Implicate the middleman?

The Strength and weakness of the “Good Samaritan Doctrine” in providing a legal shield for Internet Service Providers (ISPs) against the liability of third party contents.

By

Habib Sani Usman.  Anr: 986370

Supervisor: Professor Lokke Moerel

Second reader: Dr Colette Cuijpers

Program: Law and Technology (LL.M)

June 2014.
Abstract

“...laws and institutions must go hand in hand with the progress of the human mind...”

Thomas Jefferson 1816

The emergence of the Internet has ushered in a new form of information dissemination giving everyone the opportunity to publish almost everything and in whichever format without the least restriction. As a result, whenever offensive content is detected on the Internet, the first reaction is to "blame" the provider of the platform –the Internet service provider (ISPs). Blaming the ISP is re-enforced by the fact that ISPs have technical control over the content; ISPs are in a better financial position and can always be identified with ease, compared to original publishers of offensive contents who can be anonymous on the Internet. By implication ISPs have found themselves crammed between the hammer of the law and the anvil of aggrieved users.

Accordingly, this calls for regulation on the use of the Internet and in this regard the spotlight falls on the government and ISPs. In other words a hybrid of ‘self-regulation and government intervention’ is desired to control abusive use of the Internet. However, over regulating the use of the Internet will definitely choke the growth of e-commerce in particular and information society services in general. Hence the laws left some space for ISPs to wriggle free of liability as long as they perform the role expected of them.
# TABLE OF CONTENTS

**Chapter 1: Introduction.**

1.1 Background of the study ................................................................. 5

1.2 Aims and objectives of the Research ............................................... 9

1.3 Research question ........................................................................... 10

1.4 Research methodology .................................................................. 10

1.5 Overview of thesis chapters ............................................................ 11

**Chapter 2: Theoretical framework and general overview of the nature of ISPs.**

2.1 Introduction ...................................................................................... 13

2.2 Definition of ISP and basic terminologies in ISP liability .................. 13

2.3 Functions of ISPs ............................................................................ 15

2.4 The status of ISPs ........................................................................... 17

2.5 Technical means of restricting third party contents on the Internet .... 18

**Chapter 3: Nature and extent of ISP liability under the EU legal regime**

3.1 Introduction ...................................................................................... 21

3.2 Regulating ISP liability under the e-commerce Directive 2000/31/EC .... 23

3.2.1 Mere conduit .............................................................................. 23

3.2.2 Caching ..................................................................................... 24

3.2.3 Hosting ..................................................................................... 25

3.3 Notice and take down procedure ...................................................... 27

3.4 Legal duty of care and moral obligation on ISPs under the EU ISP liability regime ........ 30

3.4.1 Burden of proof and defences available to ISPs under the EU ISP liability regime ........ 31

3.5 Merits and drawbacks of the e-Commerce Directive on ISP liability ........................................... 39
Chapter 4: Guideline on ISP liability regime in the United States.

4.1 Introduction .................................................................................................................44
4.2 The Digital Millennium Copyright Act 1998 ..............................................................45
4.2.1 Notice and take down Procedure ........................................................................49
4.3 The scope, limitation and interpretation of the Communication Decency Act 1996.....51
4.3.1 Good Samaritan Doctrine of screening and blocking ........................................54
4.4 Burden of proof and defences available to ISPs under the U.S ISP liability regime ....58
4.5 Merits and drawbacks of the US ISP liability regime ...............................................60

Chapter 5: Case analysis; Jones v. Dirty World Entertainment Recordings, LLC, 2013

5.1 Introduction ..................................................................................................................63
5.2 Jones v. Dirty World Entertainment Recordings, LLC ..................................................64
5.3 The impact of the Good Samaritan Doctrine on the freedom of expression ...............69
5.4. ISP neutrality and anonymity under the First Amendment ......................................70
5.5 Limitations to anonymous speech under the First Amendment ...............................77

Chapter 6: Conclusion.

6.1 Summary ....................................................................................................................79
6.2 What is the effect of screening and blocking third party contents on the Internet .........81
6.3 What is the basis for holding ISPs liable for third party contents ..............................81
6.4 Recommendations ....................................................................................................82

Bibliography. 85
Chapter one: Introduction.

1.1 Background of the study.

In November, 2013, the ruling in the case of JONES v. DIRTY WORLD ENTERTAINMENT RECORDINGS, LLC\(^1\) by the Kentucky District Court, gave rise to a further interpretation of section 230 of the United States’ (U.S) Communication Decency Act (CDA) 1996- a law promoting free speech, but which regulates pornographic and defamatory contents on the Internet. The CDA also provides immunity to ISPs against civil liability for the act of ‘blocking and screening any deemed offensive material’ that has been posted by third parties on the Internet. This shield against civil liability for blocking and screening contents on the Internet is known as the “Good Samaritan Doctrine.” The Good Samaritan Doctrine is not an absolute immunity for ISPs against liability for third party contents on the Internet, but a qualified immunity which can be lost once it is established that an ISP is contributory negligent or has aided or abetted third party content development. The roots of the Good Samaritan Doctrine can be traced back to a principle of the law of tort\(^2\) which absolves a party from being negligently liable, provided there is no recklessness in an effort to save another individual who seems to be in imminent and serious danger. Thus the Good Samaritan Doctrine becomes a legal shield where;

\[
\text{“[a]n ISPs takes any action voluntarily in good faith to restrict access to (or restricts availability of) material that is considered to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, even if such material is constitutionally protected.”}\]

\(^1\) An appeal from the United States District Court for the Eastern District of Kentucky No. 2:09-CV-219-WOB
\(^2\) A tort is a civil wrong or an injury which gives rise to a civil suit often rewarded in damages or legal injunctions. Black law dictionary- free online dictionary available at http://thelawdictionary.org/tort/.
\(^3\) Section 230 Communication Decency Act 1996.
Invariably, ISPs may not be liable ‘for any offensive contents which have been provided by third parties’\textsuperscript{4} when they rely on the Good Samaritan Doctrine of screening and blocking.

ISPs are, however liable for third party content if they became aware of its offensive nature, but failed to take expeditious action in removing the contents.\textsuperscript{5} This thesis is in response to the court ruling in \textit{JONES v. DIRTY WORLD ENTERTAINMENT RECORDINGS, LLC, Dist. Court, ED Kentucky 2013}. The ruling of the court sets a “precedent which supports the proposition that; the CDA provides only a sort of qualified immunity that can be lost, if an ISP intentionally develops, and/or materially contributes to the illegal or objectionable material on the Internet.”\textsuperscript{6} Purposely, this ruling re-evaluates the intends of the U.S congress in enacting section 230 of the CDA which provides for the Good Samaritan Doctrine. Essentially, the ruling in the \textit{JONES} case seeks to balance the freedom of expression of anonymous posters on the Internet which is protected by the First Amendment to the United States Constitution against, both the protection of reputation and the right to privacy of aggrieved victims on the Internet.\textsuperscript{7}

Connected with this, is the fact that in the U.S ISP liability is broadly regulated by two legislations. Namely; the CDA, which regulates ISP liability for the circulation of pornography and defamation online by way of screening and blocking, and the Digital Millennium Copyright Act of 1998 (DMCA) which deals with the liability of ISPs -for copy rights infringements on the Internet through a notice and take down procedure. Both screening and blocking of the CDA and notice and take down procedure of the DMCA are self- regulations aimed at controlling abusive use of the Internet. However under the CDA ISPs on their own accord and in good faith, can

\textsuperscript{4} Ibid.
\textsuperscript{5} (Susy Frankel and Geoff McLay \textit{Intellectual Property in New Zealand} (LexisNexis Butterworths, Wellington, 2002) 734.)
\textsuperscript{6} \textit{JONES v. DIRTY WORLD ENTERTAINMENT RECORDINGS, LLC, Dist. Court, ED Kentucky 2013}, 840 F.Supp.2d 1008-2
screen and block contents that are glaringly offensive. But under the DMCA offensive contents are taken down based on a valid notice issued by aggrieved party. Speaking of a notice and take down procedure brings to mind other jurisdictions where the same procedure is applied— the European Union (EU). However, the legal framework on ISP liability in the European Union (EU) is slightly different from what is available in the United States.

In the EU the liabilities of ISPs are generally regulated by the e-Commerce Directive 2000/31/EC. Offensive third party contents on the Internet are equally avoided through a notice and take down procedure. Unlike the United States where Internet rules are specified based on the type of civil liability, the e-Commerce Directive is a horizontal directive that fused all civil liability that an ISP can incur such as; copyright infringement, trademark violation, and defamation. Similarly, the e-Commerce Directive provides for a special ISP liability regime which; as a general rule does not oblige ISPs to monitor third party contents, where they simply perform a passive role of; mere conduit, caching, and hosting. In other words, ISPs are exempted from liability of third party contents, this is because as Bayer puts it, “ISPs generally do not know the content of the cache, nor do they know the content of the hosted material.”

However, there are situations where ISPs possess knowledge of what is contained in caches. For example when dealing with huge amount of requests especially in peak periods, ISPs make extra effort and intentionally creates cache copies of selected content so as to facilitate easy access to the main content. Within the context of the e-Commerce Directives, intentional caching attracts liability if the cached contents turn out to be offensive. In this regard the requirements of the e-

---

8 Articles 15 e-commerce Directive 2000/31/EC
9 The role and status of ISPs are discussed further in the second chapter of this thesis.
The Good Samaritan Doctrine are partly similar to those of the DMCA, meaning that ISPs under circumstances are obliged to take the content down immediately.

Supposedly, ISPs should not be held accountable for disseminating offensive contents posted by third parties, except where they tacitly encourage misuse of the Internet which results into harming innocent citizens.

Based on the discussions generated by the recent ruling in *Jones v. Dirty World Entertainment Recordings, LLC, Dist. Court, ED Kentucky 2013* and the brief outline of the ISP liability regime in the EU and US the question that can be posed is; given the conflicting interest of freedom of expression and the protection of the reputation of aggrieved parties on the Internet, what is the effect of screening and blocking third party contents on the Internet, and on what basis should ISPs be held liable for third party contents?

In an attempt to answer this question, the thesis will commence with a general overview of the status and functions of ISP from a technical perspective. Focusing on definition, function and status of ISPs. This will give a clue on why ISPs on the various technical means of restricting contents on the Internet employed by ISPs. Thirdly, an examination of the scope and limitation of ISP liability regime in the EU and the U.S will be conducted. In particular the provisions of the e-Commerce Directive, the CDA and the DMCA will be reflected upon. Not only the legislation, but also recent cases that involved liability of major ISPs in the EU and the U.S for third party content will be analysed.

The analysis will help in revealing the effects of the Good Samaritan Doctrine on the freedom of expression and the right to privacy. In this regard suggestion will be made in having a balanced
system that will provide a safe harbour for ISPs to operate freely on the one hand, and a system which protects those who might be harmed by third party contents on the other hand.

Finally, after evaluating the strengths and weakness of the Good Samaritan Doctrine, recommendations will be made on the need of harmonising the EU ISP liability regime with that of the U.S., providing an international standard dealing with ISP liability for third party contents.

Since the Internet is not restricted in a particular region, offensive contents are equally accessed globally.

1.2 **Aims and objectives of the research.**

The aim of this research is to prove the strength and weakness of the Good Samaritan Doctrine as a legal shield for ISPs against the liability of disseminating third party contents on the Internet, and to offer recommendation on the need of improvising an international legal framework that will regulate ISP liability against third party contents based on the existing EU and US ISP liability regime.

The objective of this research is to investigate what would be the right balance that will allow ISPs to operate with satisfactory certainty, at the same time adhering to the principles of freedom of expression on the one hand, and to protect those who might be harmed by third party contents on the other hand. For this is currently not given, considering that major ISPs like *CompuServe*, *Yahoo* and *America On-Line*\(^{11}\), were defendants in a series of civil and/or criminal proceedings:

---

b. Zeran v America Online, Inc (1997) 958 F Supp 1124 (ED Va)  
d.[Blumenthal v Drudge and AOL, Inc. (1998) 992 F Supp 44;  
  e.Stratton Oakmont Inc. v Prodigy Services Co (1995) 23 Media L Rep 1794 (NY)
in relation to questionable content they hosted or provided access to, such as child pornography, defamatory or racist materials.

