison with Court Procedure and the Court Order Measures

French mail notification does not conflict with the presumption of innocence. A warning email/mail system does not establish a sanction and an accusation but gives information and presents rebuttable facts. Moreover, it reminds users of their obligations to secure their internet use and warns them of possibly futuristic prosecution. After two

formal warnings, the case may be referred to a public prosecutor for consideration if the infringement continues.

Under the Thai system, P2P online infringement continually shares content and damages copyright owners' interests. This situation warrants 'necessary' for the prohibition of the sharing. The court order similar to the GR three strikes gives rise to several conceivable legal and practical problems. Legally, a court order for the first and second mail notification is questionable as to whether or not it is 'reasonable' and 'ceases' the infringement. The mail notification order accompanied by the third strike criminal prosecution is more likely to be granted. Practically, the court order for criminal prosecution is not necessary because a right holder does not need such an order to prosecute an end-user. Thai right holders can directly initiate criminal prosecution by lodging a complaint to an authority if copyright infringement is found. For these reasons, the Thai court order procedure is neither efficient nor effective for copyright protection in P2P technology. CA 2015 remedy is not a suitable method of enforcement. It can be concluded that the French GR mailing system followed by prosecution has more advantages than the Thailand court procedure in many respects.

Firstly, in France a right holder does not need to go to the court to file a subpoena to disclose the identity of the subscriber, to file a motion for injunction or both. An email may be sent to the recipient through an IAP's system without subscriber identity disclosure and with essentially no cost. This can spare the resources otherwise required. Here, a Thai right holder cannot avoid entering into a lawsuit merely to send a warning email or a cease-and-desist letter.[178] The Thai approach wastes the right holder's resource.

Secondly, French mail content contains more useful information than the Thai cease and desist letter. It is compulsory for the mail to have educational and informative qualities. Indeed, it is the GR informative and educative function that gave it worldwide renown. This function raises public awareness. The Thai 'cease and desist' letter has no compulsorily legal format as to what is required in the content of the letter.

Thirdly, the GR method has a gradually increasing degree of severity which correspondingly decreases the magnitude of online infringement. The first warning is

[178] The US has the same problem about P2P user identity revelation. (*See* chapter 4 -- 4.4.2.2 Does a Notice and Takedown System Adequately Protect P2P?)

noticeably effective in reducing the size of the initial batch. The second registered mail ensures mail notification and a second time screening of users. It has legal consequences. It can be adduced as evidence to prove infringer intent in court. This information triggers a strong message to users which, as a result, reduces the number of prosecutions. The GR approach is successful in a certain extent as shown by the following graphic.

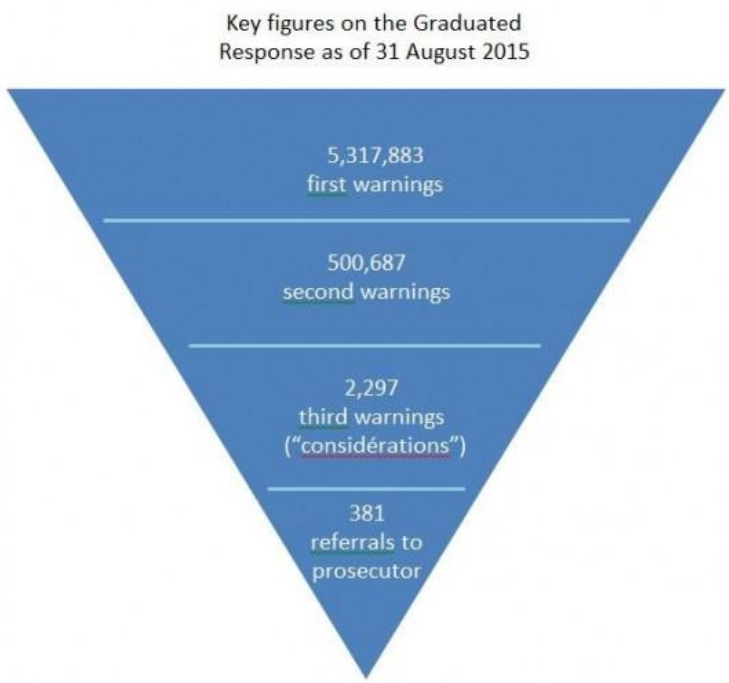

Figure 4: Key Figures on the Graduated Response as of 31 August 2015

(Source: http://graduatedresponse.org/new/?page_id=24)

The figure above shows the reducing numbers of infringement. As of August 2015, there was a difference in the numbers of warnings at each stage. The first emails totalled more than five million. Emails requiring a follow-up registered mail were limited to five hundred thousand. The number requiring a third warning was substantially lower still as was also the number of cases referred to public prosecutors. Actual prosecution cases resulting from the referrals will be lower still after a final filtering. This is significant because it shows that the system structurally deals well with a large number of infringers by ways of giving constructive information and shaping down requisite prosecution to the minimal. Hence, one may conclude that the French GR system proves efficient and effective in the P2P environment.

5.6.5 Internet Access Restriction and Traffic Management as a Solution

In France, internet suspension has to be prescribed in the law on legitimate grounds.[179] An administrative agency could not be allowed to apply the internet suspension.[180] The court is the only institution authorized to apply the sanction. Suspension is still available for cases of breach of copyright where an internet account holder is proved to be the same individual as the copyright infringer.[181] In Thailand, internet suspension is not available as a criminal or administrative sanction. As with the current CA 2015 § 32/3 provision, the request for a court injunctive order or decision to suspend an internet account is likely to be found 'unreasonable' because suspension is not prescribed by the copyright law.

In both countries internet suspension can violate human rights guaranteed by a democratic regime. Internet suspension must be stipulated in the legislation and apply to a given circumstance. Moreover, it can only be applied by a court, not by a public or private administrative entity. This suggests that a country needs to pay careful attention should it determine to use internet suspension legalised as a remedy for a copyright infringement purpose.

In contrast to internet suspension, internet disconnection and traffic management are alternatives. In CA 2015 § 32/3 injunction, the request for a court order to manage internet traffic and disconnect an internet subscriber can be found 'reasonable'. These measures are not necessarily prescribed by a law but in the terms and conditions of a subscription. The terms state under which circumstances an IAP is entitle to apply these measures.[182] Copyright infringement can be added as a condition for disconnection and/or traffic management.

The table 7 below summarises different online copyright protection legal measures against P2P technology infringement by users under the jurisdictions of France and Thailand.

---

[179] Under the European Convention on Human Rights Article 10 (2), freedom of expression may be subject to restrictions as are prescribed by law and are necessary in a democratic society, in the interests of protection of rights of others.

[180] The French Constitutional Council Decision no. 2009-580, *op.cit.*

[181] France, Hadopi, *op.cit.*, p.36-38.

[182] For example, non-payment of subscription fee (in case of disconnection), or peer-to-peer network (in case of traffic management). (*See* chapter 2 -- 2.3.2 Suspension and De-subscription of an Internet Account.)

Table 7: The France and Thailand P2P Online Copyright Protection Systems in Comparison

Country / Objects of Comparisons	France	Thailand
1. Affected ISPs	-Internet Access Providers (IAPs) under FIPC Article L. 331-35	-Access Service Provider[IAPs] under CA 2015 § 32/3 paragraph two (1)
2. Subscriber Duty to Monitor Internet Use	-Yes, under FIPC Article L. 336-3	-No.
3. Warning Notifications	-Yes, the notification directed to a potential subscriber	1. By a right holder herself: -Theoretically, yes. - Practically, no, because the account holder is unknown. - a court subpoena to reveal the internet subscriber identity needed. 2. By the court order: - Questionable (not certainly satisfied the 'cessation' ground) - The notification and then criminal prosecution request is possible, but not practical
4. Presumption of Guilt	-Yes, on breach of subscriber duty ground	- Yes, on copyright infringement ground under CA 1994 § 69 and 70 paragraphs one, and CRPC 1934 § 37(1)
5. Minor Offences	-Yes.	- Yes but partly. Copyright infringement carries a fine £400-4,000 under CA 1994 § 69 paragraph one (primary infringement), and £200-2,000 under CA 1994 § 70

Country / Objects of Comparisons	France	Thailand
		paragraph one (secondary infringement) but minor offences are generally fined no more than £200 under the PC 1956 §102.
6. Fine Imposed by Judges or Administrative Authorities	- Yes, by a single judge on breach of subscriber duty. (summary procedure) -The subscriber may refute the allegation in which case a court trial follows.	-Theoretically yes, by Director of DIP on breach of copyright ground. -Practically no, because the fine has to be imposed on the real infringer who is not identifiable.
7.Internet Suspension	-Yes, if a subscriber is proved guilty of copyright infringement.	-No. -The court order for Internet suspension is questionable.
8. Advantages and Disadvantage	1) Advantages (criminal proceedings) 1.1 Breach of Internet Subscriber Duty 1.2 Educative and Informative Warning 1.3 Legal measure is more likely an administrative basis 1.4 Minor Offences and presumption of guilt (No problem of proportionality.) 1.5 No need to identify the real infringer 1.6 Internet suspension is an option	1) Disadvantages (civil and criminal proceedings) 1.1 No Breach of Internet Subscriber Duty 1.2 No Educative and Informative Aspects (criminal and civil) 1.3 Legal action is on a case-by-case basis (criminal and civil) 1.4 Not criminal minor offences and no presumption of guilt (Problem of Proportionality --Fine is too high (see number 5. above) (criminal)) 1.5 No need to identify the real infringer in the motion but after the order is granted: 1.5.1 Problem of Investigation of the real infringer (criminal) 1.5.2 Problem of Proof of the real infringer (criminal and civil) 1.6 No option of internet suspension

In this chapter, a functional comparison of many aspects of online copyright protection remedies employed by France and Thailand has been carried out. First, the two countries IAP groups are required to implement the remedies by their own legislation. Thai IAPs are inconvenienced more heavily by the court order. They may need to contest in a trial while French IAPs may not need to do anything other than inform their allegedly defaulting subscribers. Secondly, Thailand does not have such a subscriber duty in its legislation whereas France does. Thirdly, France legislates mail warnings to reduce the amount of infringers while Thailand's cease and desist letter goes practically unused. Fourthly, France has presumption of fact/guilt which facilitates remedial procedure whereas Thailand does not. Fifthly, France deals with the problem of proportionality by classifying a breach of subscriber duty as a minor offence, while Thailand copyright infringements are not readily classed as minor offences. Sixthly, the French summary court can fine an internet account holder while the Thai Director of the Intellectual Property Department (DIP) can legally, not practically, fine an infringer, not an internet account holder. Finally, with respect to internet suspension, the French court has the authority to suspend internet access. No Thai institution may do so.

As answer of the above comparative functional analysis, it can be concluded that the French GR system provides more advantages than disadvantages as compared to Thailand online P2P copyright protection. Weaknesses in the Thailand digital copyright enforcement system include no subscriber monitoring duty, less educative and informative notification, no presumption of guilt, issues with respect to the proportionality of fine awarded, no right to suspend internet access, and generally speaking the unsuitability of the case-by-case basis for enforcing P2P infringement given the volume. This observed general weakness is congruent with an EU report which suggests a more cost effective measure to enforce online copyright infringement for Thailand.[183] These shortcomings in the Thai system form the basis for the final conclusions

[183] European Commission, 2015. *Report on the protection and enforcement of intellectual property rights in third countries.* p.22. Available at: https://euipo.europa.eu/ohimportal/documents/11370/0/Report+on+the+protection+and+enforcement+of+intellectual+property+rights+in+third+countries [Accessed: 7 July 2016].

and recommendations proposed in the final chapter, chapter 6: Conclusions and Recommendation.

Lastly, the final chapter will also recommend the legal framework regarding the argument against GR on the issue of balance between copyright and right to privacy. Chapter 2 has concluded that right to privacy can be disturbed because an IP address is personal data if a person who collects the IP address can manage to identify the data subject, i.e., an internet account subscriber. However, CJEU ruled that such personal information that can be disclosed by the domestic law of Member States for the purposes of individual right protection and criminal investigation if the law guarantees general fundamental rights of the public. Applying the CJEU standard, Thailand can address the issue of right to privacy in its legislation.

Chapter 6: Conclusions and Recommendations

This thesis endeavours to examine current Thailand remedies for infringement of online copyright in client/server and Peer-to-Peer (P2P) file sharing technology. It examines the legal remedies of the US for client/server technology (Notice and Takedown or N&T) and those of France for P2P file sharing technology (Graduated Response or GR). The central question, which directed the course of this study, is how Thailand can develop its legal system to be effective and efficient through the adoption and development of N&T and GR systems. In order to answer this question, pertinent issues have been examined and discussed throughout the chapters of this thesis.

6.1 Conclusions of Research Results from Chapters 1 and 2

Chapter 1 introduced legal background and defined necessary terms. It showed the motivation for this thesis, set out the aim and objectives therein, identified the methodological framework deployed to provide answers to thesis questions, stated the field and deficits in the current research and literature and the contribution to the knowledge offered by this thesis, and clarified its focus and scope of this thesis. It foreshadowed issues discussed in the subsequent chapters.

Chapter 2 considered the justification of the N&T and GR systems. The N&T system has internal equilibrium whereas both copyright holders and users can secure their own rights. As illegitimate use of copyrighted works on the internet is so widespread, strengthened enforcement in this situation is legitimate. The GR system deploys a device for surveillance and the recording of repetition which are minimally necessary and avoid intrusion into the right to privacy. The system can compromise freedom of speech by authorising that only the court may impose internet suspension and by only applying internet access restriction to the home usage. On technological issues, client/server protocol and P2P are the major infringing platforms. N&T and GR are the main court-circumvention legal remedies where internet suspension, and disconnection, traffic management and filtering are among the technologies which can assist the main remedies. The current infringement detection and identification of Internet Protocol Addresses (IP addresses) are reliable in revealing an internet account holder but not a precise wrongdoer.