1.3 **Research questions.**

What is currently the effect of the Good Samaritan Doctrine as a legal shield for screening and blocking third party contents on the Internet, and on what basis should ISPs be held liable for third party contents?

1.3.1 **Sub-questions:**

a. What is the legal status of ISPs, and do ISPs have a duty of care on the Internet?

b. What are the scope and limitations of the EU ISP liability regime?

c. What is the scope and limitation of the US ISP liability regime particularly the CDA which provided for the Good Samaritan Doctrine?

d. Based on case law that interprets the Good Samaritan Doctrine, how will ISPs strike the right balance between respecting the right to privacy of individuals and observing freedom of expression on the Internet?

e. How would an international standard that regulates ISP liability for third party contents best look like?

1.4 **Research Methodology.**

In order to expose the strength and weaknesses of the Good Samaritan Doctrine, this research will employ a doctrinal/traditional legal research method by analyzing recent court cases that interpret the provisions of the United States’ CDA 1996. The analysis will also slightly involve a comparison between the provisions of the CDA 1996, and other regulatory frameworks which exempt ISPs against liability for third party contents within the U.S and from the EU, such as the DMCA 1998 and the e-Commerce Directives 2000/31/EC. This is because in many respect
these legislations provides similar requirements in exempting ISPs against the liability for disseminating third party contents on the Internet.

1.5 **Overview of thesis chapters**

The Thesis consists of six Chapters. The first chapter basically serves as the introduction consisting of the background of the study, research questions, the methodology of conducting the research and the overview of the Thesis Chapters.

The second chapter will provide a theoretical framework, and a general overview of the nature of ISPs highlighting; the definition of an ISP, some basic terminologies used in ISP liability, function and the status of ISPs. This chapter will also discuss the technical means of restricting contents on the Internet. Some of the issues touched in this chapter are linked to topics investigated in other chapters such as; the status of ISPs will provide the causal link for the technical means of restricting contents on the Internet, and the basis for holding ISPs liable for defamatory contents and copy right infringement.

Chapter three will explore the EU ISP liability regime, with the aim of evaluating the exemption granted to ISPs by the e-Commerce directive 2000/31/EC from the liability of acting as mere conduit, caching or hosting, of third party contents. Subsequently; the legal duty of care, the burden of proof required by the courts in finding ISPs liable for third party contents, and the defences available to ISPs for disseminating offensive content posted by third parties will be examined. This will be followed by an evaluation of the notice and takedown procedure. The last part of this chapter will draw a conclusion on the merits and drawbacks of the EU regulations on ISP liability.
Chapter four will discuss the U.S ISP liability regime, mainly consisting of the DMCA and the CDA. More focus will be on the scope and limitation of the CDA 1996 as a regulatory framework dealing with ISP liability. Particular attention will be given to the merits and demerits of the Good Samaritan Doctrine, as a legal shield against liability for hosting, processing and making available third party defamatory contents in the United States. Furthermore, court cases will be analyzed in order to acknowledge the various interpretations of the Good Samaritan Doctrine in combating and/or controlling abuse on the Internet, especially defamation. In order to avoid confusion and overloading this chapter, an analysis of the most recent case involving the Good Samaritan Doctrine is reserved for the next chapter. Before that the last part of this chapter will expose the merits and drawbacks of the US ISP regime.

Chapter five will be an analysis of the most recent case that interprets the Good Samaritan Doctrine- JONES v. DIRTY WORLD ENTERTAINMENTRECORDINGS, LLC, Dist. Court, ED Kentucky 2013. The case analysis will bring forth arguments such as whether an application of the Good Samaritan Doctrine by ISPs will have a chilling effect on the freedom of expression as guaranteed by the First amendment to the U.S constitution. In other words, ISP neutrality and freedom of expression of anonymous posters under the First Amendment will be assessed. This chapter will conclude with a brief analysis of some of the limitations on the freedom of expression under the First Amendment.

Chapter six will summarise the thesis and provide answers to the central research question namely, what is the effect of screening and blocking third party contents on the Internet, and on what basis should ISPs be held liable for third party contents? This will be followed by recommendations on how to standardize the ISP liability regime.
Chapter two: Theoretical Framework and the nature of ISPs.

2.1 Introduction.

This chapter will provide a general overview of the role and status of ISPs from a technical perspective. Thereafter some basic terminologies in ISP liability will be explained. This will be followed by the technical means of restricting contents on Internet. Historically the first widely known ISPs such as America Online (AOL) and CompuServe were not actually full ISPs in the strict sense of the term, but they were simply content providers because of their ‘members-only’ offering of services and rather narrow Internet access. According to Bayer, content providers usually work with smaller amount of data than the actual ISPs of this age such as EarthLink, MindSpring, Yahoo, Google, etc. These ISPs offer higher-speed Internet access and greater long term stability in a broad geographical area than content providers.

Thus, in order to appreciate the role and status of ISPs “as the provider of the facility (technology) that enables users of the Internet to post content on websites” a proper definition of an ISP will be a good point to start.

2.2 Definition of ISP and basic terminologies in ISP liability

Technically Microsoft defines an ISP as “a company that provides access to the Internet by way of a phone line (dial-up) or a broadband connection (cable or DSL), and offers allied services such as e-mail accounts and management of web portals usually for a fee.”

From a legal perspective ISP is “[a]n entity providing the transmission, routing, or providing connections for digital on-line communications, between or among points specified by a user of

12. This is because detailed legal analysis has been dedicated for subsequent chapters, but where necessarily reference will be made on a particular law and/or jurisdiction.
14 http://windows.microsoft.com/en-us/windows/what-is-internet-service-provider#1TC=windows-7
material of the user’s choosing, without modification to the content of the material as sent or received.”\textsuperscript{15}

Based on the Organization for Economic Co-operation and Development (OECD) classification of Internet intermediaries, some examples of ISPs include; Verizon, Comcast, NTT, Internet Initiative Japan, BT, Free Fr, Vodafone, Orange, T-Mobile and MTN. In addition to these examples of ISP the OECD on Internet intermediaries explained the following technical terminologies as follows;

1. Web portal- an electronic page designed to consolidate array of information under a given heading.
2. Proxy server- a conduit which coordinates command and request between users of the Internet.
3. Exemplar- a model or pattern which can be copied or imitated from a proxy server.
4. Internet protocol (IP) address- a numerical label assigned to any device that connects to the Internet for communication purposes.
5. Domain name server (DNS) - the translation of binary numbers assigned to the IP address/number of a device that connects to the Internet.
6. Search engine- a program designed to enable for the quick retrieval of selected topics in an indexed manner.
7. Encryption- a special way of encoding contents so that only persons with access code such as keys or passwords can access the contents.
8. Wi-Fi: a service which allows a device to connect to the internet within a given radius.
9. Hyperlink- a special link embedded in webpages that when clicked re-directs the visitor of the webpage to another site.

\textsuperscript{15} Digital Millennium Copyright Act 1998, section 512(k)(1)(A) (Supp. IV 1998).
From foregoing definitions and examples, inference can be made on the functions of ISPs which is very relevant in determining civil liability for third party contents on the Internet.

2.3 Functions of an ISP:

From a technical point of view, ISPs perform the following functions;

1. Provision of access to the Internet for users. Basically, this is a fundamental connection between a user and the *World Wide Web* which allows for the download and upload of any content. This function is similar to the traditional telephone service.

2. The second function of an ISP is hosting and processing of data services for content providers. For instance providing email facilities, web-hosting, or online storage services. Other services include the provision of a virtual server, or a physical server operation. Hosting services may also include cloud computing services, in a situation where ISPs store data of its customers on a flexible and scalable server for easy on demand access.

A typical hosting service takes place where ‘a database is used to store hosting and access descriptors’. The hosting and access descriptors describe the configuration of Internet services using protocols such as; Hypertext transfer protocol (HTTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3), Internet message access protocol 4 (IMAP4), and File Transfer Protocol (FTP), for a hosted site. Functionally, these protocols are required because when a client over the Internet or other network requests a service from the hosted domain. The domain is then is interfaced to the

---

18 A detailed discussion of these protocols and how they work is out of the scope of this thesis.
database via a protocol, so as to select a computer that can be used in supporting the requested access.\(^{19}\)

3. The third function of an ISP is caching services. Caching is the technical ability to automatically create a temporary copy of a hosted content, so that it can be accessed more easily and quickly the next time when it is needed. The cached copy enables the requesting machine to access the page from the closest possible exemplar (the cache), and to reload only those details that have changed.\(^{20}\) The benefit of such an action is to reduce the cost of transmission in peak periods with high requests, for instance in banks.

4. The fourth function of ISPs is the provision of searching services, and the maintenance of web portals. Almost all major ISPs have their own search engines, for example Yahoo! operates a search engine based on a broad topical directory which has been systematically indexed and catalogued by humans. Google has search engines such as Google scholar, which is a search engine for scientific information; and Google Books which is a search engine containing millions of books that have been scanned into electronic format.

5. Finally, ISPs may engage in peering services. Peering is where multiple ISPs interconnect at Internet exchange points (IXs) for the routing of data transmission. Without peering the data would have otherwise passed through a third upstream ISP, incurring charges from the upstream ISP.\(^{21}\)

An average ISP would provide at least three of the above mentioned services, and in addition serve as an e-commerce intermediary or an Internet payment system, as well as provide its own


\(^{20}\) In relation to liability, ISPs do not know the content of the cache, except when they deliberately select content for permanent storage.

content in situations where it advertises its own product and maintains its own website. For instance, Google does this by providing services such as chrome, Google maps, Gmail etc. Legally speaking, providing access to the Internet and hosting contents are mainly done on a contractual basis, whereas caching and searching services do not necessarily involve a contract. Rather caching and searching service are simple technicalities employed by ISPs to ensure the optimization of access to requested websites. These functions give a clue about the role of ISPs.

2.6 The status of ISPs

The status of ISPs is a usually controversial. Intellectual property rights owners and those who contest free access to offensive materials on the Internet maintain that ISPs are publishers. Adding that ISPs should be saddled with the task of policing the cyberspace against obscene and defamatory material, and where ISPs fail in carrying out this task they become liable for the offensive contents.22 Conversely, ISPs in an attempt to justify self-protection against liability for offensive contents posted by third parties on the Internet simply identify themselves as the necessary link between users and the Internet, akin to the traditional telephone operator. Therefore, by revisiting the functions of ISPs that were previously stated, ISPs are generally intermediaries who are in a special situation. This position allows ISPs to technically control contents on the Internet and take those contents down where there is allegations offensiveness, as opposed to the telephone operator who has no control of the contents in the transmission cables.

2.5 Technical means of restricting third party contents on the Internet

Lawrence Lessig\(^{23}\) identified the four modalities of regulation as law, morality, market and architecture (codes). According to Lessig codes means any technological process that can be used to regulate behaviour, and this he called it ‘techno-regulation’. With regards to the Internet, techno- regulation means any technical means that can be employed in restricting access to or the availability of contents on the Internet. This is generally described as censorship and the most common measures adopted include but not limited to;

1. **Filtering.** This is the most common means adopted by ISPs in restricting contents on the Internet. Screening is another name given to this technique. It has been successful in regulating offensive and unwanted content on the Internet mostly pornography and unsolicited messages aimed at direct marketing. In this regard Chinese filtering technology has proved to be the most sophisticated in the world.\(^{24}\) However filtering is, from an economic perspective very expensive and would in most cases affect the popularity of a website. For example Yahoo’s products and services lost popularity in France following the *France vs. Yahoo case*,\(^{25}\) when Yahoo was ordered to filter its sites for all materials connected with Nazi memorabilia.

2. **Removal of search links and cache copies.** Where an ISP learns or is being notified that a content is offensive, it technically sweeps all search links and cache that might be connected with the offensive contents. Primarily, this is done in order to restrict further access to or the availability of the offensive contents. Removal of search links and cache copies is currently carried out by Google\(^{26}\) as a means of restricting child pornography on the Internet.

3. **Blocking of blacklisted websites.** Web sites allegedly containing infringed copyright materials for instance are automatically blocked. This is the same as the so-called


\(^{26}\) Eric Schmidt, ‘‘we’ve listened- and this is how we’ll halt this depravity’’ Google executive chairman on child pornography: mail online 18 November 2013.
“Graduated Response” regime introduced by the French HADOPI Authority. Wherein an ISP acting upon information provided by the right holder, warns its customer that its Internet connection appears to have been used for copyright infringements and requesting it to cease the infringement. However graduated response regime can only be binding upon an ISP by virtue of a private agreement between an ISP and its customers.

4. **Notice and takedown (NTD):** The e-Commerce Directive and the DMCA, requires ISPs (in exercising the legal duty of care) to remove illegal and harmful content from the internet once they have received notice. This process is technically described as the NTD. After filtering, the NTD procedure is the most popular route for restricting offensive contents posted by third parties on the Internet. It works well in cases where the reputation of an individual is at stake, or where there are allegations of intellectual property rights infringement on the internet. Although the e-Commerce Directive did not provide for a detailed procedure, the technical steps for a NTD, under the DMCA involves ‘report, remove, respond and replace’.

   ii. Report: a protest in a form of written report is sent to the ISPs concerned, and this serves as a valid notice of the offensive nature of the content.

   iii. Remove: the ISP removes the alleged offensive content, without judging its merits.

   iv. Respond: the author of the alleged offensive content can contest its removal by way of a counter notice asking for replacement and,

   v. Replace: depending on the merits of the counter notice, the ISP acts routinely and replaces the contents or declines from doing so until a competent court order demanding replacement is issued.

---

28 *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* (HADOPI)
29 Ibid. This because HADOPI is an administrative body without legal enforcement powers.
30 Tamiz v Google [2013] EWCA Civ 68
31 Case C-70/10 Scarlet Extended SA v. Société belge des auteurs compositeurs et éditeurs (SABAM); also Tiffany (NJ) Inc. v. eBay Inc., -F.3d - 2010 WL 1236315 (2d Cir. Apr. 1, 2010).
32 This is from a technical point of view; full analysis of the procedure from a legal perspective is reserved for subsequent chapters.
5. **Terminating user subscription** “three strikes and you are out”. This happens mainly where Internet users are suspected of downloading illegal contents. In the first instance, they receive a warning from their ISPs via an email, followed by suspension of Internet service in the second instance, and finally termination of contract for Internet service as the third strike.\(^3\) The French HADOPI Authority adopts this method in carrying out the graduated response regime that has been stated above.

This concludes a brief theoretical framework on the nature, status and function of ISPs mainly from a technical perspective. The following chapter will extensively deal with ISP liability for third party contents under the EU jurisdiction.

\(^3\) The most frequently employed strategy includes; bandwidth reduction, protocol (IP) blocking, and account suspension or total disconnection from the Internet.
Chapter three: The nature and extent of ISP Liability under the EU Legal Regime

3.1 Introduction.

The European Union (EU) is an amalgamation of 28 states sharing common interest on political and economic matters. Legal affairs in the EU are jointly coordinated by the European parliament and the European council through ‘Regulations’ and ‘Directives.’ Regulations have direct effect on member states, but Directives must be transposed and implemented into the laws of member states (MS) in order to be effective. For the purpose of regulating ISP liability within the EU, the relevant legislation is “Directive 2000/31/EC on certain legal aspects of electronic commerce in the Internal Market, commonly referred to as the "E-Commerce Directive.”(E-CD).

The E-CD consists of 24 Articles and 65 recitals. The main enactments are contained in the Articles, while the recitals simply illuminate the meaning of the provisions in the Articles. These Articles and recitals broadly cover four sections- namely;

i. Establishment of Information Society service providers,

ii. Commercial communications (advertising, direct marketing, unsolicited messages etc.),

iii. Formation and conclusion of online contracts and,

iv. Liability for online intermediaries (service providers),

Accordingly, the main objective of the E-CD is to create a flexible; technology-neutral and stable legal framework, which will cover specific aspects of the electronic commerce within the internal market. The rationale behind the main objective of the E-CD is to ensure the free movement of information society services by removing cross-border provision on online services,

and providing legal certainty to businesses and citizens of MS of the EU. In referring to ISPs, the E-CD adopted the general name of Information Society Network and defines an ISP as:

“[a]ny service normally provided for remuneration at a distance by electronic means at the individual request of a recipient of services.”

In furtherance to its objective of regulating ISP liability within the EU, the E-CD introduced the controversial country of origin principle.\(^{36}\) The country of origin principle simply means that, as a general rule ISPs are subjected to the laws of the MS in which they are principally established. For example if an ISP is established in the UK, then it has to fulfil all the laws of the UK that regulates ISPs in the UK. However, intellectual property rights, consumer contracts and the freedom of parties to a choice of law in online transactions are excluded from the scope of the country of origin principle.

Likewise, regardless of whether the nature of claim is contractual, tortious, or administrative, all forms of liability triggered by third party activities against ISPs is addressed by the E-CD. This approach has been described as a horizontal approach.\(^{37}\) Typically, the most re-occurring examples of third party-triggered liability against ISPs under the E-CD include; intellectual property rights infringements, defamation, hate speech and child pornography.

In exempting ISPs against liability for third party contents, the E-CD introduced a special liability regime. The scope of special liability regime is limited to activities of technical nature that; consist of access, transmission and storage of data offered by [ISPs] information society services. The special liability regime can only benefit ISPs that operate subject to certain

---

35 Article 2(b) e-commerce Directives 2000/31/EC
36 Article 3 e-commerce Directives 2000/31/EC
conditions. That is, ISPs serving as mere conduit are not allowed under the special liability regime to take any step that interferes with the transmission of data. The same can be said with regards to caching services. The special liability exception will only benefit ISPs offering caching services when the caching is automatically done, and not when ISPs intentionally go further, and makes cached copies by selecting the proxy server from which to transmit contents. This is because the technical ability to select content means an interference with data transmission and it invariably dissolves immunity.

In respect of hosting services, ISPs are included in the special liability of the E-CD when they have no knowledge of the offensive nature of third party contents, but upon having knowledge they expediously remove the offensive contents. As a result, the E-CD in articles 12-15 provides for a safe haven to ISPs when they act as mere conduit, caching and hosting platforms subject to certain conditions that are discussed below.

3.2 Regulating ISP liability under the E-CD 2000/31/EC.

Under the E-CD, ISPs are generally exempted from the obligation of monitoring third party contents. In addition ISPs are not required to keenly pursue facts or circumstances indicating illegal activity as long as they serve as a "mere conduit" or provides momentary “caching services,” or basically offer hosting services. The reason for exempting ISPs from liability when they provide the aforementioned services is explained as follows;

3.2.1 Mere conduit.

Hypothetically, mere conduit is a situation where ISPs delivers transitory services in connecting subscribers to the Internet for instance by means of a dial-up modem. Within the context of the

38 Article 15
39 Article12
40 Article 13
41 Article 14
E-CD ISPs are excluded from liability based on mere conduit, because ISPs do not make any further selections or changes to the information, instead information are transmitted in their original form. This implies a purely passive role of neither having knowledge of nor the ability to control the contents. In other words where ISPs acts as mere conduit the knowledge requirement is not strictly applied. Specifically, the E-CD states in Article 12 that an ISP acting as mere conduit will not be held liable for information transmitted on condition that an ISP:

\begin{itemize}
\item[a.] does not initiate the transmission;
\item[b.] does not select the receiver of the transmission; and
\item[c.] does not select or modify the information contained in the transmission."
\end{itemize}

Mere conduit is very crucial in exempting ISPs from liability in allegations involving defamation and intellectual property rights infringement, and this position has been confirmed by court decisions. The similitude of mere conduit is the postal service system that delivers a defamatory letter or a copied picture in violation of copy rights. The post office cannot be held liable for failing to know the illegal nature of the contents of the letter.

3.2.2 Caching.

Exempting ISPs offering caching services from liability under the E-CD depends on; whether portions of a data is automatically and temporarily stored, or a whole set of data is deliberately and permanently stored in a proxy server in order to make it more efficient for onward transmission. Automatic and temporary storage of data is known as system caching. While deliberate and permanent storage of data is called mirror caching.

Article 13 of the E-CD generally exempts ISPs from the liability of third party contents resulting from system caching. This is because ISPs only have a restricted level of knowledge in relation

---

43 Telekabel Wien GmbH v Constantin Film Verleih GmbH Case C-314/12
to the data they transmit or store. In essence ISPs do not interfere with the data in system caching. But with regards to *mirror caching* ISPs are *not generally* exempted from liability by the E-CD,\(^\text{44}\) because there is technical interference with the data intended for onward transmission. This situation transforms ISPs from passive intermediaries into active intermediaries. Based on the requirements of Article 13, it is self-evident that ISPs can only be exempted from liability of third party contents in terms of *mirror caching* under the following conditions:

i. if the cached contents are not enhanced and/or re-modified. For example a cached copy should not be re-modified to circumvent technological protection measures such as passwords or encryptions.\(^\text{45}\)

ii. similarly, any form of update in the original copy must be reflected in the cached copy as well, and if access to the original copy is blocked or removed because it is considered to be offensive, then access to the cached copy must be blocked or removed as well. This is significant because contents containing defamation or intellectual property infringement for instance, having once existed on the original page may linger for quite a long time until deleted from each cache where they have been duplicated.

Hence Article 13 E-CD does not mainly concern itself with the illegal content in issue, rather it aims to protect the system that temporarily stored the illegal contents- ISPs hosting the proxy server from which the exemplar is stored.\(^\text{46}\)

### 3.2.2 Hosting services.

Practically, hosting services is the ability to store contents or to make contents available on the internet. Examples of hosting services include; maintaining a website, managing personal pages

---

44 Article 13. e-Commerce Directive
45 Affirmed by the EUCJ in Case C-466/12, Nils Svensson et al v Retriever Sverige AB.
46 This has been technically explained in chapter two.
online and storage of data in the cloud\textsuperscript{47}. As opposed to mere conduit and caching services, ISPs offering hosting services mostly performs an active role. This is because contents are purposely selected, uploaded and then hosted or stored for a longer period of time.\textsuperscript{48} Article 14 of the E-CD provides that ISPs will not be held liable for the contents it stored or hosted provided that an ISP:

\begin{quote}
\begin{enumerate}
\item \textit{does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of the facts or circumstances from which the illegal activity is apparent; and},
\item \textit{upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access of the information}.  
\end{enumerate}
\end{quote}

Accordingly, under Article 14 actual knowledge is the basic element for attaching and/or exempting ISPs from liability. Ahlert et al, argues that the meaning of actual knowledge is not well settled, because sending an email is still a form of notification and it remains to be proven if the email actually emanates from the complainant. Furthermore the term “awareness” will by implication require a self-effort on the part of ISPs to monitor the Internet for offensive contents instead of waiting to be notified by affected parties.\textsuperscript{49}

The European Union Court of Justice (EUCJ) interpreted actual knowledge or awareness to mean “\textit{the awareness of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question}.”\textsuperscript{50} Moreover, in an effort to establish a working definition of actual knowledge, a workshop tagged “The EU regulatory framework for

\textsuperscript{47} Previously explained in the last chapter.
\textsuperscript{48} The EUCJ in C-236-238/08 and C-324/09 respectively.
\textsuperscript{50} L’Oreal vs. eBay, C-324/09
e-commerce” conducted by the World Trade Organisation,\(^{51}\) formulated the following steps on how to obtain actual knowledge or awareness.

i. Through a notification from an affected user in a concise, sufficient and adequately substantiated manner,

ii. Through an investigation undertaken as a result of ISPs own initiative.

iii. When performing an active role.

Apparently, these prerequisites place ISPs in a dilemma between the distress of succumbing to unfounded claims and being subject to liability. This is true considering the variety of data that passes through their servers, and the possibility of encrypting some contents. In principle, these requirements appear to defeat the purpose of Article 15 E-CD which does not oblige ISPs to monitor their servers for offensive contents posted by third parties. However, “the E-CD at the same time specifically allows Member States to impose a duty of care on ISPs, in order to detect and prevent certain types of illegal activities.”\(^{52}\) This duty of care connotes employing any means necessary by ISPs to avoid incurring liability for offensive contents.

According to Lodder,\(^{53}\) ISPs can avoid liability for third party contents when they temporarily remove the offensive contents claimed of, and thereafter wait for a counter-claim maintaining that the content is not offensive. If there is a counter-claim ISP must re-instate the content, otherwise the content stays down\(^{54}\). This is generally called ‘notice and take down’.