6.2 Conclusions of Research Results from Chapter 3 and Recommendations for Ensuring the Inviolable Right of Communication to the Public

Thailand's substantive copyright law, Copyright Act 1994 (B.E.2537) (CA 1994), meets international standards with certain specified weaknesses identified in this thesis. It has sufficient breadth to cover client/server and P2P activities in both civil and criminal liabilities. Primary and secondary infringement involves infringing/infringed copyrighted materials.[1] CA 1994 section 4 paragraphs 13 and 14 (i.e. reproduction and adaptation definitions) incriminate client/server and P2P users in primary sense.[2] Only a client/server user, not a P2P, can infringe the right of communication to the public in secondary sense.[3] However, CA 1994 section 4 paragraph 15, the definition of 'communication to the public'[4] is not clear when applied to digital online infringement in many respects:

1. At present in CA 1994, infringement of 'communication to the public' right can be both primary and secondary because the definition encompasses 'distribution'. A client/server and P2P user infringement is not certain whether it is fallen into primary or secondary discipline. When a copyrighted work is illegally reproduced, adapted and is made available on the internet, the available work is in form of counterfeit material. The Supreme Court is inconsistent on this issue.[5]

---

[1] An infringed copyrighted material is the original while an infringing one is a counterfeit copy that contains a copyrighted work.

[2] Supreme Court case no.1829/B.E. 2553 (2010) (ruling making a copy of content between digital formats is infringement of reproduction and adaptation right under CA 1994 section 27(1))

[3] Under CA 1994 section 31, the fourth secondary infringement element is 'a profit motive'. A client/server user can gain financial benefit from a number of viewers while a P2P user cannot. (*See* chapter 3 -- 3.2.2 Are Posting and Sharing, Types of Secondary Infringement?)

[4] CA 1994 section 4 paragraph 15 states:

"Communication to the public means making a work available to the public by means of performing, lecturing, preaching, playing music, causing the perception by sound or/and image, constructing, distributing or by any other means."

[5] Supreme Court case no. 6804/B.E.2548 (2003), making available of an illegally reproduced 'Kwaokrua' article on a website was found to be primary infringement of the right to communication to the public. However, in 994/B.E.2543 (2000), making available of illegally reproduced copyrighted books ended in a guilty of secondary infringement. In addition, Supreme Court case nos.1829/B.E.2553 (2010) and 3882/B.E.2553 (2010), negated primary communication to the public infringement because content sold and played came from the illegally made resources.

2. The definition is unclear in application to client/server and P2P infringement regarding 'real time showing' and 'actual access'.[6] Currently, means such as, 'performing, lecturing, preaching, playing music and constructing' connote that performance of copyrighted works is real time (or live). It follows that there has to be an audience who is attending the performance (actual access). In contrast, means such as 'distribution' and 'causing perception by image and sound' does not necessarily carry the same connotation.

In order to eliminate these problems, it is recommended that:

1. Thailand differentiate 'communication to the public' and 'distribution' rights by setting up a separate 'distribution' definition. The 'communication to the public' right focuses on performance of a copyrighted work in an intangible form.[7] A copyrighted work is intangible by nature. 'Communication to the public' highlights the display of content irrespective of the product medium. In contrast, the 'distribution' right focuses on making available the original or copies of a copyrighted work "through sale or other transfer of ownership".[8] The original and copies can be in any forms, i.e., physical, digital, etc.[9] In other words, the distinction is that the former is of appreciation of a copyrighted work and the latter is of acquisition of a copy of a copyrighted work.

In principle, distribution should only be classed as secondary infringement because distribution of legal copies is legitimate ('first sale doctrine').[10] Having set up the 'distribution' definition, it will also be able to make the 'first sale doctrine' point clear.[11]

---

[6] Some means of communication in the definition casts doubt about more advance technology means such as 'wire or wireless' or on demand service but is interpreted to encompass display of a work on the internet. Without the means of 'distribution' and 'causing perception of image and sound', a client/server and P2P user can only infringe communication to the public right in the primary sense in cases where a user performs a copyrighted work live. (*See* chapter 3 -- 3.2.1.3 The Right of Communication to the Public.)

[7] WCT Article 8 "Right of Communication to the Public" provides:

"[...], authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them."

[8] WCT Right of Distribution in Article 6 (1) provides: "(1) Authors of literary and artistic works shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their works through sale or other transfer of ownership."

[9] *See* note 5 of WCT Article 6, the expressions 'the original and copies' in the text 'refer exclusively to fixed copies that can be put into circulation as tangible objects'.

[10] *See* chapter 3 -- 3.2.1.3 The Right of Communication to the Public.

[11] Clarification of the 'first sale doctrine' issue is allowed by WCT Right of Distribution in Article 6 (2) which provides:

Secondary infringement focuses on the distribution of counterfeit copies containing copyrighted works. The term 'communication to the public' in CA 1994 § 31 (2) secondary infringement should then be replaced by the term 'distribution'. This will dispel ambiguity of whether client/server and P2P user activities infringe 'communication to the public' or 'distribution' right or whether the infringement is of primary or secondary classification. Distribution of the digital copies in P2P will then be distribution of infringing copies.

In effect, performance of a copyrighted work would be classed as 'communication to the public' primary infringement. Making available of copies of a copyrighted work would be classed as 'distribution' secondary infringement.

2. The current Thailand's CA 1994 definition of 'communication to the public' right be replaced by that of WCT which provides:

"making available to the public of works in a way that the members of the public may access the work from a place and at a time individually chosen by them".[12]

This definition would fill the gap of interpretation among different means of 'communication to the public' under the CA 1994 definition. The WCT definition will clarify that 'communication to the public', online or not, is not totally dependent on real time showing, i.e., the showing can be viewed any time any place whenever an audience wishes ("... from a place and at a time individually chosen by them."). Furthermore, it will also clarify that such communication does not necessarily require actual access. The term "...the members of the public may access the work..." suggests that even if such members may not actually access the work, mere 'making available of the work' is sufficient to satisfy the infringement claim. Finally, both a client/server and P2P user will be subject to infringement of right of communication to the public in a primary discipline whereas the 'for profit' element is not required.

"(2) Nothing in this Treaty shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the exhaustion of the right in paragraph (1) applies after the first sale or other transfer of ownership of the original or a copy of the work with the authorization of the author."

(*See* chapter 3 -- 3.2.1.3 The Right of Communication to the Public.)

[12] WCT Article 8 "Right of Communication to the Public" in note 8 above. (*See* also European Commission, 2015. *Report on the protection and enforcement of intellectual property rights in third countries.* p.22. Available at: https://euipo.europa.eu/ohimportal/documents/11370/0/Report+on+the+protection+and+enforcement+of+intellectual+property+rights+in+third+countries [Accessed: 7 July 2016]. ("...[t]he copyright system in Thailand needs to be further modernised and adapted to more accurately reflect the international standards (such as the WIPO Internet Treaties).”))

6.3 Recommendations for the General Characteristics of an Online Copyright Infringement Protection Remedy

The research finds that client/server and P2P technologies operate differently and different remedies are suitable for different technologies. Section 32/3 of CA 2015 and the US N&T are designed to deal with the client/server whereas the GR of France is for P2P. A proposed legislative framework could be made suitable for specific platforms and could be formulated to cater for future threats. As far as this research is concerned there are general elements which are preferable to the nature of online copyright enforcement.

1. Having a quick response to deter rapid and widespread dissemination of content on the internet;

2. Having warning notices incorporated with informational and educational functions to raise awareness;

3. Separating consistent infringers from periodic ones in an attempt to focus on a reduced number of infringing users;

4. Being fair, proportionate and having due process to balance copyright with other competing rights;

5. Escalating sanction severity to avoid conflict with proportionality;

6. Having judicial review available as part of due process.

It is highly recommended that Thailand facilitate enforcement by changing court-based remedies to non-court based ones.[13] Non-court based remedies were found to be more effective and efficient than court procedures. The proposed legal measures/remedies for Thailand will utilise these elements when outlining the recommendations for client/server and P2P platforms as contained in the sections below.

[13] The remedies can cope with infringement by individuals better than court proceedings in many respects. (Edwards, L., 2010. *Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights*, [Online] Available at: http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf p. 19 [Accessed: 2 December 2015])

6.4 Conclusions of Research Results from Chapter 4 and Recommendations for a Thailand Legislative Framework in Client/Server Technology

This section concludes the research results from a legal comparison between Thailand court proceedings and the US Notice and Takedown. It proposes to set up a standard ISP system with the inclusion of N&T with some adjustments. A framework and method for remedies and proceedings for online copyright infringement by end-users using client/server technology is provided. Should Thailand not accept the proposal and framework, recommendations for a current CA 2015 amendment are also provided.

6.4.1 ISP Definitions and Functions in Relation to Notice and Takedown and the Court Order and Recommendations Regarding ISP Definitions and Functions

It is concluded that a variety of infringing activities, e.g., client/server, P2P, take place in different ISP functions. ISP functions facilitate infringement and determine the extent of the ISP's copyright infringement cooperation.[14] In terms of operation, ICPs (i.e., website operators/owners) and IHPs (i.e., website storage) are responsible for implementation of an enforcement measure because copyright infringement has 'taken place' in their computer systems.[15] The US ICPs and IHPs are subject to N&T by taking down content from their systems or disabling access to it if they want to be shielded by safe harbour provisions.[16] Thai ICPs and IHPs are subject to the court order granted in accordance with the request made by a right holder.

As copyright infringement 'takes place' across all sorts of ISP computer systems and different ISPs have different functions and facility. A request to an ISP for online copyright infringement deterrence has to comply with its limitations. This is so regardless

[14] Mere conduit ISPs (mere 'IAPs' or 'Transitory Digital Network Communication') are not subject to court orders or N&T measures to remove or take down the infringing content. If the 'IAPs' or 'Transitory Digital Network Communications' provide a service in addition to a passage service, e.g., digital storage, applications, 'IAPs' or 'Transitory Digital Network Communications' are not mere conduits. They may then be classed as 'Information Residing on Systems' (IHPs and ICPs). They may well be exposed to N&T requirements or court orders for the additional services in question.

[15] CA 2015 § 33/2 paragraph one states: "In case where it is reasonable to believe that copyright infringement takes place within service provider's computer systems, the right holders may file a motion to the court to cease the infringement."

[16] See *Perfect 10, Inc. v. Ccbill Llc* 488 F. 3d 1102 (9th Cir. 2007), holding that entities hosting websites were an 'Information Residing on the systems' and *UMG Recording, Inc. v. Shelter Capital Partners LLC*, 718 F. 3d 1006 (9th Cir. 2013), holding that a website that furnished space for users to upload their content was also 'Information Residing on the systems'. Moreover, 17 U.S.C.A. § 512 (c) (1) (C) provides: "upon notification of claimed infringement …, responds expeditiously to remove, or disable access to, the material that is claimed to be infringing…"

of remedial provision, e.g., court remedy, or N&T. It is recommended that Thailand educate stake holders about ISP systems and technical issues concerned. More detail is provided in heading 4 section 6.4.4 Recommendations Regarding Thailand Court Proceedings below.

6.4.2 Recommendations Regarding ISP Systematic Standard in Thailand.

It is normally easier to stop infringement at the ISP facility than at individual user's computers.[17] The Thai government should promote and set up a minimum ISP system standard for online copyright protection. At the outset compliance with the standard should be voluntary. Government entities, such as the DIP, can consult with a meeting of stakeholders, e.g., right holders, ISPs and public/user representatives. The purpose of the consultation will be to acquire knowledge from all stakeholders and learn about their concerns. Issues to be discussed should include ISP technical limitations, potential measures available to ISPs and the consequences of same, the need for copyright protection measures, anticipated problems now and in the future (e.g., volume of enforcement notices), costs, human rights protection, etc. A better understanding on these issues could lead to an effective agreement which would result in an appropriate standard for ISPs in Thailand. Potentially, the standard measures could include (1) access disabling, (2) traffic capping, (3) website blocking, (4) content identification (Content ID) and filtering, and (5) system detection of recurring infringing posts, etc.

Any new standard for Thai ISPs should ensure that all ISPs compete on a level playing field. The cost of standard system installations must not drive a small or medium ISP out of business. Either the government or the right holders could assist by providing subsidy to a small or medium ISP. Certain practices such as traffic management and subscriber's account termination already exist and can be incorporated into the subscriber's terms of use/contract.

If the voluntary approach were not to lead to an agreement, the Thai government could then undertake to formally enact relevant legislation. The standards could be legislated by amending CA 2015 to permit the use of delegated legislation. The secondary

[17] Internet Society, 2011. *Perspective on Policy Responses to Online Copyright Infringement: An Evolving Policy Landscape*, [Online] Available at: http://www.internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape p.16 [Accessed: 6 May 2014]

legislation such as a Ministry Notification could include details of a possible standard.[18] A Ministry Notification is preferable because it is more easily amended than an Act to provide flexibility to counter possible future threats.

6.4.3 Recommendations for Adoption of Notice and Takedown with Adjustment for Legal Proceedings.

It is recommended that Thailand adopt a US N&T style remedy. With some procedural modifications, the US N&T system would benefit Thailand in many aspects.