### 3.3 The notice and take down procedure

Notice and take down (NTD) procedure as noted in the last chapter is the most popular route for restricting access to offensive contents on the internet. NTD works well in protecting copyright,

---

\(^{51}\) WTO Workshop Geneva, 18\(^\text{th}\) June 2013.


\(^{54}\) Based on the grounds that ISPs disseminates contents on the Internet by virtue of an existing contract.
child pornography and in safeguarding reputation online. ISP must ‘remove or disable access to illegal contents with due diligence when requested by law enforcement authorities or customers.’ In essence ISPs employ a NTD scheme by way of self-regulation so that they can avoid liability for offensive contents posted by third parties. The advantages of a NTD as a self-regulation is that, it reduce the high costs of litigation by providing a quick way of addressing consumers’ complaints.

Yet still, in a NTD regime ISPs are placed in a difficult position. On the one hand, they have a customer whom they had entered into an agreement with for the provision of internet connectivity and/or web hosting services. If an ISP removes materials posted by that customer without the appropriate right to do so, this will potentially incur a civil liability resulting from breach of contract and/or a violation of freedom of expression leading to the award of damages.

On the other hand, where an ISP becomes aware of unlawful contents and fails to remove them, it may be liable for the availability of or access to such contents. This also gives rise to a claim in civil liability or even criminal prosecution. Therefore the best way to address this conflict is for ISPs to have clear contractual terms and conditions setting out the circumstances under which their services may be used. Again the terms and conditions should permit ISPs in their absolute discretion, to remove material from their servers. By doing this, ISPs can protect themselves against any claim for damages in a civil suit for breach of contract; at the same time ISPs are excluded from liability for any action taken in order to restrict access to or the availability of third party contents on the Internet.

---

As outlined in the last chapter, the E-CD contains no standard NTD procedure. Nevertheless a framework for self-regulation has been established by the combined effect of recital 40 to the E-CD which provides for ‘a rapid and reliable procedure for removing and disabling access to illegal information’ and Article 16 which established a conduct code for ISPs. What is rapid and reliable is left unexplained however, whatever means adopted will likely involve;

i. a valid notice from an aggrieved party,

ii. removal of alleged offensive content by an ISP,

iii. possibility of issuing an ISP with a counter notice requesting a reinstatement of a content previously removed and,

iv. after receiving the counter notice, depending on the conduct of the ISP concerned, (that is whether it reinstates a content or otherwise) a court order is filed by the content provider\textsuperscript{56}.

A glimmer of hope for having a detailed NTD under the EU E-CD exist, because a public consultation committee initiated by the EU on single market captioned “A clean and open Internet: public consultation on procedures for dealing with illegal content on the Internet” held between June and September 2012,\textsuperscript{57} recommended the following;

a. establishing a standardised procedure for requesting a takedown of offensive contents on the Internet,

b. having a time frame within which to take down offensive contents on the Internet,

c. putting in place safeguards against misuse of notice requesting for a takedown of offensive contents on the Internet.


Before the outcome of the recommendations of the public consultation committee, the present rapid and reliable means of enforcing self-regulation on the Internet as provided by the E-CD remains in place. Parties aggrieved by the availability of third party contents on the Internet must turn to the courts for other remedies where ISPs are recalcitrant in enforcing self-regulations. If aggrieved parties opt to seek redress against offensive contents posted by third parties, then it is noteworthy to state that; courts do not attached liability on ISPs for offensive contents except where a legal duty of care exist, and it has been established that ISPs have breached that duty.

3.4 Legal duty of care under the EU ISP liability regime.

A legal claim emanating from an action of negligence can only be successful where there is a breach of legal duty, and not a breach of moral obligation. A breach of moral obligation is not actionable, but only renders the party at fault to societal ostracisms. However, there is a thin line which separates legal duty and moral obligation as pointed out by Ridolfi;

“The interdependence of law and morality, the circular influences of one on the other, puts us in a position to fear what we want the law to do. We embrace a legal system that promotes morality, that makes better citizens of us, but we worry that the law will cross an elusive line and infringe on individual rights.”

Ridolfi further argued that, ISPs as intermediaries are required to exercise an amount of duty of care for instance when hosting copyright protected contents by ISPs technically checking uploaded information before it becomes available. Customarily, the same requirement of legal duty of care holds for contents likely to result in the breach of trade secrets, or which leads to unfair competition, defamation and trademark violation. However this argument is not plausible as ISP based under the E-CD has no general obligation to screen for copyright violations. The

---

only obligation on ISPs is to screen for child pornography based on self-regulation.\footnote{Self-regulation is generally based on agreements which have the backing of the combine effect of Article 16 of the E-CD and recital 48 to the E-CD.} This is more evidently summarized as follows;

“[a] website or Internet portal that hosts or serves as an intermediary to online fraudulent schemes, website defamation, or other information-based torts and has actual or reasonable knowledge of such activity should have a duty to take measures to protect consumers—or at least to warn them.”\footnote{Carle, Jay C., and Henry H. Perritt Jr. “Civil Liability on the Internet.” GPSolo 23 (2006): 44.}

However, the legal duty of care is relaxed and ISPs are \textit{not generally} responsible for illegal activities that take place on the Internet without their knowledge, for instance identity theft.\footnote{Stealing the personal details of an individual with the aim of committing fraud- Article 8 Cybercrime Convention 2001.} In this instance the only legal duty on ISPs is to cooperate with law enforcement agencies by supplying personal and traffic data (IP addresses) of offenders.\footnote{Article 7 and 8 of the General Data Protection directive95/46/EC (also Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data), and provisions of the e-Privacy Directive 2002/58/EC. Also in the U.S based on a subpoena ISPs can reveal user data in violation to the provisions of the First Amendment.}

\subsection*{3.4.1 Burden of proof and defences available to ISPs under the EU ISP liability regime.}

Evaluating the burden of proof requires reviewing the duty of care imposed on ISPs by the law. The E-CD is only a legal framework that seeks to regulate the role and status of ISPs as online intermediaries by exempting them from the liability of third party contents under certain general conditions aforementioned. The E-CD is not a substitute for criminal and/or civil liability laws therefore, in order to establish a claim for defamation against an ISP for instance, a plaintiff must refer to the law of tort.

In practice whenever illegal contents are discovered online, the ideal reaction is to accuse ISPs. This stems from the fact that; ISPs are more visible rather than the original content provider, and
ISPs have technical control over the content that appears on the Internet. Whether ISPs can be made liable or not depends on their role and status, and how the courts interpret ISPs' obligations. Hence in evaluating the burden of proof, usage of terminologies such as "publisher", or "broadcaster", is not generally relevant except in defamation cases. Similarly intent is not a basic requirement when dealing with the availability of offensive contents on the Internet. However negligence cannot be ruled out in dealing with ISP liability. More particularly negligence can give rise to liability if the threshold for liability is strict or absolute. As a result of this ISPs can be in danger of being made liable for something that they have not committed themselves. In principle the burden of proving that an ISP has negligently failed to take reasonable steps in protecting the reputation of individuals or enforcing intellectual property rights on the Internet, is on the plaintiff. And in this regard the plaintiff must prove that:

i. the defendant ISP owes a duty of care to the plaintiff and,

ii. the duty of care has been breached. For example, ISPs that hosts or serves as an intermediary to online fraudulent organizations or website that are notorious for defamation, customarily has actual or reasonable knowledge of such activity. In these circumstances ISPs have a duty of protecting users—or at least to warn them.

Consequently, a plaintiff alleging negligence is required to identify the appropriate standard of care which the defendant ISP should owe, and to prove that the defendant ISP failed to observe that care. In other words, ISPs are obliged to observe professional ethics or standard practices in order to provide ‘reasonable’ protection to users against fraudulent organizations or against website that are notorious for defamation.

---

In addition, the plaintiff should be permitted to assert various genuine theories to show that the defendant ISP breached the standard of care required. For instance, that an ISP (by means of offering free WIFI services), actively facilitated easy access to a site that is notorious for fraudulent activities, or that an ISP failed to install basic security measures such as passwords, firewalls, and antivirus software or other authentication methods especially encryption keys, against websites that are notorious for fraudulent or reprehensible activities.

iii. The plaintiff must also prove that the injury is ‘sine qua non’ with the defendant’s breach of duty of care. Apart from establishing a causal link between the defendants conduct and the injury suffered, the plaintiff must show that the injury was foreseeable by a reasonable person. Carl et al were of the opinions that due to the prevalent use of the Internet and its global reach, it is impossible to deny the fact that injury is foreseeable as a result of a defendant's breach of duty of care.

These requirements emanate from a tort law perspective, and it provides for the means of holding ISPs liable for disseminating offensive contents on the Internet. ISPs on their own part are entitle to defend themselves, although in shifting the burden of proof on ISPs the standard required is not so high. This reasoning flows from a Latin maxim, ‘in pari delicto potior est condito defendantis’ loosely translated as; where both parties are at fault the condition of the defendant is better.

---

64 Conversely, any injury caused by acts independent of the defendant control is excluded.
66 This is because under the law of tort presumption of innocence operates in favour of the defendant. That the defendant is presumed innocent until proven otherwise. See Ridolfi, Kathleen M. "Law, Ethics, and the Good Samaritan: Should there be a Duty to Rescue." Santa Clara L. Rev. 40 (1999): 957.
3.4.2 **Defences**

In addition to the exemptions offered by the E-CD to ISPs against liability for third party-generated online contents, there are other defences available to ISPs as well. These defences mainly result from the nature of civil wrong alleged. In civil proceeding against ISPs for disseminating defamatory contents terminologies such as; publisher, author and editor are used interchangeably. The aim of this section is to briefly discuss defences available to ISPs in relation to defamatory contents. The reason for limiting the discussion on defamation and not including intellectual property right infringements is that, often defamation ignites more civil suits against ISPs than intellectual property right. Also protection of reputation is what entails human dignity, and once lost no amount of compensation can restore it.

In defending ISPs against liability for third party generated defamatory contents, the provisions of the Defamation Act of UK 2013 c-26(DA) will be considered. Besides being the most recent law for defamation repealing the 1996 Defamation Act, the DA provides for a well-established defence procedure for ISPs.

Against this background the DA in shielding ISPs against liability provides in section 5 as follows;

“it is a defence for the operator to show that it was not the operator who posted the statement on the website.”

In this context, the DA used the word operator to mean ISP and this description fits in perfectly, considering the nature and functions of ISPs previously stated. The conditions set forth by DA in determining if ISPs have a defence or not are;

(a) the extent of responsibility in hosting the content, and the decision to publish it,

(b) the nature or circumstances of the publication, and
(c) the previous conduct or character of the author, editor or publisher.

The defences available to ISPs for disseminating defamatory contents are as follows:

1. **Innocent dissemination**

Where an ISP is sued for hosting defamatory contents, it has a defence by simply proving that;

i. It did not authorize, edit or publish the statement complained of,

ii. It took reasonable care in hosting the publication

iii. It has no knowledge or reason to believe that it transmitted a defamatory content.  

The principle was applied in the case of *Bunt v. Tilley & Ors* where it was held by the court that ISPs are comparably equivalent to distributors of contents. The distributors’ liability as a defence emerged based on the court ruling in *Vizetelly v. Mudie’s Select Library*. In fact the ruling in *Vizetelly* was a locus classicus for notorious defamation suits involving ISPs in the United States such as Cubby, Inc. vs. CompuServe Inc, Stratton Oakmont vs. Prodigy, Zeran vs. America Online, etc.

Briefly, the facts in *Vizetelly v. Mudie’s Select Library* were that a circulating library distributed a book titled: “*Stanley’s search for Emir of Pasha in Africa*” which was alleged to have contained defamatory remarks. The issue for determination was whether the library can invoke the defence of innocent dissemination. In deciding the matter, Lord Justice Romer had this to say:

"That [they were] innocent of any knowledge of the libel contained in the work disseminated by [them], that there was nothing in the work or the circumstances under which it came to [them] which ought to have led [them] to suppose that it contained a libel, and that, when the work was

---

68 [2006] EWHC 407
69 This amplifies the provisions of the E-CD which under certain circumstances describes ISPs as mere conduits that lack knowledge about the activities of their customers.
70 [1900] 2 QB
71 776 F. Supp 135.
72 1995 WL 323710.
73 129 F.3d 327.
74 As can be seen later in Chapter four (*infra*) the United States operates under the common law legal system which allows judges to refer to cases from other common law countries in reaching a decision.
disseminated by [them], it was not by any negligence on [their] part that [they] did not know that it contained the libel, then, although the dissemination of the work by [them] was prima facie publication of it, [they] may nevertheless, on proof of the before-mentioned facts, be held not to have published it.”75.

This dictum provides a test for establishing the existence of negligence, which may defeat the defence of innocent dissemination. In addition to the defence of innocent dissemination in defamation allegations, the DA provides for the defence of; truth, honest opinion and publication based on public interest relying on the same test provided for by the Vizetelly case.

ii. Truth:

Section 2(1) DA stipulated that an ISP is defended in an action for defamation if it can show that, the posted statements complained of are substantially true. The defence of truth replaces the defence of justification hitherto obtainable under the repealed 1996 Defamation Act. However truth is not a defence where a defendant simply claims to be merely repeating a fact previously stated. This exception had been upheld in Chase v News Group Newspapers Ltd.76 In this case the claimant/plaintiff was a registered nurse employed by the South Essex Mental Health and Community Care. The Sun Newspaper of 22 June 2002, published a report under a large headline; ‘Nurse is probed over 18 deaths’. The story went on to describe how a certain nurse was suspected of administering painkillers to 18 terminally ill youngsters. Although the article did not name the nurse, a handful of readers were able to identify her. In spite of an injunction restraining the newspaper from further publication of the article, another angle of the story re-emerged in subsequent edition, and this time with a poor attempt to obscure the claimant/plaintiff photograph. The defendants maintained that “there were reasonable grounds for suspecting the

75 See note 64 supra.
76 [2002] EWCA Civ 1772
claimant of involvement in hastening the deaths of child patients. The court in dismissing the claim of the defendants stated;

“Under modern libel practice a defendant must set out in his/her statement of case the defamatory meaning he/she seeks to prove to be essentially or substantially true... The defendant does not have to prove that every word he/she published was true. He/she has to establish the "essential" or "substantial" truth of the sting of the libel. To prove the truth of some lesser defamatory meaning does not provide a complete defence.... A general requirement for journalists to systematically and formally distance themselves from the content of a quotation that might insult or provoke others or damage their reputation was not reconcilable with the press's role of providing information on current events, opinions and ideas.”

iii. Honest opinion.

Section 3 of the DA provides for the defence of honest opinion in an action for defamation. For this defence to apply, the defendant must inter-alia prove that;

a. the statement complained of was actually an opinion. What is required in this situation is the statement must be recognized by an ordinary person as a comment, and not a mere imputation of fact.

b. the statement indicated at least in general terms, the facts on which it is based either expressly or impliedly and,

c. that having regard to the existence of the publication complained of, whether an honest person could have held the opinion on the basis of any fact which existed at the time the statement was published.

These conditions were tested in Joseph v. Spiller In this case disagreement broke out between a musical band called ‘the Gilletes’ and their agent Mr. Spiller, in booking a venue for a certain event. The dispute led to exchange of letters between the Gilletes and Mr. Spiller, and according

---

77 Ibid at 12
78 Ibid at 15.
79 [2010] UKSC 53
to ‘the Gilletes’ the letter written by Mr. Spiller was defamatory. In delivering judgment in favour of the plaintiffs, Lord Philips states that;

“[w]here adverse comment is made generally or generically on matters that are in the public domain I do not consider that it is a prerequisite of the defence of fair comment that the readers should be in a position to evaluate the comment for themselves... the comments must explicitly or implicitly indicate at least in general terms, what are the facts on which the comment is being made. The reader or hearer ought to be in a position to judge for himself how far the comment was well founded.”80

According to subsection 5, the defence of honest opinion will be lost where the statement complained of was only published and not made by the defendant, particularly if the plaintiff/claimant can show that the defendant knew or ought to have known that the author did not hold the opinion.

iv. Publication on matters of public interest

The roots of this defence lay in the decision of Reynolds v. Times Newspaper Ltd.81 Based on this, the publication on matters of public interest was prior to enactment of DA 2013 known as ‘the Reynolds defence’. The publication on matters of public interest defence can be invoked principally by journalist in discharging their duties particularly in situations where an allegation of an illegality becomes so glaring, and it ought to be exposed. It matters not whether the allegations could be true or false. Similarly, it makes no difference whether the statement complained of was a statement of fact or a statement of opinion. However in order to rely on the ‘Reynolds defence’ the following conditions must be satisfied.

a. the defendant must show that the statement complained of was a statement of public interest or the statement formed part of public interest,
b. the defendant reasonably believed that publishing the statement was done in the interest of the public and,

c. in publishing the statement complained of the defendant must have observed the principles of objectivity and neutrality.

At this juncture it is relevant to state that the section 5 DA 2013 incorporated the *Reynolds defence*, as special defence for operators of websites [ISPs] in respect of defamatory statements posted on their website. However, this defence can only benefit the operator of a website if;

i. the original author of the statement complained of can be identified.

ii. furthermore the operator must not have been notified about the statement complained of, and

iii. where the operator is notified he acted promptly in removing it.

So far these are the classes of defence available to ISPs in relation to defamatory contents posted by third parties. A common denominator in these defences is that under no circumstances an ISP is allowed to moderate the website on which defamatory contents were encountered. Any form of website moderation dissolves all the aforementioned defence that ordinarily ISPs would have relied upon. By necessary implication moderation of website qualifies a website operator as the author of a defamatory publication.

### 3.5 Merits and drawbacks of the EU ISP liability regime

Remarkably, the major advantage of the EU law on ISP liability (the E-CD) is the existence of an elastic, *rapid and reliable* means of restricting contents on the Internet. The method has proven to be very efficient in enforcing the principles of international law regarding hate speech online. In this regard the interests of the harmed person or persons are safeguarded, because in order to avoid liability ISPs are anxious in removing the content as soon as possible. Similarly, the E-CD is advantageous for its generality and simplicity in regulating all illegal contents, even
though the burden of proof varies from one claim to another. For example a higher burden is placed in allegations involving child pornography than in copyright infringement or defamation. Also in line with a European approach to freedom of expression, the E-CD allows for state intervention in regulating ISP liability. Although this requirement is not so strict as can be seen;

“Member States should neither impose a general obligation on ISPs to monitor the information which they transmit or store, nor a general obligation to actively seek illegal activities on the network.” \(^{82}\)

An explanation of the above provision suggests that there is a possibility of MS, to compel ISPs to disclose the identity of authors of illegal contents; or to remove/prevent third party content from re-occurring on the Internet, specifically in a copyright infringement or child pornography cases. Although these are ex post measures which are carried out via a competent administrative body, or by a court order. The position succinctly explained when the E-CD is applied jointly with the Civil Enforcement Directive 2004/48/EC\(^ {83}\) and the Copyright Directive 2001/29/EC\(^ {84}\);

“Member States shall ensure that rights holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.” \(^ {85}\)

Notwithstanding the sophistication and good trappings of the E-CD some authors\(^ {86}\) expressed concern that the E-CD is not actually a coherent set, but a set of unbalanced topics. This statement becomes evident when one recalls that the E-CD is not a Regulation but a Directive,

\(^{82}\) Article 15 E-CD.

\(^{83}\) Article 11

\(^{84}\) Article 83

\(^{85}\) What can be sought form an injunction are; blocking of access to or the availability of offensive content, filtering content for onward transmission or expose original authors of offensive contents.

and Directives must be transposed into National legislations before they become effective. Equally too, the discretionary nature of Directives has resulted in some variations between the laws of MS one the one hand, and court interpretations of ISP liability on the other hand as can be seen in the following illustration.

i. Austria: ISP liability is regulated by the Federal Telecommunications Law of 1997. The legislation attaches liability to the operators of broadcasting installations and terminals (computer servers included), unless where these operators take ‘appropriate and reasonable steps to prevent wrongful use of their equipment.’ The existence of the Federal Telecommunications Status of 1997, has led to the neglect of the E-CD.

ii. United Kingdom (UK): the provisions of the Defamation Act 1996 (and later 2013), mainly formed the basis for defence against ISPs liability -particularly the innocent dissemination defence for distributors of hard copy and soft copy publications. As a result of this, the special liability regime designed for ISPs by Articles 12-14 is rarely refered to by the court when deciding defamation cases that involve ISPs.

iii. Spain did not enact a specific law for ISP liability, and this development created a wide-ranging legal uncertainty in terms of ISP liability. In its place the Spanish Penal Code regulates strict liability for ‘owners of any other method of communication’. While civil wrongs such as defamation are left to the Spanish Press Act, which prescribed a fault-based liability.

Secondly, the exemption from liability accorded to ISPs under the E-CD is only applicable in instances where ISPs act as; mere conduit, caching and hosting services. Impliedly this means that anything short of these services is not exempted by the E-CD. Thirdly, as Bayer puts it, the main goal of the E-CD was to set up a necessary legal environment for electronic businesses, and

---

for that reason “regulating ISPs' liability was just an additional by-product.” This statement may be the reason why the provisions of the E-CD failed to define offences and sanction against ISPs, and even where references on these topics are made they are so vague. For example, the provision of the special liability regime of the E-CD implies that; ‘ISPs are not liable as long as they do not know and have no reason to believe that the content is illegal’ opens too much room for ISPs to claim ignorance.

Another complication under the E-CD is that; ISPs have to decide whether a content is unlawful or otherwise. Invariably, a valid notice can symbolize that an ISP had knowledge of the illegal nature of content; however a notice does not actually assist an ISP in concluding whether the content in question was truly illegal. Apparently, this place more burden on ISPs to also determine the legitimacy of a notice.

Still on the issue of notice Ahlert was of the opinion that a lacuna exists in the E-CD. In attaching liability on ISPs for third party contents, instead of using the word ‘notice’ the E-CD only referred to ‘actual knowledge’ this requirement is rather too strict, and has thrown ISPs into a risky situation that demands more exhibition of expertise.

Likewise the actual knowledge requirement formulated by Article 14 E-CD in exempting ISPs offering hosting services from liability is misleading, as ISPs are confronted with a dilemma of assessing what is legal and illegal contents. In some cases such as copyright infringement the issue at hand is always obvious, however it is difficult to prove that a text is defamatory- the threshold is higher. Hence the level of actual knowledge requirement is left open for the courts of

89 These are the exceptions provided for by Article 12 -14 of the E-CD.
MS to decide, for example a court stated that; actual knowledge implies actual human knowledge and not computer knowledge.91 This has led courts of MS to further develop different practices in order to achieve the desired interpretation of actual human knowledge. For instance, in the UK courts take into account the surrounding circumstances in which manner a notice is received, such as contact details of the sender, location from which the information was posted and the unlawful nature of the information.

Another major drawback of the E-CD is that it failed to provide for an elaborate and/or harmonized procedure for taking down, and replacing content on the Internet. Neither did it provide for a safeguard against the abuse of notice for taking down contents. Case law has to be resorted to in defining the time frame for an expeditious removal of offensive contents. This somehow provides an opportunity for misuse of notices, and a biased treatment against content providers by ISPs in an attempt to steer away from liability.

In the light of the aforementioned drawbacks particularly the inconsistencies in the implementation of the E-CD among member states; a concluding remark is that, the special liability exemptions explained in Articles 12-15 is lacking in clarity, and would be difficult to rely on. These short comings are responsible for the general legal uncertainty in the EU ISP liability regime. Perhaps shifting attention to other jurisdiction such as the U.S would shed more light on ISP liability for third party contents.

91 Case : BGH, 23/09/2003, VI ZR 335/02, NJW 2003, 3764
Chapter four: Guideline on ISPs liability regime in the United States.

4.1. Introduction

The United States (U.S) operates under a vibrant and flexible legal system, called the Common law. Contractual obligations, tortious liability and issues relating to intangible properties are some of the areas covered by the Common law. The flexibility of the Common law allows judges not only to interpret the law, but also to make laws based on societal needs which are not foreseen by the legislature (Congress). In interpreting the law, Common law judges rely heavily on previously decided case law known as Stare decisis. Stare decisis means that previous judicial decision of competent court are binding and must be adopted in reaching a present decision. Stare decisis can be vertical where a judicial precedent of a higher court is adopted by a lower court and horizontal, if a court merely adopts its own previous judicial precedent or of another court but of similar status.92

In the absence of judicial precedent on a matter within a country, common law judges are allowed to adopt the decision of other judges from other common law countries. It is therefore common practise for a U.S judge to be influenced by a court ruling in Australia or the UK for instance and vice versa. This development fits in very well for this research, because the ISP liability is a global concern, and what is novel in a particular country might have been decided ages ago in another country. Accordingly, liability under the US Common law is classified into absolute liability or strict liability and vicarious or contributory liability.