Firstly, CA2015 court procedure cannot be considered as due process. It does not supply an end-user with a right of defence during a trial and also after an order is granted.[19] The US N&T system, for the most part, is more justifiable in this regard as it offers an equal chance to both a right holder and a user in forms of notice and counter notice. If the US system replaced the court procedure, the due process issue may no longer be a problem for Thailand. Moreover, an end-user's freedom of speech is sufficiently secured where an ISP takes down allegedly infringing content by a notice although such a notice is filed without reasonable investigation of infringement on part of a right holder.[20] Nevertheless, it is argued that, under the US system, when an end user counters a notice, the ISP will resume the content within 14 days during which a user will be deprived of his freedom of speech.[21] In these circumstances, Thailand could lower the 14-day period to remove content to secure end-user's freedom of speech and to imply that an end-user has a right to provide defence to the process.

Secondly, this thesis concludes that the magnitude of copyright infringement on the internet necessitates a remedy that offers a simple and reasonable quick response. The Thailand court proceedings remedy does not ensure efficient client/server online copyright infringement protection as it regularly takes 1-3 months for a matter to be heard. The Thai right holders must file a motion to the court on a case by case basis. The

---

[18] Ministry of Notification is a secondary law authorised by a primary law (e.g., an Act of the parliament) and proclaimed by a relevant ministry, in order to indicate, change or update practices and details subsisted in the primary law. In copyright law environment, Ministry of Commerce is authorised to implement CA 1994.

[19] *See* chapter 4 -- 4.6.3 Due Process Comparison.

[20] *See* justification of N&T in chapter 2 – 2.1 Justification and Characteristics of Digital Copyright Protection Remedies.

[21] 17 U.S.C. § 512 (g) (2) (B) and (C) (*See* chapter 4 -- 4.5.2 Notice and Takedown Procedure Concerning Online Infringement.)

US N&T proceedings are more efficient in terms of both time and resources as they have been formulated specifically to circumvent the necessity of a court proceeding.[22] Right holders need to file a lawsuit only if a counter notification is produced. The US system successfully limits the necessity of court proceedings for client/server online copyright infringement cases.[23]

Thirdly, the large number of notifications is a problem in the US. because of the repetition of the same and/or different infringing content.[24] It is suggested that Notice and Staydown (N&S) replace N&T and that an ISP should not have safe harbours protection if the same infringing content re-appears.[25] This approach perhaps puts too much responsibility on an ISP while diminishing user's freedom of speech. A solution to mitigate the harshness is for an ISP to be merely required to have and implement the technological tool, so-called Content Filtering.[26] The technology supports the N&T procedure in that it can record previously-uploaded infringing materials and can prevent them from being re-uploaded.[27] Having set up the technology, an ISP would not be responsible for the reappearance of the content. The technology would solve the current N&T problem of excessive notices.[28] This system supports freedom of speech in that it does not prevent content that is posted for the first time but prevent only the already allegedly infringing content from re-emerging the second time.

---

[22] US House of Representatives, the Committee on the Judiciary, Subcommittee on Courts, Intellectual Property and the Internet, 2014. *Hearing 113th second session*, Available at: https://judiciary.house.gov/wp-content/uploads/2016/02/113-86-87151.pdf p.4 [Accessed: 17 June 2016]

[23] According to Motion Pictures Association of America (MPAA), less than one per cent of notices result in a counter notice. During March-August 2013, of more than 10 million URLs sent to sites, less than 10 URLs countered the noticed claims. (Boyden, B., 2013. *The Failure of the DMCA Notice and Takedown System: A Twentieth Century Solution to a Twenty-First Century Problem* [Online] p.3 Available at: https://copyrightalliance.org/sites/default/files/resources/bruce-boyden-the-failure-of-the-dmca-notice-and-takedown-system.pdf [Accessed: 12 November 2014]

[24] Right owners and telecommunication industries all accept the statistics as proof of the large number of notices. (*See* chapter 4 -- 4.4.2.1 Voluminous Notices Issued.)

[25] This suggestion was proposed in the hearing on DMCA amendment before the US Congress Subcommittee. (*See* chapter 4 -- 4.4.3 Proposed Solution to Notice and Takedown Limitations)

[26] A content filtering technology, currently employed by certain UGC sites (such as YouTube's Content ID), records copyrighted originals in order to match them with the user uploaded infringing material and prevents it from being uploaded. (*See* chapter 2 -- 2.3.5 Content Identification and Filtering)

[27] The technology is already in use in the US. as the court elaborated in *UMG Recording, Inc. v. Shelter Capital Partners LLC*, 718 F. 3d 1006, 1012-13 (9th Cir. 2013). (*See* Chapter 4 note 78.)

[28] It is argued that filters to remove potentially infringing content are largely incapable of accommodating fair use. (*See* Sawyer, M. S., 2009. "Filters, Fair Use, and Feedback: User-Generated Content Principles and the DMCA" *Berkley Technology Law Journal*, Available via SSRN: http://ssrn.com/abstract=1369665) Fair use and exception topics are not included in the thesis and may require further study.

Fourthly, N&T has a problem of user awareness and knowledge of the system.[29] It should have a component that raises user awareness of online copyright infringement and legal protection measures. A notice from a right holder to an ISP should incorporate educative information about, e.g., how a user can legally use copyrighted content, how to assert that his own-generated content is not infringing and what would be the subsequent legal consequences for non-compliance. Moreover, a counter notice should be adjusted to be more user-friendly in order for it to be more readily in use.[30]

Fifthly, a settlement procedure could be established in Thailand. An adjusted N&T system should allow voluntary settlement to take place. A right holder could initiate the settlement process after a counter-notice has been lodged and before the initiation of a lawsuit. If right holders and users agree, the litigation following the N&T process would not be necessary. In this situation, parties in dispute would have chosen to make an attempt to reach an agreement. All parties and institutions would benefit from the settlement. The settlement would be faster than a trial and would reduce the burden on the resources of all parties and institutions concerned.

In conclusion, a modified N&T proceeding for Thailand is outlined below.

1. A notice should be initially produced by a right holder to an ISP.[31] The notice should contain information similar to that of a US notice and should include educative information:

1.1 what is copyright, how to use other's copyrighted content, how to acquire permission to use, what constitutes fair use and copyright infringement,

1.2 in case where a user disagrees, how to file a simple and straightforward counter notice,

---

[29] Many users do not know how to protect their rights by the legal tools provided and that users' amount of counter notices was low. (*See* chapter 2 -- 2.1. Justification and Characteristics of Digital Copyright Protection Remedies.)

[30] This thesis finds that the volume of counter notice is low due many factors of which unsophistication of the user takes part. (*See* chapter 4 -- 4.4.3.1 In Client/Server Technology)

[31] A right holder must bear the cost of infringement detection and of N&T similar to the US. (Leary, B. 2012, "Safe Harbor Startups: Liability Rulemaking under the DMCA", *New York University Law Review*, 87, 1135, p. 1138.) Moreover, it is the right holders who decide whether to submit a notice or not. Recent study has found illegal postings of musical works support music industries in monetising their old songs in YouTube. (Heald, P.J., 2014. "How Notice-and-Takedown Regimes Create Markets for Music on YouTube: An Empirical Study"[Online] Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2416519 [Accessed: 22 September 2014])

1.3 potential civil redress and/or criminal litigations that can follow if a user decides to lodge the counter notice in 1.2,

2. Upon receiving a request/notice, an ISP ceases the infringement by taking down content or disables access to such content, and forwards to the user the notice in 1.

3. If no counter-notice is produced within a certain time, content is then taken down permanently and the ISP can employ content filtering by recording the content prevent it from reappearing. Moreover, if there is no repeat infringement of the same content by the same user, no further proceedings are required;

4. If a counter notice is produced, the right holder will have alternatives:

4.1 Initiating the settlement process with the user;

4.1.1 If agreed at this stage, the settlement can result in a notice of withdrawal, change or approval;

4.1.2 If an agreement cannot be reached, the right holder will need to pursue the 4.2 path;

4.2 filing a motion, perhaps the one similar to CA 2015 § 32/3, or initiating a civil or criminal copyright infringement lawsuit against the user,

5. the ISP's safe harbours can be assumed if an ISP cooperates along these lines.

The above N&T-like system can be adopted in Thailand by either legislation or regulation. Currently, cooperation between right holders and ISPs is practiced and is a good example.[32] Cooperation can be solicited from all sections of society. The Thai Department of Intellectual Property (DIP) is able to centrally organise the cooperation between stakeholders. Such cooperation may result in a Memorandum of Understanding (MOU) or self-regulatory code of conduct.[33] Arguably, sanction would not be necessary if all stakeholders are in agreement. It is unlikely that an ISP will prefer to go to the court if

[32] IP industries such as Thai Entertainment Content Trade Association (TECA), GMM Grammy, Motion Picture Association, and ISPs have cooperation regarding remedies similar to 'notice and takedown'. TECA claims that takedown rate in 2012 and 2013 was more than 90 per cent. (This information is from an email corresponding with a representative from TECA dated 5th February 2014.)

[33] For example, in the US, self-regulation practices in YouTube website. YouTube's terms state "YouTube will terminate a User's access to its Website if, under appropriate circumstances, they are determined to be a repeat infringer." (Hugenholtz, P. B., 2012, "Codes of Conduct and Copyright Enforcement in Cyberspace." In Stamatoudi, I.A., ed. *Copyright Enforcement and the Internet*, Amsterdam: Kluwer Law International, 2010, p.315. Available via SSRN: http://ssrn.com/abstract=2017581)

infringement issues can be effectively dealt with through terms of an agreement. ISPs know that right holders have a legal remedy under CA 2015 § 32/3 for which they can be summoned to join in the court trial. Participating in the negotiation for an agreement is preferable than joining in the trial. If such cooperation does not materialise within a reasonable period, the Thai government should step in and make the system part of legislation.

6.4.4 Recommendations Regarding Thailand Court Proceedings

If Thailand continues to use the existing court procedure remedy under CA 2015 § 33/2, it is recommended that CA 2015 § 33/2 be amended in certain areas to improve it as shown below.

1. Court proceedings should secure due process.[34] To allow the direct infringer to contest the case, CA 2015 § 33/2 paragraph three should be amended to require allegedly direct infringer details and that a subpoena should be sent to such infringer. The required information under CA 2015 section 32/3 paragraph three should include information concerning an alleged infringing user. The alleged user should then be able to defend himself.

2. A notice to an ISP and a settlement process similar to the recommendation in 4.1 above, should be made mandatory before a motion can be filed.

3. It can be concluded that the court order to 'cease the infringement' has extensive repercussions.[35] First it can lead to excessive requests which delay the court trial.[36] Second it can lead to a disproportionate and/or imbalanced order.[37] In order to mitigate such negativity, it is recommended that CA 2015 § 32/3 should be amended to provide the court with guidance for consideration in exercising the 'reasonable'

---

[34] *See* chapter 4 -- 4.3.4 Limitations of the Thailand CA 2015 § 32/3 Court Procedure and Remedy.

[35] CA 2015 §32/3 paragraph three (6) has mainly two remedies-- 1) removal of the alleged infringing content from a service provider's computer system, and 2) cessation of infringement by other means. 'Cessation of infringement' can be any measure which can operate merely partly or completely, temporarily or permanently and proportionately or disproportionately, such as access disabling, traffic shaping or capping, website blocking (IP Address, URL), content identification and filtering, etc.

[36] *See* chapter 4 -- 4.3.4 Limitations of the Thailand CA 2015 § 32/3 Court Procedure and Remedy.

[37] For example, website blocking denies access to the whole website and all usable content as opposed to taking down specific content. (*See* chapter 4 --.4.3.3.1 Website blocking and Disabling Access to Content)

discretion.[38] Singapore legislation can be raised as an example and is recommended for adoption. In determining whether a location is 'flagrantly infringing', the Singaporean Court takes into account the factors provided for by the law.[39] In addition, other factors can be included such as proportionality, economic reasons, trading techniques, the primary purpose of the request, circumstantial damage, the ISP executing facility, business background, and free and fair trade competition. Furthermore, there should be consideration given to rights other than copyright protection such as freedom of speech, fair use and other public rights. These considerations will show concern for rights guaranteed by constitutional democratic regimes and will balance them with requested measures.

4. ISP functions are of the legal and technical knowledge that a practitioner needs to acquire in order to seek for a court order measure that does not cause technical and practical problems. Chapter 4 concludes that the court finding of fact is limited to the scope of argument of the parties in dispute and of parties' presentation.[40] Such limitation can result in a court order not being able to implement by an ISP or not fit with the infringement circumstances.[41] It is recommended that Thailand educate institutions and practitioners with regard to the technical issues concerned.[42] Without an acquired knowledge of ISP functions, their technical availability and limitations, or the nature of infringement activities, it would be a waste of time and resources for all those involved in a trial in which both copyright protection and fundamental rights could not be guaranteed.

---

[38] CA 2015 § 32/3 paragraph four states: "… If it [the court] finds that ... it is necessary and *reasonable* to grant order, it shall impose service providers to cease the alleged infringing acts, ...". [Emphasis added]

[39] For examples, the primary purpose of the website, activities the website provides. (*See* all the factors in chapter 4 -- 4.3.3.1 Website blocking and Disabling Access to Content)

[40] *See* chapter 4 -- 4.3.4 Limitations of the Thailand CA 2015 § 32/3 Court Procedure and Remedy.

[41] For example, a party might seek for content removal from the IAP's system which does not provide an information storage, instead of those of IHP's or ICP's. (*See* chapter 4 -- 4.6.1 ISPs Affected by the Digital Copyright Protection Measures.)

[42] Effective enforcement of intellectual property rights (IPRs) is limited due to a deficiency in IPR framework, which includes officials lacking sufficient knowledge and training on IPR. (European Commission, 2014. *Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee: Trade, growth and intellectual property - Strategy for the protection and enforcement of intellectual property rights in third countries*. p.5 Available at: http://trade.ec.europa.eu/doclib/docs/2014/july/tradoc_152643.pdf [Accessed: 7 July 2016].)

With educational objectives aimed at ISPs and end-users, ISPs could declare their particular functions and available facilities. Having set up the ISP system standard as mentioned in 6.4.2 above, the extent of the court order under the term 'to cease the infringement' can be held as 'reasonable' provided that the order complies with that established standard.[43]

6.5 Conclusions of Research Results from Chapter 5 and Recommendations for a Thailand Legislative Framework in Peer-to-Peer File Sharing Technology.

In this section, conclusion of research results from chapter 5 will be drawn to emphasis the extent of efficiency and effectiveness of GR, its limitations and the potential solutions of Thai CA 2015 remedy and French GR. Recommendations for Thailand will be given and evaluated.

6.5.1 Recommendations Regarding ISP Functions and Service in Peer-to-Peer Copyright Infringement Protection Measures

It can be concluded that in Thailand copyright infringing activities 'take place' in an IAP's system under CA 2015 section 32/3 paragraph one because IAPs, not IHPs or ICPs, are the ones that facilitate end-user internet connections. Hence IAPs can be subject to a court order. In France, IAPs are required to provide the subscription with terms and information about monitoring duty and GR procedures and sanctions and also to inform a subscriber of such terms and information under FIPC Article L. 331-35 paragraph one.[44] They are also required to inform a subscriber of the infringement notification under FIPA Article L. 331-26 paragraph one. [45]

---

[43] The terms 'to cease the infringement' and 'reasonable' are in CA 2015 § 32/3. (*See* discussion of these terms in chapter 4 -- 4.3 Functionality of the Thai Court System in Client/Server Technology)

[44] FIPC Art. L. 331-35 paragraph one – Persons whose activity is to offer access to public online communication services shall include, in contracts entered into with their subscribers, a clear and understandable reference to the provisions of Article L. 336-3 and the measures that may be taken by the Rights Protection Commission. They shall also include, in contracts entered into with their subscribers, the criminal and civil sanctions incurred in the event of copyright and related rights being violated."

[45] FIPA Art. L. 331-26 paragraph one provides: "Where facts likely to constitute a breach of the obligation defined in Article are referred to the Rights Protection Commission, it may send to the subscriber, under its seal and on its own behalf, by email and through the person whose activity is to offer access to public online communication services and that has entered into a contract with the subscriber, …"

It is recommended that Thailand legislation adopt compulsory copyright protection terms and information in the internet subscriptions similar to those shown in FIPC Articles L. 331-26 paragraph one and L. 331-35 paragraph one. The terms should contain further information about the additional proceedings recommended as detailed below.

Moreover, online copyright infringing acts cannot be criminalised under the Thailand Computer-Related Offence Act B.E.2550 (CROA 2007). An ISP cannot be required to store traffic data for copyright protection purpose.[46] In support of this approach, it is recommended that Thailand amend CROA 2007 to require ISPs to keep traffic data for copyright protection purposes. Such ISP duty is reflected in the international Cyber Crime Convention as regards IP offences.[47] Moreover, competent authorities are empowered, *inter alia*, to order ISPs to submit subscriber information.[48] ISPs should be obligated with other proceedings as suggested in the next section.

6.5.2 Recommendations for Thailand in Adopting the Principles of France and Graduated Response Remedy for Peer-to-Peer Online Copyright Protection

The Thai court remedy system does not facilitate the protection of copyright on P2P platform. It is neither effective nor efficient for two reasons. The anonymous nature of users impinges negatively on investigations and traditional civil and criminal proceedings, not to mention the final outcome. The second problem is the large number of infringing users which tends to destabilise the Thai justice system as well as an appropriate remedy under CA 2015 §32/3. The French approach is better able to deal with the two problems.

It is recommended that Thailand revoke the court procedure and adopt GR principles and remedy. GR should be adjusted to allow the use of a technology to facilitate control of P2P along with any other threatening platforms. The recommended legislation described below is for P2P but could be applicable to any potential future threat to online copyright.[49]

---

[46] *See* chapter 3 -- 3.4. Are Client/Server and Peer-to-Peer User Activities Criminal Offences under the Computer-Related Offence Act B.E. 2550(2007)?

[47] Article 10 and 20(1) b

[48] Articles 18(1) b

[49] The HADOPI Act is criticised in that it fails to adapt to fast changing practices on the Internet. (Bellon, A., 2015. "Governing cultural practices on the Internet: the Multi-stakeholder approach tested by

1. Thailand should adopt principles such as subscriber duty, presumption of guilt, minor offence similar to that of France.[50] In brief, a household subscriber would be required to monitor internet usage, not to use it in P2P copyright infringement.[51] The law must be flexible in order to meet the fast infringement move from one platform to another. The authorities should be empowered to proclaim a new monitoring usage rather than amending the law by the parliament. This monitoring duty could probably apply to other internet offences. Breach of the duty is a separate charge from copyright infringement offences. The purpose of this is to avoid the need of a complaint required in copyright offence which is of the compoundable offences.[52] The penalty of the charge would be for a minor offence. The subscriber would be presumed guilty, on account of which an automatic fine would be imposed. Having decided to contest the presumption of guilt, a subscriber has a chance to defend himself in court.

Having adopted the above principles, Thailand may not need to address the issue of balance between copyright and end-user's right to privacy regarding IP address as personal data and data subject identification. It is justified to disclose a household subscriber's identity which associates with the IP address because in this circumstance such disclosure is for the purpose of criminal investigation on breach of monitoring duty charge.[53]

2. It is suggested that Thailand designate an existing telecommunication agency to perform the following functions similar to that of Hadopi organization.

2.1 The thesis concludes that the educational and informational aspects of the notice are the most important functions of effective online copyright

---

institutional arrangements in France" ICPP Milan 2015, Policy Making in Governing the Internet, Available at: http://www.icpublicpolicy.org/conference/file/reponse/1433973174.pdf p.1 [Accessed: 7 January 2016])

[50] Thailand does not have a subscriber onus. A fine as a criminal penalty has to be imposed to a guilty-proved wrongdoer. It can be said that in practice Thailand does not have presumption of fact of copyright infringement counts and the counts are not classed as a minor offence. (*See* chapter 5 -- 5.2.3 Does Thailand Law have Presumption of Guilt and Are Copyright Infringement Charges Minor Offences?)

[51] In a situation such as business place or other large entity where internet access does not require security check, it may be entirely impossible to determine who the copyright infringer was. (Clayton, R., 2012. "Online traceability: who did that?" *Consumer Focus*, Available at: http://www.consumerfocus.org.uk/files/2012/07/Online-traceability.pdf p.30 [Accessed: 10 Sep. 2014])

[52] CRPC 1934 § 121 states:

"The inquiry official is empowered to undertake an enquiry in criminal affairs.

In case of compoundable offences, an enquiry shall not be initiated unless a complaint is lodged."

[53] Whether the disclosure is justified for personal right protection proceeding or not will depend on domestic law that must secure fundamental rights of the public taking to account other principles such as proportionality. (*See* discussion in chapter 2 – 2.1 Justification and Characteristics of Digital Copyright Protection Remedies.)

protection measures and that the existing Thailand court remedy does not have these essential functions.[54] Thailand should establish an appropriate warning notification system. First and second notifications should contain information regarding the copyright system, legal/illegal use of copyright, the consequence of repeat infringement, potential sanctions, and other information similar to that of the French GR.[55]

2.2 A process for a disagreeing subscriber to defend against the allegation should be created. The two notifications should provide information about how to 'counter a notification', e.g., how to acquire the relevant forms, raise and submit an argument/defence, e.g., through the same channel as the preliminary notifications (an email or registered mail). The 'counter notification' procedure may be called upon as evidence in cases where there is a prosecution as shown in 2.3 below.

2.3 In cases where a subscriber repeats the infringement after the two warnings, the case is referred to an enforcement agency (e.g., police, DIP).

3. The enforcement agency should have discretion as to whether to prosecute or not. If an authority decides to prosecute a subscriber, the subscriber is presumed guilty of breaching the internet monitoring duty and a fine will be imposed. An automatic fine ticket will be sent to him. The fine should be set as nominal similar to that of a traffic violation. It should not be fixed in law but authorities should be allowed to settle it in accordance with factual patterns such as commercial motive, intentional/inadvertent infringement, etc.[56]

---

[54] CA 2015 § 32/3 is essentially part of a civil case. A motion request can accommodate these aspects but it is very unlikely in practice. A right holder does not need the court order in sending notifications and initiating criminal prosecution. (*See* chapter 5 -- 5.3.4 The Practical Aspect of Graduated Response's Three Strikes in the Context of Thailand Proceedings.)

[55] For example, the offence of which he is alleged to be guilty, his monitoring obligation, etc. (*See* information in the first and second notification in chapter 5 -- 5.5.3 The HADOPI Act Procedure in P2P Deterrence.)

[56] The current Thai copyright infringement allegations have imprisonment or fines from 10,000 to 200,000 baht (roughly 200 pounds to 4,000 pounds sterling) or both which are too high to be minor offences. (CA 1994 § 69 paragraph one and § 70 paragraph one) If the infringement is for profit, the fines increase to between 50,000 and 800,000 baht (Thai currency or 1,000 pounds and 16,000 pounds sterling), and/or imprisonment between three months and four years (CA 1994 § 69 paragraph two and 70 paragraph two).

4. At this stage, the enforcement agency is empowered to inform ISPs to employ internet traffic management.[57] Upon informed, ISPs would then block or slow down both P2P file sharing applications and content transmission. "The consequences for infringement can include automatic redirection to a different homepage and reduction in internet download speeds."[58] Traffic management has already been practiced by reducing the internet speed for certain platforms at certain times, e.g., in the evening or at the weekend.[59] Upon informed by the authorities, an IAP could continuously reduce the internet speed for a P2P platform whilst not affecting the speed for other platforms.

Upon receipt of a ticket with acknowledgement of the traffic management, an agreed account holder may pay a fine and the traffic management will be withdrawn. A defending account holder can object to the allegation by not paying the fine. In this situation, the ISP must revoke the traffic management and an inquiry official must initiate a criminal prosecution on account of the failure of the subscriber's duty. A copyright infringement charge can also be incorporated depending on the evidence about actual infringer identities.

5. Thailand should provide a mechanism for the termination of an internet subscription contract.[60] In addition to providing the compulsory copyright protection terms as recommended in 6.5.1, ISPs should provide and implement a policy for the termination of certain types of subscribers.[61] Subscription agreements should have a clause stating ISPs may blacklist and terminate a subscription on account of specific

---

[57] Traffic management comprises of 1) traffic shaping, and 2) traffic capping. (*See* chapter 2 --2.3.3. Traffic Management.)

[58] Owen, J.M., 2012. "Graduated Response Systems and the Market for Copyrighted Works", *Berkeley Technology Law Journal,* 27(4), p. 559. Available at: http://scholarship.law.berkeley.edu/btlj/vol27/iss4/14/ (Citing Memorandum of Understanding between ISPs (SBC Internet Services, Inc. et. al) and Content Owners (RIAA et al.) (July 6, 2011), http://www.copyrightinformation.org/sites/default/files/Momorandum of Understanding.pdf).

[59] Thomas, N. 2015. "ISP Traffic Management: BT vs Virgin vs Sky vs TalkTalk vs EE" [Online] Available at: https://recombu.com/digital/article/isp-traffic-management-bt-sky-virgin-media-ee-talktalk_M11045.html# [Accessed: 5 May 2016]

[60] Internet disconnection has already practiced in subscription contracts under certain circumstances, e.g., non-payment of subscription fee. (*See* chapter 2 --.2.3.2 Suspension and De-subscription of an Internet Account)

[61] The US DMCA uses this approach. (*See* chapter 4 -- 4.4.2.3 Policy towards the Termination of Repeat Subscribers and Account Holders)

activities. In general, activities violating laws or breaching a contract should lead to blacklisting and contract termination.[62]

A subscriber who has been previously fined (or found guilty by the court) as shown in 4. above may be blacklisted. If such a subscriber commits another copyright infringement, an ISP is entitled to terminate the subscription contract. The blacklist can last for 6 months. The blacklisted subscriber is not prohibited from applying for another subscription with a new ISP.

6. Optionally, Thailand can utilise internet suspension similar to the approach of France.[63] Internet suspension should be enacted by the law prescribing the circumstance of its application and should be available only to a court. Moreover, internet suspension should be allowed only if it is proved in trial that the subscriber is the same person as the infringer. It should be used as a supplementary sanction to a fine.

In brief, the recommended GR-like remedies are as follows:

1. Right holders detect P2P file sharing of their copyrighted content;

2. Right holders inform ISPs and ISPs then send first notice via email.

3. If the infringement is repeated within a certain period time, a second notification will be sent via registered mail;

4. A subscriber can file a counter-notification against the first and second notices;

5. If there is a further infringement within a certain time period, the third action is to transmit the case to an inquiry official;

6. If the inquiry official decides to incriminate the subscriber, a set amount of fine will be imposed to the subscriber and traffic management will be applied.

7. At this stage:

- If the subscriber pays the fine, the case is dismissed and the traffic management is revoked;

---

[62] *See* an example of this clause practiced by British Telecommunication Term of Use in note 107-8 in chapter 5.

[63] *See* chapter 5 -- 5.4.4 Should termination of internet Access be Supplementary to a Minor Offence?

- If the subscriber refuses to pay the fine, the traffic management is revoked and the inquiry official initiates a case;

8. A fined or convicted subscriber is blacklisted;

9. If the blacklisted subscriber continues to infringe copyright, the ISP may terminate his subscription;

10. A court has the discretion of imposing internet suspension if a subscriber is found guilty of copyright infringement. (This is optional.)

11. All the above proceedings must be declared explicitly in subscriber contracts. ISPs will be safeguarded if they practice in line with this system.

The author considers the approach recommend above to be effective and efficient in P2P copyright enforcement in Thailand in many respects.