Absolute or strict liability results from a defendant’s direct conduct. With regards to ISPs, absolute liability can be inferred based on their role and/or status. Admittedly, attaching absolute liability on ISPs means that hosting of offensive contents for instance are discouraged, and that

---

moral values are upheld on the Internet. Similarly, the administration of justice, especially prosecution of ISPs is effectively achieved through the attachment of absolute liability.

While contributory or vicarious liability results when a partly knowingly aided another to commit an injurious act. Vicarious liability arises from a special relationship which is developed in the course of contract for instance. Vicarious liability may arise on the Internet where for example, ISPs provide the incentives which aid third parties (customers of the ISP) to infringe intellectual property rights, or to post defamatory comments.93

In regulating ISP liability, the US set the pace in enacting laws and other countries follow. In this regards ISP liability in the US is broadly regulated by the Communication Decency Act 1996 (CDA), and the Digital Millennium Copyright Act 1998 (DMCA).

The CDA regulates ISP liability for hosting of defamatory and pornographic contents, while at the same time preserving free speech. The CDA immunized ISPs from tortious liabilities with regards to materials they gave access to, but which originates from third parties. The CDA explicitly exempted ISPs from liability by stating that; “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider94”

Whereas the DMCA was enacted to regulate copyright infringement with particular emphasis on the fast emerging technology of the time- the Internet.

4.2 The Digital Millennium Copyright Act 1998 (DMCA)

In complying with the requirements of the World Intellectual Property Organization (WIPO) treaty of 1996,95 the U.S Congress enacted the DMCA in 1998.96 The DMCA settles ISP liability by virtue of the Online Copyright Infringement Liability Limitation Act (OCILLA), under Title II.

---

95 The WIPO is body of the United Nations that administers the provisions of the Trade Related Aspects of Intellectual Property Rights (TRIPS), which required member countries to protect the interest of right holders against unauthorised access.
The OCILLA is enacted on the one hand to ensure that ISPs are provided with the incentives for removing infringing materials, and to protect ISPs from civil suits. On the other hand, the OCILLA was enacted in response to the concerns that ISPs are becoming afraid of incurring liability, and would be so reluctant to invest in technological experimentation.

The OCILLA served as a model for enacting part IV of the e-Commerce Directive 2000/31/EC (ECD) which deals with liability for online intermediaries in the EU. However, compared to the ECD which adopts a horizontally approach in exempting ISPs against all sorts of liability arising from third party content, the OCILLA is only limited to the liability for copyright infringements.

The DMCA through the OCILLA, sanctions digital infringement of copyright through a notice and take down (NTD) procedure. In a similar fashion to the ECD, the DMCA exempts ISPs from liability when they provide access, host or serves as a mere data transmission conduit. This exemption from liability is known as the ‘Safe harbour.’ However, unlike the ECD, the safe harbour under the DMCA also extends to ISPs that offers searching services. In addition, ISPs acting as service providers to non-profit bodies such as educational institutions are exempted from the liability of disseminating copyrights infringing contents.

The most important provision of the DMCA dealing with ISP liability is contained in section 512. Structurally, section 512 consists of 11 subsections which are numbered from (a) to- (k). The contents of these subsections include; setting conditions for ISPs wishing to enjoy the safe harbor (which is further explained below), sanctions against persons that willfully misrepresent a notice that leads to a content take down, and exemption of ISPs from the liability of removing

---

90 The DMCA was preceded by the Home Recording Act of 1992(HRA). The aim of the HRA was to regulate the production of digital audio tapes equipments and blank digital audio tapes on the one hand, and to immunise the producers of digital audio tape equipment and manufacturers of blank digital audio tapes on the other hand.
infringing contents. In addition the possibility of issuing subpoenas against ISPs requiring the identity of copyright infringers is also contained in the subsections of section 512. Finally, definition of terms such as what is an ISP, and what are the duties and liabilities of an ISP are to be found in section 512.

As stated above, the most central part of section 512 is the provision for a safe harbour to ISPs against liability for; data transmission conduit, caching, hosting, and serving as search engines. In order for ISPs to enjoy the safe harbour the following conditions must be satisfied;

i. ISPs functioning as mere transitory conduit for data are exempted against liability arising from third party content. 97 This is elaborated more where an ISP transmits, rout or provides connection at the request of another party- similar to the mere conduit explained under the ECD 2000/31/EC. However, this immunity will be forfeited where an ISP makes alterations and/or modification to the data intended for transmission, for instance initiating the transmission and selecting the recipient of the content. Knowledge of the offensive nature of content is not required under this heading.

ii. Where ISPs temporarily and automatically retain copies of data for onward transmission (caching), 98 then they are exempted from any liability that might arise in respect of those contents. Again an ISP intending to rely on this safe harbor must fulfil requirements such as; no modification of the contents, adhering to content provider’s request of updating, refreshing, and reloading of contents. In addition, where a copy of an original content has

---

97 Section 512(a) DMCA
98 A detailed explanation of this topic had been previously discussed in chapter three dealing with ISP liability under the ECD.
been removed, an ISP is expected to also comply and remove cached copies as well.\textsuperscript{99} These requirements are the same as those previously discussed under the ECD.

iii. Under the DMCA safe harbor, ISPs are exempted from the liability of storing third party contents.\textsuperscript{100} As opposed to caching which is usually automatic and temporary, storing of content is permanently done by ISPs on behalf of a party following a request in a form of contract. Storage of content is synonymous with hosting, and nowadays it is fashionable to host contents on the cloud for easy access and scalability. Consequently, ISPs wishing to rely on the hosting safe harbor must prove that they lack actual knowledge of the offensive nature of the questionable content. In addition to lack of having actual knowledge of the nature of infringing material, ISPs must not have received some financial benefits, such as profit accruing from the infringement.

iv. In contrast to the ECD, the DMCA provides a safe harbor for ISPs serving as; search engines,\textsuperscript{101} online referencing site and a hyperlink redirecting to other sites. However, exemption from liability means that an ISP only provided a hyperlink that redirects to a freely available web page. If the hyperlink gives access to users not hitherto intended by the author of the web page, ISPs incurs liability for whatever infringement that accrues.

An ISP that fulfils the aforementioned requirements is exempted from liability, and will therefore enjoy the comfort of the safe harbor. However the safe harbor is not free from invasion as ISPs are faced with allegations of hosting or transmitting offensive contents which they are unaware of. Consequently, upon receiving notice of having hosted or transmitted an offensive content, an ISP is obliged to take the alleged questionable content down.

\textsuperscript{99} Section 512(b) DMCA. It should be noted that storing is permanent and it is at user’s request, which implies that an ISP has knowledge of the contents. While caching is automatic and temporarily done from a technical point without user’s prompting.

\textsuperscript{100} Section 512(c) DMCA

4.2.1 Notice and take down Procedure

While the ECD requires ISPs to act expeditiously in removing or disabling access to illegal materials; the Directive did not establish a procedure for NTD, instead the liberty of implementing a NTD scheme is left to member states (MS). Unlike the ECD, the DMCA provides for a NTD procedure, including an obligation under section 512 for the replacement of contents previously taken down. The replacement must be accompanied by a valid request from the content owner. The DMCA provides for an elaborate NTD called the ‘report, remove, respond and replace’ procedure. Under the procedure a protest in a form of written report is sent to the ISPs concerned, and this serves as a valid notice regarding the offensiveness of a content.102

According to section 512, a protest notice must inter-alia contain a description of the subject matter of infringement, contact information of the complainant, a statement by the complainant stating in good faith that the use of the alleged material was an unauthorized use. What follows after receiving a protest notice is that;

i. an ISP takes down the alleged offensive material without judging its merits, and then informs the content provider of its action.

ii. the content provider is availed with the opportunity of contesting the removal of the questionable content. This is done by way of a counter notice (-usually sent within five working days), requesting for the replacement of the content previously taken down.

iii. depending on the merits of the counter-notice,

102 The protest notice has been upheld by the courts in Metro-Goldwyn-Mayer Studios Inc (MGM), et al. v. Grokster, Ltd., et al 545 U.S 913 (2005), and recently in UMG Recordings, Inc. v. Shelter Capital Partners LLC 667 F.3d 1022 (2013)
a. The ISP reinstates the content between 10 and 14 days after the reception of the counter notice, and where the ISP failed to honour the counter notice;

b. The party providing counter notice files for a court order confirming his claim. In this situation the ISP holds the information down, until the court has decided on the matter.

iv. Where, however the ISP does not receive any counter notice, then the content stays down indefinitely.

From the foregoing, the NTD procedure under the DMCA truly tilts in favour of the plaintiff (the intellectual property right owner) and the content provider is much at a detriment. In order to rectify this anomaly, Hughes\textsuperscript{103} is of the opinion that ISPs confronted with a notice of alleged infringements must, instead of immediately taking down alleged offensive content, forward such a claim to the content provider in the first instance. Where the content provider did not respond to the notice within a reasonable time (usually five working days), then the ISP can proceed and take down the alleged offensive content.

Discussions on the DMCA is meant to give a brief overview of ISP liability regime in the US especially in relation to the means of restricting access to the Internet, and it is not intended to deal with the DMCA extensively. Instead the focus of this research will be on the CDA more particularly the strength and weakness of the Good \textit{Samaritan Doctrine} in providing a legal shield for ISPs against liability of third party contents.

Prior to the enactment of the CDA, courts in the US resorted to the analogous common law liability regime in determining ISP liability for offensive contents posted by third parties on the

\textsuperscript{103} J. HUGHES, “The Internet and the Persistence of Law”, \textit{Boston College Law Review}, 2003, Vol. 44, No. 2, p. 383
Based on the Common law liability regime, ISPs are classified as publishers, distributors, or common carriers.

1. **Publishers** according to the common law liability regime, ISPs as publishers have substantial editorial control over the information they disseminate, similar to the traditional newspaper publisher. Because publishers actively select what to publish, it also means that defamatory contents will not go unnoticed. Knowledge of defamatory contents will be evident both to the traditional newspapers and ISPs as well.\(^\text{105}\)

2. ISPs classified as **distributors** are similar to public libraries or bookstores. These distributors have options on the type of information to disseminate, but lacks editorial control which publishers have. To establish liability for defamation against ISPs in the distributor category, a plaintiff must prove that the material was defamatory and that the ISP has knowledge of the defamatory nature of the content.\(^\text{106}\)

3. ISPs categorized as **Common carriers** have no editorial control and awareness over the information they transmit, because their role is merely a passive one. Common carriers are similar to the telephone company that connects users with each other, but does not have knowledge about the contents of information that passes through the transmission cables. A common carrier classification of ISP is equivalent to the mere conduits classification under the ECD.

This common law liability regime for ISPs (above) was subsequently integrated into the CDA.

### 4.3 The scope and interpretations of Communication Decency Act 1996 (CDA).

The application and also a rejection of the common law ISP liability regime as enunciated in the ruling of **Cubby, Inc v. CompuServe Inc.**\(^\text{107}\) and **Stratton Oakmont, Inc. v. Prodigy Services Co**\(^\text{108}\) below, spearheaded the enactment of the CDA. In **Cubby, Inc v. CompuServe Inc**, Internet.\(^\text{104}\)
CompuServe was sued for publishing false and defamatory statements on its forum. The statement alleged that “individuals at Skuttlebut gained access to information through a back door”. CompuServe pleaded inter-alia that; it only acted as the distributor (similar to a bookstore or a library), and not as the publisher of the statement. Furthermore CompuServe argued that it had no knowledge of the statements. Accordingly the reasoning of the court was in conformity with the arguments of the defendants that; bookstores and libraries are distributors, and therefore they are not liable if they have no knowledge of the defamatory nature of the content. In dismissing the case, the conclusion of the court was that; although CompuServe runs an electronic for-profit library by which its customers are charged, it was not feasible for CompuServe to sift every publication it disseminates for defamatory statements. Thus CompuServe was not liable for defamation.