1. Legal principles such as a presumption of guilt for a digital copyright online infringement minor offence is in accordance with international standard, e.g., EU, the US.[64] A chance to disprove the presumption in the court guarantees due process of law.[65] The subscriber duty principle could avoid difficulty of actual infringer identification.[66] Although subscriber's IP addresses may contribute to the possibility of wrongful infringer identification, they are still reliable because they normally represent correct information.[67]

It is expected that the subscriber duty will benefit an end-user. Without the duty, if he has been convicted of a 'breach of copyright infringement' in a criminal case and if the right holder then pursues a civil case for compensation, the wrongdoer can hardly deny the fact constituting infringement in the criminal case. The reason being the civil court must infer the fact to the civil case as prescribed by the criminal procedure law.[68] In this

---

[64] *See* chapter 5 -- 5.4.2 Is Subscriber's Reverse Burden of Proof Legitimate?

[65] *See* judicial review experience from the UK in Mansell, R. and Steinmueller, W. E., 2013. "Copyright infringement online: The case of the Digital Economy Act Judicial Review in the United Kingdom", *New Media & Society*. 15(8), 1312.

[66] *See* chapter 5 -- 5.2.2 Does Thailand Law have Internet Subscriber Obligation and Does the CA 2015 Motion Need to identify the Subscriber?

[67] Globally, around one fourth of all internet users misguide the IP address and affect a system which relies on it. (*See* note 121 in chapter 2 -- 2.4.2 Process of Identification of Infringement and Precise Wrongdoers)

[68] In the civil case related to a criminal offence, Thailand Criminal Procedure Code B.E.2477 (1934) (CRPC 1934) § 46 states:

"In delivering the judgement in the civil case, the court shall be bound by the facts as found by the judgement in the criminal case."

situation, the defendant will most probably have to pay compensation. On the contrary, having been convicted of a 'breach of subscriber duty', a wrongdoer would be in a better position in the civil case because there can be no inference about the fact.

2. Notifications would educate subscribers and raise the level end-user awareness with respect to copyright infringement.[69] A system of gradually increasing severity (or literally, 'graduated response') would correspondingly decrease the magnitude of infringement and would filter hard core infringers from intermittent ones.[70] Moreover, notifications can turn illegal downloaders to the legal ones.[71]

3. The automatic fining system can bolster an copyright holder's income in that part of the fine can be given to the copyright holder.[72] The system circumvents the court procedure and could reduce country's and right holder's resource in litigating individual users.[73] A recent study shows that the comparatively modest fine for online infringement is more acceptable than internet access suspension.[74]

---

[69] "A survey published by Consumer Focus in February 2010 found that 73 per cent of consumers do not know what they are allowed to copy or record." Moreover, among P2P users, 44 per cent stated that they believed that their actions were lawful. (Hargreaves, I., 2011. *Digital Opportunity, A Review of Intellectual Property and Growth, An Independent Report*, Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/32563/ipreview-finalreport.pdf [Accessed: 21 December 2015][Internal Citation omitted])

[70] The key figure of GR shows the reducing numbers of infringement at each stage from the first to the third strikes. (*See* chapter 5 -- 5.6.4 Mail Notification Followed by Prosecution in Comparison with Court Procedure and the Court Order Measures.)

[71] "[P]revious studies have shown that illegal Internet downloaders prefer digital sales channels over physical ones when purchasing legally." (Danaher, B. et.al, 2014. "The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France", *The Journal of Industrial Economics,* 62(3), 541, note 8)

[72] In the present regime, the successful copyright holder in the criminal trial is entitled to half of fine imposed by the court under CA 1994 section 76 which states:

"One half of the fine imposed by a judgment shall be paid to the owner of copyright or performers' rights; the right of the owner of copyright or performers' rights to bring a civil action for damages for an amount which exceeds that part of the fine that the owner of copyright or performers' rights has received shall not be prejudiced."

[73] Under CA 2015 § 32/3, a right holder must litigate twice. (*See* chapter 4 -- 4.3.4 Limitations of the Thailand CA 2015 § 32/3 Court Procedure and Remedy.) The legal action incurs excessive resource on both private and public sectors. (Masnick, M. 2010, "RIAA Spent $17.6 Million In Lawsuits... To Get $391,000 In Settlements?", *Techdirt* [Online] Available at: https://www.techdirt.com/articles/20100713/17400810200.shtml [Accessed: 9 September 2016])

[74] Geiger, C. 2014, "Challenges for the Enforcement of Copyright in the Online World: Time for a New Approach," *Max Planck Institute for Innovation and Competition Research Paper No.14-01* [Online] Available at: https://www.researchgate.net/publication/260791463_CHALLENGES_FOR_THE_ENFORCEMENT_OF_COPYRIGHT_IN_THE_ONLINE_WORLD_TIME_FOR_A_NEW_APPROACH note 74 [Accessed: 28 October 2015]

4. Traffic management is in accordance with principle of proportionality and principle of minimum. Reduction of internet speed can be considered as a sanction in proportion with failure of monitoring duty. It is comparatively of lower severity than website blocking which denies the public accessing to both legal and illegal content subsisted in the blocked website. Traffic management is only temporarily and will be immediately revoked if the subscriber refuses the allegation and opts to defend the prosecution at the inquiry stage and/or in a court trial.

Traffic management benefits both content industry and ISPs.[75] Content Industries support this policy.[76] ISPs willingly desire to use traffic management because P2P file sharing requires a high volume of bandwidth.[77] Moreover, traffic management restrains hard core P2P file sharers who unresponsively download huge amounts of data and exceed their ISPs internet fair usage policy which in turn affects the internet traffic in general.[78] Traffic management is actually already practiced in slowing down file-sharing.[79] File sharing with a copyright infringement claim is a more concrete ground for such management.

Perhaps the only drawback of traffic management is that it does not differentiate between legal and illegal content.[80] In consequence, it can adversely affect the legal use of P2P file-sharing. However, research has shown that more than half of P2P file sharing involve illegal exchange of copyrighted content.[81] This would lend support for the introduction of traffic management in Thailand.

---

[75] Wisegeek, n.d., "What Is a Bandwidth Cap?" [Online] Available at: http://www.wisegeek.com/what-is-a-bandwidth-cap.htm [Accessed: 4 July 2014].

[76] *Ibid.*

[77] P2P occupies more than half of global internet traffic. (*See* chapter 2 -- 2.2.3 Peer-to-Peer Protocol)

[78] Blabey, D. 2014. "A guide to broadband fair use policy (FUP)"[Online] Available at: http://www.simplifydigital.co.uk/faqs/what-is-a-fair-use-policy/ [Accessed: 24 June 2016] ("Fair usage policies are designed to stop a small number of users from essentially hogging all of the traffic at the exchange by downloading huge amounts of data each month.")

[79] *See*, for example, Virgin Media Cable traffic management policy at note 73 in chapter 2.

[80] "The Internet does not distinguish between copyright content and non-copyright content." (Internet Society, *op.cit*., p.16.)

[81] *See* chapter 2 -- 2.2.3 Peer-to-Peer Protocol. (Taking BitTorrent traffic as an example, nearly two-thirds of the traffic is estimated to be copyrighted content shared illegitimately. (63.7% of all Bittorrent traffic or 11.4% of all internet traffic) (Envisional 2011, *Technical Report: An Estimate of Infringing Use of the Internet* [Online] Available at: http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf p.2 [Accessed: 23 October 2013])

5. Before a fine is imposed or before the court renders a decision, it may not be easy for an ISP to determine whether a subscriber is infringing because copyright infringement is a complex matter.[82] However, when a fine has already been paid previously or the subscriber has already been convicted, these facts alone will safeguard an ISP and allow it to be more confident in blacklisting a subscriber and in terminating an internet contract.

6. Under the court proceedings, allegation of internet suspension in violation of presumption of innocence can be avoided. Sentenced by the court, the suspension will have been given due process. These conditions would escape repetition of the problem encountered by France.

Without internet suspension legal enactment, if all ISPs cooperated with each other and with right holders by refusing a client subscription, such refusal would be tantamount to a suspension of the internet. This could turn out to be an identical problem to that of France. Indeed, if public administrative authorities cannot practice suspension, there is no justification for allowing the private sector to do so. In this situation a subscriber's fundamental right to freedom of speech would be undermined in circumstances not prescribed by law. Learning from France's experience, a sensible right holder and an ISP may think twice about practicing internet suspension. An ISP should not be allowed to prohibit a subscriber, by a clause in a contract, from applying for another internet service. Neither should all ISPs be allowed to blacklist a subscriber on internet suspension.

In conclusion, this thesis finds that the problem with both client/server and P2P end user infringement in the online environment are that it involves (1) a large number of end users; (2) the ease of reproduction and distribution of content; (3) lack of user awareness; and (4) limitation of legal proceedings. In dealing with these complex issues, Thailand has chosen the traditional court procedure by enacting Copyright Act (No.2) B.E.2558. The thesis has found that Thailand's court procedure is not effective in a digital online copyright enforcement context because it is costly, complex and slow. Because of this, the rights of right holders are not adequately merited. In addition, the rights of end-

[82] Eivazi, K. 2012, "Is termination of internet users' accounts by an ISP a proportionate response to copyright infringement?" *Computer Law & Security Review*, 28(4), 458. p.462 [Internal Citation omitted]

users themselves are not adequately warranted because they are not given a chance to be heard in the court hearing. In view of this, these conclusions are by and large in line with an EU report which concludes that the court system is slow, and costly. In 2015, the same year that Thailand enacted Copyright Act (No.2) B.E.2558, the European Commission criticised the Thai system in its Report on the Protection and Enforcement of Intellectual Property Rights in Third Countries which stated:

"Actions against digital piracy have not been sufficient. An Internet Service Provider only becomes liable for copyright infringement after a court order, which the court system in Thailand is unlikely to quickly deliver and would cause significant and repeated legal fees. A more cost effective system to enforce copyright online would be opportune.[...]"[83]

The thesis recommends a framework which adopts and further develops the Notice and Takedown and Graduated Response systems in Thailand by way of legislation, cooperative regulation and functional operation. It proposes remedies that reduce reliance on criminal and civil litigation in the Thai courts. The proposed Notice and Takedown and Graduated Response remedies are intended to balance copyright with freedom of speech and, at the same time, ensuring due process and other human rights.[84] Copyright owners' and end-users' rights, including those of ISPs, are guaranteed. The author considers the recommended sanctions are proportionate and remedies are quick and cost effective in response to massive, rapid and widespread digital dissemination and would assist to alleviate excessive burdens on Thailand's judicial resource. These remedies are constructive and would raise social awareness as to the issue of digital online copyright infringement whilst providing end-user access to justice. Furthermore, certain recommendations introduce legal principles to facilitate legal proceedings (such as subscriber's duty, presumption of guilt). If necessary, such principles could potentially be applied to other computer-related offences. Finally, technological measures also have the potential to assist with enforcement, compromising the severity of sanctions. In the light

[83] European Commission, 2015. *Report on the protection and enforcement of intellectual property rights in third countries.* p.22. Available at: https://euipo.europa.eu/ohimportal/documents/11370/0/Report+on+the+protection+and+enforcement+of+intellectual+property+rights+in+third+countries [Accessed: 7 July 2016].

[84] *See* chapter 4: Notice and Takedown: Thailand and US Approaches and chapter 5: The Thailand and France Approaches to Graduated Response.

of these advantages, the recommended framework does not attempt to benefit copyright owners alone: end-users, ISPs, the public, enforcement agencies, the court, the copyright system, and Thailand as a whole would also benefit from a new legal framework to combat digital online copyright infringement.

List of References

Books and Articles

Amornpinyokiat, P., 2010. *Computer-Related Crime B.E. 2003 Explanation*. Bangkok: SE-Ed Plc. [Thai]

Aguiar, L. and Martens, B., 2013. *Digital Music Consumption on the Internet: Evidence from Clickstream Data.* [Online], Available at: http://www.scribd.com/doc/131005609/JRC79605 [Accessed: 23 June 2014])

Aguiar, L. et. al., 2015 "Online Copyright Enforcement, Consumer Behavior, and Market Structure." [Online] Available at: http://druid8.sit.aau.dk/druid/acc_papers/khu2mchxelh7g4fvnc9pio6cdh71.pdf [Accessed: 16 Sep. 2015]

Anagnostakis, K. et.al, 2006. "On the Impact of Practical P2P Incentive Mechanisms on User Behavior." *NET Institute Working Paper No. 06-14* [Online] Available at: http://netecon.seas.harvard.edu/NetEcon07/Papers/zghaibeh_07.pdf [Accessed: 6 March 2016]

Aroba, N., 2013. *Implementation and Success Analysis of Various Global Graduated Response Programs for Piracy with Special Focus on the "Six Strikes" Policy*. Bachelor Degree. Thesis, University of Arizona.

Andy, 2013. "Three Strikes and You're Still in- France Kills Piracy Disconnections." [Online] Available at: http://torrentfreak.com/three-strikes-and-youre-still-in-france-kills-piracy-disconnections-130709/ [Accessed: 8 May 2015])

BBC, 2007. "Thailand blocks access to YouTube." [Online] Available at: http://news.bbc.co.uk/1/hi/world/asia-pacific/6528303.stm [Accessed: 17 February 2015]

Bellon, A.2015. "Governing cultural practices on the Internet : the Multi-stakeholder approach tested by institutional arrangements in France." ICPP Milan 2015, Policy Making in Governing the Internet, Available at: http://www.icpublicpolicy.org/conference/file/reponse/1433973174.pdf [Accessed: 7 January 2016]

Berne, X., 2015. "Hadopi: several sentenced to 300 subscribers and 500 euro fine. The last sentence?" [Online] Available at: http://www.nextinpact.com/news/96525-hadopi-plusieurs-abonnes-condamnes-a-300-et-500-euros-d-amende.htm [French] [Google Translation] [Accessed: 8 January 2016]

Blabey, D. 2014. "A guide to broadband fair use policy (FUP)."[Online] Available at: http://www.simplifydigital.co.uk/faqs/what-is-a-fair-use-policy/ [Accessed: 24 June 2016]

Blakeney, M. n.d., *Guidebook on Enforcement of Intellectual Property Rights.* [Online] Available at:http://trade.ec.europa.eu/doclib/docs/2005/april/tradoc_122641.pdf [Accessed: 10 Nov. 2013])

Blocman, A., 2011. "State Council Confirms Legality of the HADOPI Decrees." [Online]. Available at: http://merlin.obs.coe.int/iris/2011/10/article15.en.html [Accessed: 1 July 2016].