Conversely, the common law distributor liability was debunked in Stratton Oakmont, Inc. v. Prodigy Services Co. In the Stratton Oakmont case comments were made on a bulletin board ran by Prodigy alleging that Stratton Oakmont had committed securities fraud. Prodigy (defendant) was sued for defamation by Stratton Oakmont (plaintiff). The Plaintiff argued that the defendant was a publisher because it committed itself into editing services. The defendant in a counter argument confirmed that its policies of editing contents of the bulletin board was to please its readers, and not to judge whether a content is defamatory or not. The defendant further argued that it received about 60,000 posts daily, making it practically impossible for it to screen all contents for defamatory statements. In entering Judgement for the plaintiff the court referred to Cubby v CompuServe (supra) and asked the question, whether Prodigy’s ability to exercise

---

109 See note no 107 (supra).
110 1995 WL 323710
editorial control was enough to make it an equivalent of a newspaper publisher? In answering the question, the court considered the following:

i. *Prodigy* presented itself to the public and its customers as controllers of the contents of its bulletin,

ii. *Prodigy* set guidelines on editing and screening contents posted on its platform.

The court held that a publisher status rather than a distributor status can be discerned from Prodigy’s action, and that liability accrued on Prodigy for granting access to the platform on which the defamatory comments were made.

Going by the conflicting ruling of the courts in *Stratton and Prodigy* cases which treated ISPs as publishers as well as distributors, the CDA was enacted to provide the right balance. According to the ‘general’ rule of the CDA,111 ISPs were no longer held as publishers or speakers of third party contents. Rather ISPs are merely distributors of contents provided by others on the Internet. Obviously the rationale for holding ISPs as distributors instead of publishers of contents rests on the premise that the huge number of contents hosted by ISPs makes it difficult to screen all contents for defamatory statements. If ISPs are to screen all contents the implication is that freedom of expression on the Internet will be stifled.

Indeed the CDA wishes to exempt ISPs from liability, where they exercise traditional editorial functions including taking decisions whether to give access to or block contents from the Internet. As a result of this ‘early interpretation’ of the CDA, ISPs operated with impunity not minding whether the interests of aggrieved parties are protected on the Internet or not. Moreover, early interpretation of the CDA only contemplated the safeguard of freedom of expression and legal

111 The exceptions are discussed below while analysing various cases.
certainty on the Internet. It was not until cases such as Zeran v. American Online\textsuperscript{112} and Blumenthal v. Drudge\textsuperscript{113} were decided that a new interpretation of the CDA began to emerge.

The ‘\textit{new interpretation}’ of the CDA is that ISPs are not liable as publishers, but are liable as distributors subject to certain conditions. Accordingly, “\textit{ISPs do not become publishers if they filter or screen content in order to enhance user satisfaction}.”\textsuperscript{114} Following the new interpretation of the CDA, publishing liability and distribution liability are clearly distinguished. Publishing connotes the ability to edit or alter contents, which by implication, means there is a high degree of involvement with contents that triggers the allegation of defamation. While distribution simply means to transmit content ‘\textit{as is}’ without the least interference except for optimizing user accessibility.\textsuperscript{115}

However in practice courts tend to ignore the thin line that separates the publisher- distributor status in dealing with ISP liability,\textsuperscript{116} and as a result ISPs are held liable for third party contents. This attitude of the court has resonated in the enactment of section 230 of the CDA which is known as the \textbf{Good Samaritan Doctrine}.

\textbf{4.3.1 Good Samaritan Doctrine of screening and blocking}

Concerned that court rulings such as in Cubby, Inc v. CompuServe Inc. and Stratton Oakmont, Inc. v. Prodigy Services Co\textsuperscript{117} cases would force ISPs to exercise stringent editorial control over third party contents, Congressmen Christopher Cox and Ron Wyden proposed an amendment to

\begin{itemize}
  \item\textsuperscript{112} 129 F.3d 327(4th Cir.1997).
  \item\textsuperscript{113} 992 F.Supp.4 (D.D.C 1998).
  \item\textsuperscript{115} David R. Sheridan, Zeran v. AOL and the Effect of Section 230 of the Communications Decency Act Upon Liability for Defamation on the Internet, 61 ALB. L. REV. 147, 179 (1997).
  \item\textsuperscript{116} \textit{Reno v. American Civil Liberties Union}, 521 U.S. 844, 117 S. Ct. 2329, 138 L. Ed. 2d 874 (1997).
  \item\textsuperscript{117} See notes 107 and 108 above.
\end{itemize}
the CDA. The outcome of the Cox-Wyden proposal saw the injection of section 230 into the CDA. The main provision of section 230 provides that;

1. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

2. No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.

By virtue of section 230 of the CDA, the traditional publisher liability inferred from newspaper to ISPs is abrogated and in its place a distributor liability takes charge. Thus section 230 serves as Justification for the legal shield provided by the Good Samaritan for blocking and screening of offensive [third party] contents carried out in good faith.

Section 230 contains six subsections which are arranged in the following order;

(a) summary of Congress findings that led to the enactment of section 230.
(b) policy goals of the US government in promoting the growth of the Internet and regulating user generated contents,
(c) immunity for Good Samaritan’s blocking and screening of offensive contents.
(d) duties of ISPs to inform users on the availability of parental control embedded protections,
(e) scope of section 230 which excludes Intellectual Property law, and Communication Privacy law,
(f) definition of terms contained in the provision.

The first case in which section 230 of the CDA was tested was Zeran v. America Online Inc. In Zeran an anonymous person posted a message on a bulletin board of America Online (AOL), advertising T-shirts with inscriptions relating to the Oklahoma City bombing. The message

118 129 F.3d 327, 330 (4th Cir. 1997).
linked users of AOL to the personal phone number of one Kenneth Zeran, and as a result Zeran started receiving disturbing phone calls including dead threats. All efforts by Zeran to get AOL to remove the posting from the bulletin failed, instead the phone calls increased. It was not until Zeran granted an interview to a local newspaper that people discovered that the message was actually a hoax. Consequently, Zeran filed a defamation suit against AOL for providing the platform on which a third party posted the alleged message. The court relied on section 230 of the CDA and held that AOL is only liable as a distributor, but not as a publisher. Furthermore the court stated that the aim of section 230 “was to promote the continued development of the Internet and other interactive computer services and to preserve the vibrant and competitive free market... for the Internet and other interactive computer services, unfettered by federal or State regulation.”

However in the opinion of legal experts, section 230 (c) was erroneously and broadly interpreted to include immunity for all tort-based liabilities, instead of only narrowing the interpretation to defamatory liability. Accordingly, ISPs should only be immune from liability when they lack editorial control and or knowledge. As Lindskey puts it "court decisions interpreting section 230(c) have broadened its ambit far beyond merely protecting 'Good Samaritan' editorial control.”

In spite of the erroneous interpretation of section 230(c) by the court in Zeran it nevertheless became a judicial precedent for post CDA court rulings. In fact the Zeran ruling established what is widely known as the ‘elements of the Good Samaritan Doctrine’. The elements are as follows:

1. The defendant must be a provider or user of an interactive computer service.

2. The questionable content must be provided by a third party, ideally another content provider but not the ISP in dispute. However, the defence of Good Samaritan will be lost if the ISP

---

119 Section 230(b)(1)-(2)
122 An interactive computer service has been defined in Schneider v. Amazon.com, Inc., 31 P.3d 37, 39 (Wash. Ct. App. 2001), to mean website operators and ISPs
takes part in creating the content in question. This is similar to the mere conduit provided by the ECD.

3. The plaintiff’s claim must treat the defendant as a publisher or speaker of the information in question.

Another breakthrough decision interpreting section 230 (c) of the CDA was *Batzel v. Smith.* In *Batzel* the question was whether according to the meaning of section 230 an ISP engaged in electronic newsletters qualifies as the publisher of e-mails that sparked defamatory allegations. The court referred to the case of *Doe v. AOL Inc.* where the Supreme Court of Florida stated as follows;

“*the aim of the congress in passing section 230 of the CDA was to encourage the development of technologies, procedure and techniques by which objectionable material could be blocked or deleted either by the interactive computer service provider[ISPs] itself or by the families and schools receiving information via the internet.*”

In delivering its judgment, the *Batzel* court held that since the defendant did not make material contribution to the questionable e-mail by altering the content, the plaintiff’s claim for defamation has failed.

Bothered by the widespread appeals and criticisms from legal experts, courts in the US were forced to narrow the interpretation of section 230 (c) CDA. For example a narrowed interpretation was applied in *Fair Housing Council of San Fernando Valley v. Roommates.com,*

---

123 *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1124 (9th Cir. 2003).
125 A publisher in this regard means a secondary publisher who contributed in developing contents supplied by the original (primary) publisher.
126 333 F.3d 1018, 1033 (9th Cir. 2003)
127 2001 Fla. LEXIS 449
128 Ibid at 450.
The Good Samaritan Doctrine

The Roommates case involved a real estate site that uses an online mandatory questionnaire. The questions were previously banned by the Housing Council on the grounds that they were discriminatory. The claim of the plaintiff was that Roommates qualified as an interactive service provider within the meaning of section 230(c) of the CDA. In addition the plaintiff claimed that, the services offered by Roommates which included the posting and dissemination of unlawful questions, which forced users to make discriminatory choices through a pull down menu goes beyond a mere distributor. The court adopted the reasoning of the plaintiff and held that; Roommate was not entitled to immunity within the meaning of section 230 (c) of the CDA, as it was Roommates (and not the users) who authored the questionnaire.

According to the court above, “the motive of the Congress behind the CDA was to immunize ISPs from the liability of removing user generated contents and not to provide immunity to ISPs against liability for content creation”. In this case the court is of the opinion that the website “contributes materially to the alleged illegality …”, and therefore the defendant in this case was the publisher of the information in dispute.

4.4 Burden of proof and defences available to ISPs under the US ISP liability regime.

There is a rebuttable legal presumption that ISPs do not have the slightest knowledge about the content they host nor cache- just like the library. Offences which ISPs may commit without mens rea include; making a cache copy of an objectionable publication in order to further display or publish to other users, or hosting the said objectionable content in anticipation of payment or financial gain. Therefore this section will briefly analyse the burden of proof required to establish liability against ISPs, and the defences available to ISPs under the CDA and DMCA.

---

130 521 F.3d 1157 (9thCir. 2008)
The Good Samaritan Doctrine

As a general rule under the CDA an ISP sued for defamation is innocent until proven guilty.\textsuperscript{131} Therefore a plaintiff seeking to hold an ISP liable for defamation under the CDA must prove that, an ISP which hosted the defamatory content was wilfully negligent by not screening the content before it became available. A plaintiff in a defamation suit also needs to prove that an ISP has been duly notified of the defamatory contents, but failed to block the contents. Put differently, an injured party must satisfy the ‘Calder effect test’.\textsuperscript{132} The Calder effect test simply requires the plaintiff to prove that the defendant instrumentally made the content available on the Internet.

What is required of the defendant ISP is evidence proving its innocence, and that the plaintiff’s allegations are false, or the statement is a qualified privilege under the common law of tort. The defence of innocent dissemination, honest opinion, and publication on matters of public interest which has been discussed in chapter three of this thesis while dealing with defences available to ISPs under the UK Defamation 2013 Act also apply here.

Whereas under the DMCA\textsuperscript{133} the plaintiff must prove, in a suit against an ISP for copyright infringement that;

i. The infringed content is a copyright protected content.
ii. The plaintiff must also prove that he is the owner of the infringed content,
iii. That the defendant ISP caused the work to be available to the public by hosting it on the Internet and,
iv. The plaintiff is also required to prove that the ISP has knowledge of the infringement.

These requirements were upheld in \textit{MGM Studios, Inc. v. Grokster, Ltd}\textsuperscript{134}. Where the question asked by the court was whether distributing a peer-to-peer (P2P) software amounts to

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{131} Section 230 CDA 47 USC 1996
\item \textsuperscript{132} \textit{Calder v. Jones}, 465 U.S. 783 (1984)
\item \textsuperscript{133} Section 512( c) DMCA 1998.
\item \textsuperscript{134} 545 U.S 913 (2005),
\end{itemize}
\end{footnotesize}
contributory liability in a suit for copyright infringement? In answering the question the court stated that;

"[t]he record is replete with evidence that from the moment Groskster...began to distribute [its] free software, [it] clearly voiced the objective that recipient used it to download copyrighted works, and [it] took active steps to encourage Infringement"\(^{135}\)."