Boardman, M., 2011. “Digital Copyright Protection and Graduated Response: A Global Perspective.” *Loyola of Los Angeles International and Comparative Law Review*, 33, 223. Available at: http://digitalcommons.lmu.edu/ilr/vol33/iss2/1 [Accessed: 31 May 2015]

Borland, J., 2004. “Covering tracks: New privacy hope for P2P.”[Online], Available: http://news.cnet.com/2100-1027-5164413.html [Accessed: 24 July 2014].

Boyden, B., 2013. “The Failure of the DMCA Notice and Takedown System: A Twentieth Century Solution to a Twenty-First Century Problem.” [Online] Available at: https://copyrightalliance.org/sites/default/files/resources/bruce-boyden-the-failure-of-the-dmca-notice-and-takedown-system.pdf [Accessed: 12 November 2014]

Brain, M., n.d. “How Gnutella Works” [Online] Available at: http://computer.howstuffworks.com/file-sharing3.htm [Accessed: 26 June 2014])

Brain, M. and Crosby, T., n.d. “How email works” [Online], Available at: http://computer.howstuffworks.com/e-mail-messaging/email.htm [Accessed: 17 June 2014]

Brand, O., 2007. “Conceptual Comparison: Towards a Coherent Methodology of Comparative Legal Studies.” *Brooklyn Journal of International Law*, 32(2).

Bridy, A., 2012. “Graduated Response American Style: Six Strikes Measured against Five Norms.” *Fordham Intellectual Property, Media and Entertainment Law Journal,* 23, 1, Available at: http://www.fordhamiplj.org/wp-content/uploads/2013/01/C01_Bridy.pdf [Accessed: 4 November 2015].

Broadband Stakeholder Group, 2013, “Broadband providers launch new traffic management transparency code.” [Online] Available at: http://www.broadbanduk.org/2011/03/14/broadband-providers-launch-new-traffic-management-transparency-code/ [Accessed: 2 July 2014]

Brown, M. 2009, “White Paper: How BitTorrent Works” [Online] Available at: http://www.maximumpc.com/article/features/white_paper_how_bittorrent_works [Accessed: 26 June 2014]

Buford, J.F., Yu, H. and Lua, E.K., 2009, "Chapter 7 - Search." *In:* Buford, J.F. et. al., eds. *P2P Networking and Applications*. Boston, 2009.

Buell, S.W. and Griffin, L.K., 2012. “On the Mental State of Consciousness of Wrongdoing.” *Law and Contemporary Problem*, 75(2), 133. [online] Available at: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1671&context=lcp [Accessed: 4 March 2016]

Carmack, C., n.d., “How BitTorrent Works” [Online] Available at: http://computer.howstuffworks.com/bittorrent1.htm [Accessed: 27 June 2014]

Chirgwin, R., 2012. “Russian upstart claims BitTorrent-killer: ‘Pirate Pay’ names Microsoft as investor” [Online]. Available at: http://www.theregister.co.uk/2012/05/13/pirate_pay_dos_against_torrents/ [Accessed: 30 June 2016].

Clayton, R., 2012. “Online traceability: who did that?” *Consumer Focus*, Available at: http://www.consumerfocus.org.uk/files/2012/07/Online-traceability.pdf [Accessed: 10 Sep. 2014]

Cobia, J. 2009, “The Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process”, *Minnesota Journal of Law, Science & Technology*, 10(1), 387-411

Conradi, M. 2003. “Liability of an ISP for allowing access to file sharing networks”, *Computer Law & Security Report,* 19(4).

Cutlack, G. 2015. “Best free Android Apps 2015” [Online] Available at: http://www.techradar.com/news/phone-and-communications/mobile-phones/70-best-free-android-apps-2013-687252 [Accessed: 17 June 2015]

Danaher, B. et.al, 2014. “The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France.” *The Journal of Industrial Economics,* 62(3), pp. 541-553.

Davies, W. and Media, D. n.d. “The Difference Between Peer-to-Peer and Client/Server Networks.” [Online] Available at: http://science.opposingviews.com/difference-between-peertopeer-client-server-networks-1122.html [Accessed: 18 June 2014])

Dachis, A., 2010. “How to Get Started with Usenet in Three Simple Steps” [Online] Available at: http://lifehacker.com/5601586/how-to-get-started-with-usenet-in-three-simple-steps [Accessed: 25 June 2014]

Depreeuw, S. and Hubin, J., 2014. *Study on the Making Available Right and its Relationship with the Reproduction Right in Cross-Border Digital Transmissions*, [Online] Available at: http://ec.europa.eu/internal_market/copyright/docs/studies/141219-study_en.pdf [Accessed: 3 December 2015]

Duke, 2012. “The Effectiveness of Anti-Piracy Laws; Lessons to Learn from Hadopi” [Online] Available at: http://legalpiracy.wordpress.com/2012/03/06/effectiveness-hadopi/ [Accessed: 25 June 2014])

Dunaytsev, R.; et al. 2012. “A Survey of P2P Traffic Management Approaches: Best Practices and Future Directions.” *Journal of Internet Engineering*, 5(1), 318, Available at: http://www.jie-online.org/index.php/jie/article/viewFile/90/52 [Accessed: 2 May 2014])

Durrieu, R.F., n.d. “Terrorism, organized crime, drug trafficking and due process” [Online] Available at: https://translate.google.co.uk/translate?hl=en&sl=es&u=http://www.estudiodurrieu.com.ar/articulo_2013_03_21.html&prev=search [Accessed: 10 October 2015]

Edwards, L., 2010. *Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights*, [Online] Available at: http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf [Accessed: 2 December 2015])

Elton, S. 2013. "Graduated responses to online piracy: Approaches taken in the United States and around the world." In: Deflem, M., ed. *Music and Law (Sociology of Crime, Law and Deviance, Volume 18)* Emerald Group Publishing Limited, pp.37-58. Available via Emerald: http://dx.doi.org/10.1108/S1521-6136(2013)0000018005 [Accessed: 16 October 2015].

Elton, S. 2014. "A Survey of Graduated Response Programs to Combat Online Piracy," *Journal of the Music & Entertainment Industry Educators Association.* 14(1), pp.99-

122. Available at: http://www.meiea.org/Journal/Vol.14/Elton-MEIEA_Journal_vol_14_no_1_2014-p89.pdf [Accessed: 6 July 2016]

Eivazi, K., 2012. "Is termination of internet users' accounts by an ISP a proportionate response to copyright infringement?" *Computer Law & Security Review*. 28(4) 458.

Envisional, 2011. *Technical Report: An Estimation of Infringing Use of the Internet*, [Online] Available at: http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf [Accessed: 14 June 2014].

Ernesto, 2010. "Truly Decentralized BitTorrent Downloading Has Finally Arrived." [Online] Available at: http://torrentfreak.com/truly-decentralized-bittorrent-downloading-has-finally-arrived-101208/ [Accessed: 25 June 2014]

Ernesto, 2013. "Music biz Demands Piracy Filter from Torrent Sites or else." [Online] Available at: http://torrentfreak.com/music-biz-demands-piracy-filter-from-torrent-sites-or-else-130701/ [Accessed: 25 June 2014]

Ernesto, 2014. "This is how the UK piracy warnings will work."[Online] Available at: http://torrentfreak.com/how-uk-piracy-warnings-work-140517/ [Accessed: 18 Aug. 2014]

European Court of Human Rights, 2015. "ECHR Press release: Blocking without a legal basis users' access to YouTube infringed the right to receive and impart information".

European ASEAN Business Centre (EABC), 2013. "Protecting your Intellectual Property in Thailand" [Online], available: http://www.eabc-thailand.eu/images/files/EABC_PROTECTING_PROPERTY_RIGHT.pdf [accessed: 7 January 2014]

France, The State Council, 2011. "The Council of State rejects requests from Apple Inc and French Data Network against the decrees *Hadopi*"[Online]. Availble (in English by google translation) at: https://translate.google.co.uk/translate?hl=en&sl=fr&u=http://www.nancy.cour-administrative-appel.fr/Actualites/Communiques/Decrets-Hadopi&prev=search [Accessed: 1 July 2016].

Geiger, C., 2014, "Challenges for the Enforcement of Copyright in the Online World: Time for a New Approach," *Max Planck Institute for Innovation and Competition Research Paper*, 14(1) [Online] Available at: https://www.researchgate.net/publication/260791463_CHALLENGES_FOR_THE_ENFORCEMENT_OF_COPYRIGHT_IN_THE_ONLINE_WORLD_TIME_FOR_A_NEW_APPROACH [Accessed: 28 October 2015].

Giblin, R., 2014. "Evaluating Graduated Response." *Columbia Journal of Law & the Arts*, 37(2), 147.

Giblin, R., 2014. "When ISPs Become Copyright Police." *IEEE Internet Computing*, 18(2), 84.

Gil, P. 2014, "The Best Torrent Downloading Software, 2014"[Online] Available at: http://netforbeginners.about.com/od/downloadingfiles/tp/best-torrent-downloading-software-2012.htm [Accessed: 25 June 2014]).

Ginsburg, J. C. and Ricketson, S. 2006, "Inducers and Authorisers: A Comparison of the US Supreme Court's Grokster Decision and the Australian Federal Court's Kazaa Ruling."

Media & Arts Law Review, 11(1) Available via SSRN: http://ssrn.com/abstract=888928 [Accessed: 18 June 2016]

Google, n.d., "How Content ID works." [Online] Available at : https://support.google.com/youtube/answer/2797370?hl=en [Accessed: 14 December 2014]

Graduatedresponse.org, n.d., "France"[Online] Available at: http://graduatedresponse.org/new/?page_id=24 [Accessed: 1 July 2016]

Green, J., n.d., "How do people earn money from YouTube?"[Online], Available at: https://www.quora.com/How-do-people-earn-money-from-YouTube-1 [Accessed: 5 February 2016]

Halbert, D., 2009. "Mass Culture and the Culture of the Masses: A Manifesto for User - Generated Rights." *Vanderbilt Journal of Entertainment and Technology*, 11, 921.

Hargreaves, I., 2011. *Digital Opportunity, A Review of Intellectual Property and Growth, An Independent Report*.[Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/32563/ipreview-finalreport.pdf [Accessed: 21 December 2015].

Helman, L., 2010. "Pull Too Hard and the Rope May Break: On the Secondary Liability of Technology Providers for Copyright Infringement." *Texas Intellectual Property Law Journal*. 19, 111.

Heald, P.J., 2014, "How Notice-and-Takedown Regimes Create Markets for Music on YouTube: An Empirical Study"[Online] Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2416519 [Accessed: 22 September 2014]

Hugenholtz, P. B., 2012, "Codes of Conduct and Copyright Enforcement in Cyberspace." In Stamatoudi, I.A., ed. *Copyright Enforcement and the Internet, Information Law Series*, Amsterdam: Kluwer Law International, 2010, pp.303-320. Available via SSRN: http://ssrn.com/abstract=2017581.

IFPI, 2012. *Digital Music Report 2012*, Available at: http://www.ifpi.org/content/library/dmr2012.pdf [Accessed 23 October 2013]

ILaw Freedom, 2015. "October 2015: Famous people and police arrested for *lese majeste* case, giving flowers charged for sedition and journalists were summoned." [Online] Available at: http://freedom.ilaw.or.th/en/report/october-2015-famous-people-and-police-arrested-lese-majeste-case-giving-flowers-charged-sedit [Accessed: 16 February 2016]

Indana, N., 2003. "Copyright Protection in Information Technology Age," [Thai.] Available: http://people.su.se/~nain4031/copyrightIT.htm [Accessed: 13 Dec.2013.]

Internet Society, 2011. *Perspective on Policy Responses to Online Copyright Infringement: An Evolving Policy Landscape*, [Online] Available at: http://www.internetsociety.org/perspectives-policy-responses-online-copyright-infringement-evolving-policy-landscape [Accessed: 6 May 2014]

International Bureau, WIPO, n.d. *The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)*[online]. Available at : http://www.wipo.int/export/sites/www/copyright/en/activities/pdf/wct_wppt.pdf [Accessed: 19 December 2013.]

IP Kat, 2015. " BGH on blocking injunctions: first go after the source."[Online] Available at: http://ipkitten.blogspot.co.uk/2015/11/bgh-on-blocking-injunctions-first-go.html [Accessed: 20 May 2016])

IP Kat, 2015. "Blocking orders across Europe: personality disorder or are the Swedes right?"[Online] Available at: http://ipkitten.blogspot.co.uk/2015/12/blocking-orders-across-europe.html [Accessed: 20 May 2016]

Jacobsen, S.S. and Petersen, C.S. 2011. "Injunction against Mere Conduit of Information Protected by Copyright: A Scandinavian Perspective." *International Review of Intellectual Property and Competition Law*, 42(2), 151.

Khopuangklang, K., 2011. "Should ISPs in Thailand act at the behest of the entertainment industry to control P2P file sharing?" *European Intellectual Property Review*, 33(10), 632.

Konstantinou, I., 2013. *The compatibility of a Graduated Response System at EU level with the fundamental human rights to privacy, data protection and freedom of expression*. LL.M. thesis, Tilburg University.

Kiss, J., 2014. "Privacy tools used by 28% of the online world, research finds" [Online] Available at: http://www.theguardian.com/technology/2014/jan/21/privacy-tools-censorship-online-anonymity-tools [Accessed: 11 Sep. 2014]

Leary, B., 2012. "Safe Harbor Startups: Liability Rulemaking under the DMCA." *New York University Law Review*, 87, 1135.

Lemley, M.A., 2007. "Rationalizing Internet Safe Harbors." *Journal on Telecommunications & High Technology Law*, 6(1) 101.

Li, J., 2007. "A Survey of Peer-to-Peer Network Security Issues" [Online] Available at: http://www.cse.wustl.edu/~jain/cse571-07/ftp/p2p/#ddos [Accessed: 11 Sep. 2014]

Lippma, M., 2010. *Contemporary Criminal Law: Concepts, Cases, and Controversies*, Los Angeles: Sage Publications.

Mansell, R. and Steinmueller, W. E., 2013. "Copyright infringement online: The case of the Digital Economy Act Judicial Review in the United Kingdom." *New Media & Society*, 15(8), 1312.

Masnick, M., 2010. "RIAA Spent $17.6 Million In Lawsuits... To Get $391,000 In Settlements?" *Techdirt* [Online] Available at: https://www.techdirt.com/articles/20100713/17400810200.shtml [Accessed: 9 September 2016]

McIntyre, J. J., 2011. "Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected as Personally Identifiable Information." *DePaul Law Review*, 60(3) Available via SSRN: http://ssrn.com/abstract=1621102

Meyer, T. and Van Audenhove, L., 2012. "Surveillance and Regulating Code: An Analysis of Graduated Response in France." *Surveillance & Society,* 9(4), 365. Available at: http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/reg_code/reg_code [Access: 29 April 2015]

Mitchell, B., n.d. "P2P"[Online] Available at: http://compnetworking.about.com/od/p2ppeertopeer/g/bldef_p2p.htm [Accessed: 18 June 2014]

Monagham, J., 2011. “Social Networking Websites’ Liability for User Illegality.” *Seton Hall Journal of Sports and Entertainment Law*, 21, 499.

Muir, A., 2013. “Online copyright enforcement by Internet Service Providers.” *Journal of Information Science*, 39 (2), 256.

Mundhra, A., n.d. “What is an IP Address and Difference Between a Static and Dynamic IP Address?” [Online] Available at: http://www.guidingtech.com/8987/gt-explains-what-is-an-ip-address-and-difference-between-a-static-and-dynamic-ip-address/#top [Accessed: 22 July 2014]

Murray, A., 2010. *Information Technology Law: The Law and Society*, Oxford University Press: Oxford.

Organisation for Economic Co-operation and Development (OECD), 2009. *Piracy of Digital Content*. Available at: http://www.oecd.org/sti/ind/piracyofdigitalcontent.htm [Accessed: 6 May 2014].

Out-Law.com, 2007. “Emails can infringe copyright, ruling: Think twice before forward” [Online], Available at: http://www.theregister.co.uk/2007/02/15/email_copyright_infringement/ [Access: 18 June 2014]

Owen, J.M., 2012. “Graduated Response Systems and the Market for Copyrighted Works.” *Berkeley Technology Law Journal,* 27(4). Available via SSRN: http://ssrn.com/abstract=1369665)

Pakinkis, T., 2014. “Weatherley: 'Cutting off ad revenue to illegal sites is key to piracy battle.” [Online] Available at: http://www.musicweek.com/news/read/weatherley-cutting-off-ad-revenue-to-illegal-sites-is-key-to-piracy-battle/058830 [Accessed: 10 July 2014]

Parker, K.R.L., 2014. “Do Not Forward: Why Passing Along an Email May Constitute Copyright Infringement.” *Northwestern University Law Journal*, winter, Available at: http://nulj.org/sites/default/files/files/Parker_Final%20Draft_4_23_2014.pdf [Access: 18 June 2014].

Patel, A.R., 2010. "BitTorrent Beware: Legitimizing BitTorrent against Secondary Copyright Liability." *Appalachian Journal of Law*, 10, 119.

Pavlick, P., 2013. “Music Lockers: Getting Lost in a Cloud of Infringement.” *Seton Hall Journal of Sports and Entertainment Law*, 23, 247.

Peukert, A. 2009, “A Bipolar Copyright System for the Digital Network Environment.” In: Strowel, A. *Peer-to-Peer File Sharing and Secondary Liability in Copyright Law*, 2009. Cheltenham: Edward Elgar.

Piatek, M., Kohno, T. and Krishnamurthy, A., 2008. “Challenges and Directions for Monitoring P2P File Sharing Networks or Why My Printer Received a DMCA Takedown Notice.” [Online] Available at: http://dmca.cs.washington.edu/dmca_hotsec08.pdf [Accessed: 10 Sep. 2014]

Pitiyasak, S., 2003. "Does Thai law provide adequate protection for copyright infringement on the Internet?" *European Intellectual Property Review,* 25(1), 6.

Private Tunnel, [Online] Available at: https://www.privatetunnel.com/index.php?referral=OPENVPN [Accessed: 4 August 2014]

Quinn, G., 2009. “Sample DMCA Take Down Letter.” [Online] Available at: http://www.ipwatchdog.com/2009/07/06/sample-dmca-take-down-letter/id=4501/ [Accessed: 9 June 2016]

Rambaud, S., 2010. “Illegal internet file downloads under HADOPI 1 and 2.” [Online] Available at: http://www.twobirds.com/en/news/articles/2012/france-struggle-against-illegal-downloads-050510 [Accessed: 6 January 2016]

Rajah S.C., I., n.d. “Supporting the Digital Environment: the Copyright (Amendment) Bill 2014.“[Online], Available at: http://www.scca.org.sg/images/resources/Announcements/SMS%20Note%20on%20Copyright%20Bill.pdf [Accessed: 5 June 2015]

Reicher, A., 2011. “Redefining Net Neutrality After *Comcast v. FCC.*” *Berkeley Technology Law Journal*, 26(1), 733.

Rimmer, M., 2007. *Digital Copyright and the Consumer Revolution: Hands Off My IPod*, Cheltenham: Edward Elgar.

Rue, F.L., 2011. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/17/27.

Runbox.com, n.d. “How Email Works.” [Online], Available at: https://runbox.com/email-school/how-email-works/ [Accessed: 17 June 2014]

Ryan, J., 2010. “Internet access controls: Three Strikes ‘Graduated Response’ Initiatives.” [Online] Available at: http://www.iiea.com/documents/draft-overview-of-three-strikes-measures-nlm-study [Accessed: 2 December 2015]

Sakawee, S., 2014. “Thailand’s Coup Spreads from Streets to the Web, 219 Sites Blocked so far.” [Online] Available at: https://www.techinasia.com/thailands-coup-spreads-streets-web-219-sites-blocked/ [Accessed: 24 Aug. 2015]

Sandvine, 2013. *Global Internet Phenomena Report,* [Online]. Available at: https://www.sandvine.com/downloads/general/global-internet-phenomena/2013/2h-2013-global-internet-phenomena-report.pdf [Accessed: 2 May 2014]

Sawyer, M. S., 2009. “Filters, Fair Use, and Feedback: User-Generated Content Principles and the DMCA.” *Berkley Technology Law Journal*, Available via SSRN: http://ssrn.com/abstract=1369665

Schulze, H. and MochalskiIpoque, K., 2009. “Ipoque Internet Study.” [Online] Available at: http://www.ipoque.com/sites/default/files/mediafiles/documents/internet-study-2008-2009.pdf [Accessed: 3 June 2014]

Seng, D., 2014. “The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices.” *Virginia Journal of Law and Technology*, Forthcoming. Available via SSRN: http://ssrn.com/abstract=2411915 or http://dx.doi.org/10.2139/ssrn.2411915

Serbin, D., 2012. "The Graduated Response: Digital Guillotine or a Reasonable Plan for Combating Online Piracy?" *Intellectual Property Brief*, 3(3), 42.

Sfetcu, N., 2014. “Client/Server Architecture.” [Online]. Available: http://www.teleactivities.com/clientserver-architecture/ [Accessed: 13 June 2014].

Shayesteh, S.A. 2000. “High-Speed Chase on the Information Superhighway: The Evolution of Criminal Liability for Internet Piracy.” *Loyola of Los Angeles Law Review*, 33, 183.

Shipley, T.G. and Bowker, A., 2013. *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*. Amsterdam, London: Elsevier.

Stessens, G., 2004. *Money Laundering: A New International Law Enforcement Model*, Cambridge: Cambridge University press.

Stokes, S., 2009. *Digital Copyright: Law and Practice,* 3rd ed. Oxford: Hart Publishing.

Storie, M. N., n.d. “Best Practices for Wireless Access Providers to Avoid Copyright Infringement Liability.” [Online] Available at: http://www.stoel.com/files/BestPractices_WirelessAccessProviders.pdf [Accessed: 1 October 2015]

Strowel, A. 2009. “Internet piracy as a wake-up call for copyright law makers – Is the *graduated response* a good reply?” *WIPO Journal*, 1(1), 75.

Suphapholsiri, T., 1990. *Principles of Copyright Law.* Bangkok: Nititham Publishing House. [Thai].

Suwanprateep, D., 2010. “The Offence of Contributory Infringement of Intellectual Property Rights.” *The Central IP and IT Court Journal 12th: Special Issue 2010*, 226. [Thai]

Techopedia, n.d., “Network Service Provider.” [Online] Available at: http://www.techopedia.com/definition/27327/network-service-provider-nsp [Accessed: 20 June 2015]

Teran, G., 1999. “ISPs Liability for Copyright Infringement.” [Online]. Available at: http://cyber.law.harvard.edu/property99/liability/main.html [Accessed: 19 June 2014]

Thailand, Office of the Court Judiciary, 2003. *Explanation of Computer-Related Offence Act B.E.2550(2007)*. Bangkok: Dokbier Publishing. [Thai]

Thailand, National Statistical Office (NSO), n.d. “The Household Survey on Information and Communication Technology.” [Online] Available at: http://web.nso.go.th/en/survey/data_survey/560619_2012_Information-.pdf [Thai] [Accessed: 3 June 2014]

Thailand, Electronic Transactions Development Agency (Public Organization)(ETDA) Available at: http://www.etda.or.th/etda_website/mains/display/1848 [Thai] [Access: 20 September 2014].

Tham, I. 2015. “Music and movie firms back website-blocking.” [Online] Available at: http://news.asiaone.com/news/singapore/music-and-movie-firms-back-website-blocking [Accessed: 5 June 2015]

The 1709 Blog, 2013. “Three Strike Struck Out.” [Online] Available at: http://the1709blog.blogspot.fr/2013/07/third-strike-struck-out.html [Accessed: 8 May 2015]

Thomas, N. 2015. “ISP Traffic Management: BT vs Virgin vs Sky vs TalkTalk vs EE.” [Online] Available at: https://recombu.com/digital/article/isp-traffic-management-bt-sky-virgin-media-ee-talktalk_M11045.html# [Accessed: 5 May 2016]

Torremans, P., ed., 2014. *Research Handbook on Cross-border Enforcement of Intellectual Property*, Cheltenham: Edward Elgar.

Trillet, G.V.R., 2012. *Liability and Evidence in case of Infringement of copyright of the internet: A Legal Comparison between Belgium and France.* LL.M. thesis, Tilburg University, Available at: http://arno.uvt.nl/show.cgi?fid=127512 [Accessed: 22 October 2015]

UK, The Crown Prosecution Service, n.d. "Minor Offences" [Online] Available at: http://www.cps.gov.uk/legal/l_to_o/minor_offences/ [Accessed: 10 October 2015]

UK, Intellectual Property Office, 2015. *International Comparison of Approaches to Online Copyright Infringement: Final Report,* Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/404429/International_Comparison_of_Approaches_to_Online_Copyright_Infringement.pdf [Accessed: 30 June 2016].

UK, Office of Communications (Ofcom), n.d. "A Guide to Internet Traffic Management." [Online] Available at: http://consumers.ofcom.org.uk/files/2013/09/traffic.pdf [Accessed: 1 July 2014]

Urban, J. M. and Quilter, L., 2006, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act." *Santa Clara Computer and High Technology Law Journal*, 22, 621, Available via SSRN: http://ssrn.com/abstract=2210935.

U.S., Copyright Office, 1998. *Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary*, Available at: http://www.copyright.gov/legislation/dmca.pdf [Accessed: 7 October 2014].

Vassenaix-Paxton, A.S., 2012. "The French Law Hadopi # 1 & 2" In: ALAI Meeting, slide 14. Available at: http://www.barrysookman.com/2012/10/10/the-french-hadopi-law-its-history-operation-and-effectiveness/ [Accessed: 26 December 2015]

Virgin Media, n.d. "Why are some websites not available through Virgin Media?" [Online] Available at: http://help.virginmedia.com/system/selfservice.controller?CMD=VIEW_ARTICLE&ARTICLE_ID=2374&CURRENT_CMD=SEARCH&CONFIGURATION=1001&PARTITION_ID=1&USERTYPE=1&LANGUAGE=en&COUNTY=us&VM_CUSTOMER_TYPE=Cable&buspart=web_block_CR [Accessed: 24 June 2014]

Walden, I., 2007. *Computer Crimes and Digital Investigations*, Oxford: Oxford University Press.

Watts Up With That?, 2011. *The Climategate email network infrastructure* [Online] Available at: http://wattsupwiththat.com/2011/11/30/the-climategate-email-network-infrastructure/ [Accessed: 18 June 2014]

Werbach, K., 2005. "Breaking the Ice: Rethinking Telecommunications Law for the Digital Age." *Journal on Telecommunication and High Technology Law,* 4, 59.

WhatIsMyIPAddress.com website, n.d. "Hide IP." [Online] Available at: http://whatismyipaddress.com/hide-ip [Access: 10 May 2014])

WhatIsMyIPAddress.com website, n.d. "How do I find email headers?" [Online] Available at: http://whatismyipaddress.com/find-headers [Accessed: 10 September 2014])

WIPO, n.d., "Summary of the WIPO Copyright Treaty (WCT) (1996)." [online]. Available: http://www.wipo.int/treaties/en/ip/wct/summary_wct.html [Accessed: 18 December 2013.]

Wisegeek, n.d. "What is Traffic Shaping?" [Online] Available at: http://www.wisegeek.com/what-is-traffic-shaping.htm [Accessed: 4 July 2014]

Wisegeek, n.d. "What Is a Bandwidth Cap?" [Online] Available at: http://www.wisegeek.com/what-is-a-bandwidth-cap.htm [Accessed: 4 July 2014]

Xu, C., 2014. "Redefinition of Current Legal Measures' Role as *Panaceas* in Digital Rights management Play." *US-China Law Review*, 11(2), 135.

Yu, P.K., 2010. "The Graduated Response." *Florida Law Review*, 62, 1370.

Yu, P. K., 2013. "Digital Copyright Enforcement Measures and Their Human Rights Threats." In: Geiger, C., ed. *Research Handbook on Human Rights and Intellectual Property.* Edward Elgar Publishing, 2015. Available via SSRN: http://ssrn.com/abstract=2363945

YouTube, n.d. "Keep your YouTube Account in Good Standing" [Online] Available at: https://support.google.com/youtube/answer/2797387?hl=en&ref_topic=2778545 [Accessed: 8 July 2014]

Yurkiw, J., 2013. "Subpoenas seeking identifying information and login data associated with email addresses did not violate First Amendment or privacy rights." [online]. Available at: http://www.technologylawsource.com/2013/08/articles/information-technology/subpoenas-seeking-identifying-information-and-login-data-associated-with-email-addresses-did-not-violate-first-amendment-or-privacy-rights/ [Accessed: 19 May 2016]

Zweigert, K. and Kotz, H., 1987. *An Introduction to Comparative Law*, 2nd ed. Oxford: Oxford University Press.

Legislation

Act for the Establishment of and Procedure for Intellectual Property and International Trade Court B.E.2539 (1996)

Digital Millennium Copyright Act 1998

Thailand Civil and Commercial Code B.E.2468 (1925)

Thailand Civil Procedure Code B.E.2477 (1934)

Thailand Criminal Procedure Code B.E.2477 (1934)

Thailand Computer-Related Offence Act B.E. 2550 (2007)

Thailand Copyright Act B.E.2537 (1994)

Thailand Copyright Act (No.2) B.E.2558 (2015)

Thailand Penal Code B.E.2499 (1956)

French Intellectual Property Code

The High Authority for the Dissemination of Works and the Protection of Rights on the Internet 2009 (French Intellectual Property Code 2009)

Singapore Copyright (Amendment) Act 2014

Cases

A & M Records v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001)

Cembrit Blunn Ltd. v. Apex Roofting [2007] EWHC 111 (Ch)

Chevron Corp v. Donziger, No. 12-mc-80237 (N.D. Cal. Aug. 22, 2013)

Cindy Lee Garcia v. Google, Inc., Slip. Op. No. 12–57302, (9th Cir. 2014)

Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020 (9th Cir. 2013)

Commonwealth v. Rudinski, 382 Pa. Super. 462 (1989)

EMI Records & Ors v. Eircom Ltd, [2010] IEHC 108.

Constitutional Court Case no.5/B.E.2556 (2013) Available at: http://www.constitutionalcourt.or.th/index.php?option=com_docman&task=cat_view&gid=542&Itemid=94&lang=th&limitstart=10 [Thai] [Accessed: 20 September 2015]

Constitutional Council Decision no. 2009-580 of June 10th 2009

Corbis Corp. v. Amazon.com, Inc., 351 F.Supp. 2d 1090 (W.D. Wash.2004)

Craigslist, Inc. v. 3Taps, Inc., 942 F.Supp.2d 962, 969 (N.D. Cal. 2013)

Ellison v. Robertson, 189 F.Supp.2d 1051 (C.D. Cal. 2002), 1065.

In re: Charter Communication, Inc., 393 F.3d 771 (8th Cir. 2005)

Interscope Records v. Does, 494 F.Supp.2d 388 (E.D. Va. 2007)

Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150 (N.D. Cal. 2008)

Metro–Goldwyn–Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913

Ouellette v. Viacom International, Inc., 2012 WL 850921

Perfect 10, Inc. v. Giganews, Inc., 993 F.Supp.2d 1192.

Perfect 10, Inc. v. Ccbill Llc, 488 F. 3d 1102 (9th Cir. 2007)

Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D.Fla. 1993)

Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C.Cir.2003)

Religious Technology Center v. Netcom Online Communication Services, Inc., 907 F.Supp. 1361 (N.D. Cal. 1995).

Salabiaku v. France, Publ. ECHR, Judgment of 7 October 1988, [Online] Available at: https://www.coe.int/t/dghl/cooperation/economiccrime/corruption/projects/car_serbia/ECtHR%20Judgements/English/SALABIAKU%20v%20FRANCE%20-%20ECHR%20Judgment%20_English_.pdf [Accessed: 10 October 2015]

Sega Enterprises Ltd. v. MAPHIA, 857 F. Supp. 679 (N.D. Cal. 1994)

Supreme Court case no.954/B.E.2476

Supreme Court case no.466/B.E.2478

Supreme Court case no. 2149/B.E.2516

Supreme Court case no. 970/B.E.2519

Supreme Court case no. 2574/B.E.2519

Supreme Court case no.1479/B.E.2520

Supreme Court case no.6/B.E.2534

Supreme Court case no.1343/B.E.2538

Supreme Court case no.1714/B.E.2539

Supreme Court case no.5294/B.E.2540

Supreme Court case no.753/B.E.2541

Supreme Court case no.4746/B.E.2541

Supreme Court case no.3040/B.E.2541

Supreme Court case no.6558/B.E.2541

Supreme Court case no.10/B.E.2542

Supreme Court case no.5337/B.E.2542

Supreme Court case no. 4250/B.E.2542

Supreme Court case no.9028/B.E.2542

Supreme Court case no.994/B.E.2543

Supreme Court case no.873/B.E.2544

Supreme Court case no.7221/B.E.2544

Supreme Court case no.704/B.E.2545

Supreme Court case no.5273/B.E.2546

Supreme Court case no.7024/B.E.2546

Supreme Court case no.290/B.E.2548

Supreme Court case no.2572/B.E.2548

Supreme Court case no.3054/B.E.2548

Supreme Court case no.3741/B.E.2549

Supreme Court case no.3054/B.E.2548

Supreme Court case no.6804/B.E.2548

Supreme Court case no.7873/B.E.2549

Supreme Court case no.5036/B.E.2550

Supreme Court case no.1366/B.E.2553

Supreme Court case no.1829/B.E.2553

Supreme Court case no.3882/B.E.2553

Supreme Court case no.6802/B.E.2553

Supreme Court case no.8366/B.E.2553

Supreme Court case no.2492/B.E.2558

The Council of State case No. 342405 Available at: https://translate.google.co.uk/translate?hl=en&sl=fr&u=http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-octobre-2011-French-Data-Network-n-342405&prev=search [Translated by Google Translation][Accessed: 5 October 2015]

UMG Recording, Inc. v. Shelter Capital Partners LLC, 718 F. 3d 1006 (9th Cir. 2013)

Viacom Int'l Inc. v. YouTube, Inc., 679 F.3d 19 (2d Cir. 2012)

Well Go USA, Inc. v. Unkown participants in filesharing swarm identified by Hash, WL 4387420 (S.D.Tex. 2012).

International Legal Instruments

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs)

Berne Convention for the Protection of Literary and Artistic Works

Directive 2000/31/EC of the European Parliament and of the Council on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (E-Commerce Directive)

WIPO Copyright Treaty 1996 (WCT)

WIPO Performances and Phonograms Treaty 1996 (WPPT)

Other Materials

European Commission, 2014. *Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee: Trade, growth and intellectual property - Strategy for the protection and enforcement of intellectual property rights in third countries.* Available at: http://trade.ec.europa.eu/doclib/docs/2014/july/tradoc_152643.pdf [Accessed: 7 July 2016].

European Commission, 2015. *Report on the protection and enforcement of intellectual property rights in third countries.* Available at: https://euipo.europa.eu/ohimportal/documents/11370/0/Report+on+the+protection+and+enforcement+of+intellectual+property+rights+in+third+countries [Accessed: 7 July 2016].

France, Hadopi, 2011. *Annual Report 2011*, Available at: http://hadopi.fr/sites/default/files/page/pdf/Hadopi_Rapportannuel_ENG.pdf [Accessed: 30 April 2015]

France, Hadopi, 2013. *Report on the prevention of unlawful streaming and direct downloading*, Available at: https://hadopi.fr/sites/default/files/page/pdf/Rapportstreaming_eng.pdf [Accessed: 7 October 2016].

Letter from Permanent Secretary of Ministry of Information and Communication Technology to the Superintendent 3 of Technology Crime Suppression Division, No. Tor Kor 0212.2/6312, Dated: 7 June 2016 [Thai]

Memorandum of Understanding between ISPs (SBC Internet Services, Inc. et. al) and Content Owners (RIAA et al.) (July 6, 2011), Available at: http://www.copyrightinformation.org/sites/default/files/Momorandum of Understanding.pdf).

Record of live chatting with Verizon's agent through "Chat Now" on Verizon website at: http://www.verizon.com/smallbusiness/fiosInternetOverview.jsp?smbReferenceValue=SMBFIOSInternetPackageRef [conducted on 24 Oct 2014 at 14:45-14:51 (UK time)]

Thai Cabinet Resolution on the 28th February B.E.2482 (1939).

Thailand, Office of the Council of State, Opinion No.343/B.E.2549 (2006)[Thai] Available: http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=cmd&year=2549&lawPath=c2_0343_2549 [Accessed: 23 December 2012.]

Thailand, Electronic Transactions Development Agency (Public Organization) (ETDA), 2015. "ICT Law Center Forum: Open Forum for Public No. 3: How the Draft Copyright Act that has just passed by National Legislative Assembly Benefits Digital Economy", (Seminar) [Thai] Available at: https://www.youtube.com/watch?v=Od3O9kVHSYc [Accessed: 23 June 2015].

Thailand, ETDA, 2016, *Thailand Internet User Profile 2016*, [Online] Available at: https://www.etda.or.th/publishing-detail/thailand-internet-user-profile-2016-th.html [Thai] [Access: 14 October 2016].

Thailand, The Prime Minister office, 2013, "the Note" accompanied the Draft Copyright Act (No. …), Document enclosed with a Letter to the President of the House of Representative No. Nor Ror 0503/24266 dated the 10th of September 2556(B.E.)(2013) [Thai] Available:https://edoc.parliament.go.th/Meeting/MeetingViewer.aspx?id=143 [Accessed: 30 January 14.]

Thailand, High-Tech Crime Unit, Royal Thai Police, n.d. "Guidance on Criminal Investigation of Technological Case" [Online]. Available at: http://www.hightechcrime.org/inv [Thai] [Accessed: 5 December 2015]

Thailand, Office of Attorney General, n.d. *Criminal Proceeding Handbook for Computer-Related Crime*. [Thai].

Tingsmith, W., 1999. *Ending Remark of Supreme Court case no. 4250/B.E.2542 (1999)*

UK, Intellectual Property Office, 2015. *International Comparison of Approaches to Online Copyright Infringement: Final Report,* [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/404429/International_Comparison_of_Approaches_to_Online_Copyright_Infringement.pdf [Accessed: 25 October 2015]

U.S., House of Representatives, the Committee on the Judiciary, Subcommittee on Courts, Intellectual Property and the Internet, 2014. *Hearing 113th second session*, [Online] p.4-5. Available at: http://judiciary.house.gov/_cache/files/22c3acda-551c-41ba-b330-8dd251dd15fd/113-86-87151.pdf [Accessed: 10 November 2014]

U.S., Commercial Service, n.d., "IPR Toolkits for the Kingdom of Thailand" [Online] Available at: http://origin.www.stopfakes.gov/sites/default/files/thailand_toolkit.pdf [Accessed: 8 March 2014].

U.S., The US. Congress, 2002. Congressional Record Vol. 148-Part 11: Proceedings and Debates of the 107th, Second Session, 2002 Available at: https://www.congress.gov/crec/2002/07/25/CREC-2002-07-25-bk2.pdf [Accessed: 2 June 2015].

U.S. House of Representatives, 1998. *Report to the House of Representatives on Digital Millennium Copyright Act of 1998 for the 105th Congress, 2nd Session (105-551)*, Available at: http://digital-law-online.info/misc/HRep105-551pt2.pdf [Accessed: 4 October 2014]

U.S., Senate, Committee on Judiciary, 1998. *Report to the Senate on Digital Millennium Copyright Act of 1998 for the 105th Congress, 2nd Session (105-109)*, Available at: http://digital-law-online.info/misc/SRep105-190.pdf [Accessed: 19 February 2015]

U.S., Office of United States Trade Representative(USTR), 2014. *2014 Special 301 Report*, Available at: https://ustr.gov/sites/default/files/USTR%202014%20Special%20301%20Report%20to%20Congress%20FINAL.pdf [Accessed: 14 October 2016]