The defences available to ISPs under the DMCA were massively deployed from the U.S Copyright Act of 1976. The following are the most commonly invoked defences against claims for copyright infringements.

1. Copyright invalidity: a defendant can prove that a work which the plaintiff alleges to have been infringed is not original and therefore not copyright protected.

2. Fair use is also a defence in a claim for copyright infringement.

3. Expiration: copyright in the U.S usually last for 95 years after the lifetime of the author, a defendant can prove that the duration of protection has lapsed, or the right holder has forfeited his rights in the work.

4. License: a valid authorisation from the right holder can also serve as a defence to copyright infringement.

**4.5 Merits and drawbacks of the US ISP legal regime.**

Beginning with the DMCA, an apparent NTD procedure has been highlighted as one advantage which other ISP liability regime such as the E-CD does not have. In the same context the DMCA protects abuse of notice requesting for a NTD by providing that "*any person who knowingly misrepresents facts causing a content to be taken down is liable in damages*"\(^{136}\).


\(^{136}\) Section 512(1) (f)
As a corollary the DMCA suffers some setbacks, for instance the incentive for a counter notification is vague as it is not clear under what circumstances that content previously removed may be allowed to resurface. Secondly, the privacy of content owners is not as protected under the DMCA as it is under the ECD. This is because in the US a simple subpoena to an ISP will ultimately give away the identity of a content owner. Unlike in the EU where courts of Member States are required to strike the right balance between the protection of fundamental rights and the enforcement of intellectual property rights.  

In assessing the other segment of ISPs liability regime in the US- the CDA, proponents of the law maintained that; Section 230 of the CDA was enacted in order to regulate obscene and indecent contents, but was later enlarged by virtue of cases so as to include all contents perceived as offensive and objectionable.

Critiques of the CDA are of the opinion that the CDA has been interpreted too broadly giving ISPs blanket immunity, and occasioning untold injustice to the victims of defamatory messages posted by third parties. The basis for this assertion is that courts in interpreting the CDA have often assigned a distributor status to ISPs in disregard of the editorial role of ISPs.

The Pitfalls of assigning the distributor status to ISPs are; ISPs classified as distributors may wilfully ignore defamatory contents posted by third parties simply claiming lack of knowledge. In Barret v. Rosenthal the court noted that a knowledge-based approach ‘will discourage active monitoring of Internet posting thereby frustrating the goal of self-regulation’ that had been envisioned by the Congress in enacting the CDA.

---

137 Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU Case C-275/06,
139 51 Cal. Rptr. 3d 55, 73 (Cal. 2006)
A counter argument to the above reasoning advanced by advocates of the CDA is that, too much screening of contents will diminish the popularity of ISPs. According to Sheridan “an ISP that removes members’ posting without any investigation is likely to get a bad reputation in a community whose first value is the free flow of information.” Consequently, ISPs will be required to maintain a balance between removing a defamatory content for instance and upholding their reputation.

Finally the CDA stimulates ISPs to practice self-regulation on the Internet by way of active monitoring especially for child pornographic contents. The drawback of active monitoring is that ISPs are often in a dilemma about which contents to disseminate, and which content to block. Weiner commented that, “immunizing a system operator (ISP) who knowingly and wilfully transmits inaccurate content on an electronic bulletin board does not promote the vibrant speech policy behind the CDA.” Will Weiner’s opinion serve as a prognosis to ISP immunity under the CDA? Perhaps looking at more recent cases such as Jones v. Dirty World Entertainment Recordings, LLC in the next chapter will undoubtedly clarify some of the underlying issues discussed above.

142 (840 F. Supp. 2d 1008 (E.D. Ky. 2012))
Chapter five: Analysis of Jones v. Dirty World Entertainment Recordings.

5.1 Introduction

The Communication Decency Act 1996 (CDA) has dominated the discussion in the last chapter. Several cases interpreting the CDA were looked into, and it was settled that ISPs should not be treated as publishers, but distributors of third party contents. However with the recent ruling in the case of Jones v. Dirty World Entertainment Recordings LLC, most of the salient features of the CDA emerged. Remarkably, commenting on third party comments will transform an ISP from a distributor into a content developer of third party contents. Simply put, for an ISP to enjoy the safe harbour against liability for third party contents provided for by the Good Samaritan Doctrine through the CDA, it must prove that it had nothing to do with the creation and/or development of the questionable contents. This is even the more so because ISPs are expected to act as neutral gateway to the Internet, notwithstanding their technical ability to restrict or allow access to the Internet.

However, the neutrality of ISPs is generally impaired by conflicting rights that once again places ISPs in between crossfire. These conflicting rights on the one hand are the right of content providers to post comments on the Internet anonymously which is protected by the First Amendments to the U.S Constitution, and on the other hand the right of aggrieved parties to seek redress for harm against their reputation. This raises debate about which right must be allowed to pave way for the other between the CDA and the First Amendments protected rights. Some authors maintained that “Freedom of expression must be upheld even if it means suppressing other fundamental rights.”144 Freedom of expression should not be interpreted to apply to a

---

particular medium of communication. Freedom of expression entails the right to seek, receive and impart information and ideas of all kinds irrespective of the medium that is involved whether orally, written or in the form of artistic design both offline and online. Accordingly, freedom of expression on the Internet will be meaningless if access to connection is denied.\textsuperscript{145}

The aim of this chapter is to scrutinize the case of \textit{Jones v. Dirty World Entertainment Recordings LL.C}; and conclude whether the court has properly balanced the freedom of expression of anonymous posters against both, the protection of reputation and the right to privacy of aggrieved victims on the Internet.

\textbf{5.2 Jones v. Dirty World Entertainment Recordings.}

The plaintiff in this case was Sarah Jones, who use to be a high school teacher in a district of Kentucky, and also a member of the football team cheerleading band called the \textit{Cincinnati Bengals}. Jones filed a suit against a gossip website known as \textit{TheDirty.com} operated by Hooman Karamian a.k.a Nik Richie. The website invites and disseminates posts from the visitors of the site. The defendant Richie responds to anonymous posts, by adding a comment that is always preceded by a tagline and written in bold fonts.

The plaintiff alleged that certain comment made about her on the defendant’s site were defamatory. According to the plaintiff, the comments lowered her esteem in the eyes of the public including the high school where she teaches. Jones sent an email to the defendant requesting for the removal of the alleged defamatory contents. Initially the defendant assured Jones that the comment would be removed, but instead more comments followed.

\textsuperscript{145} See, for example, testimony of the Organization for Security and Co-operation in Europe (OSCE) Special representative on freedom of the media to the U.S. Helsinki Commission in July 2011; available at http://www.osce.org/fom/81006.
In one of the subsequent posts that were disseminated, a photo of Jones appeared with comments underneath which partly read as:

“Nik, here we have Sarah J, captain cheerleader of the playoff bound cinci bengals. Most people see Sarah has [sic] a gorgeous cheerleader AND high school teacher. . yes she’s also a teacher. . but what most of you don’t know is . . Her ex Nate . . cheated on her with over 50 girls in 4 yrs. . in that time he tested positive for Chlamydia Infection and Gonorrhea. . so I’m sure Sarah also has both . . what’s worse is he brags about doing Sarah in the gym . . Football field. . her class room at the school where she teaches at DIXIE Heights.”146

Richie then added his own comment in the manner previously described and which reads as:

“why are all high school teachers freak in the sack?-nik.”147

Jones emailed the website operator for the second time requesting for the removal of the post, but this time around her request was flatly refused by the defendant. Disturbed, the plaintiff filed a law suit charging the defendants (DirtyWorld.com and its operator Nik Richie) with the defamation of character and the invasion of privacy. The defendants responded to the suit and pleaded that they are content providers merely disseminating comments posted by third parties, and that they are immunized from liability by section 230 of the CDA.

In determining whether the defendants are content providers/developers or merely distributors of third party contents, the Kentucky District Court referred to two cases as judicial precedent. One case was *Fair Housing Council of San Fernando Valley v. Roommates.com LLC,*148 and the other case was *Fed. Trade Communication v. Accusearch Inc.*149 The courts defined content development in the following manner: “a website helps to develop unlawful content, and thus falls within the exceptions to section 230, if it contributes materially to the alleged illegality of

---

146 Supp.2d 1008 (ED Ky. 2012)
147 Ibid.
148 *Fair Housing Coun., San Fernando v. Roommates. com*, 521 F.3d 1157 (9th Cir. 2008).
149 570 F.3d 1187, 1199 (10th Cir. 2009)-
the conduct.”150 And that “[o]ne is not “responsible” for “developing” allegedly actionable information only “if one’s conduct was neutral with respect to the offensiveness of the content.”151

By interpreting the opinion of the courts in the two cases it referred to, the Kentucky District Court in Jones formulated the following issues for determination;

i. The name of the site www.Dirty.com explicitly encourages the posting of filthy contents, by which the privacy and reputation of the plaintiff in this case were harmed by comments posted about her on the site.

ii. Mr Richie operated the website in such a manner that gives him the ability to review third party postings, and ultimately to remove any post complained of. But in this case which involves Jones, Richie simply refused to remove the posts.

iii. Richie’s added comments “Why are all high school teachers freaks in the sack?” complements third party post and incited more defamatory remarks. Indeed Richie’s conduct “effectively ratified and adopted the defamatory third-party post.”152

Based on the foregoing, the Kentucky District Court held that Richie’s conducts constitutes content development, and therefore the defendants are liable for the third party post. The Kentucky District Court further supported its position by stating that the provision of section 230 CDA only grants immunity to interactive computer service [ISPs], and not content providers that are by their name responsible for the creation and development of offensive contents.153 Noting that;

150 Ibid at page 25.
151 Note no 141 (supra)
152 Supp.2d 1008 (ED Ky. 2012)
153 “No provider... of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” 47 U.S.C. § 230 (c).
“[W]e therefore concludes that a service provider is "responsible" for the development of offensive content only if it in some way specifically encourages the development of what is offensive about the content”\textsuperscript{154}.

The court entered judgment in favour of the Plaintiff and awarded the sum of $300,000 as punitive damage, and $38,000 as compensatory damages.

Dissatisfied with the judgment of the Kentucky District Court, the defendants appealed to the Court of Appeal for the Sixth Circuit. At the Court of Appeal, the defendant (now appellants) contended among others that their name www.Dirty.com is not an issue worthy of determination. That they were immunized against liability for hosting anonymous third party posts, and that the Kentucky District Court applied the wrong standard in interpreting the provisions of section 230 of the CDA. According to the appellants, the CDA has immunized their activities as users of an interactive computer services and as distributors of third party contents. In their brief of arguments the following submission (drawn from the elements of the Good Samaritan) were made;

i. That they were both providers and users of an interactive services

ii. They were treated as speakers or publishers and,

iii. The questionable contents were provided by another content provider,

iv. According to the appellants there was no evidence which showed that they incited and caused more post which defamed Sarah Jones.

However, the following was not disputed by the appellants in seeking to rely on the immunity granted by section 230(c) (1) CDA;

\textsuperscript{154} Note no 147 (supra)
a. The alleged defamatory post were created by an anonymous third party and then submitted to the appellant,

b. The appellant did not modify the original post which gave rise to the allegation for defamation.

c. That Richie posted his own follow-on comments stating, “Why are all high school teachers freak in the sack?”

The Appeal court in re-affirming the decision of the Kentucky District Court, construed section 230 (c) of the CDA to mean that the appellants’ involvement with comments posted by third parties goes beyond mere editorial functions, but extends to the creation of contents. Richie’s comments at the end of each post added impetus to the original anonymous post. In other words Richie’s conducts in relation to the promotion of the offensive contents is far from being neutral, and any plea of immunity from liability by virtue of section 230(c) of the CDA will fail. In the opinion of the Court of Appeal a website designed to promote defamation is exempted from the protection of the CDA immunity. Particularly if its operators “invite invidious postings, elaborate on them with comments of their own, and call upon others to respond in kind, the immunity does not apply.”

However, the Court of Appeal took a different view with the Kentucky District Court with regard to its first issue of determination –the appellants name www.Dirty.com. The Court of Appeal referred to a decision by another court involving the same appellant, and concludes that the appellants’ website name alone does not render the appellant liable for comments which gave rise to the defamation suit, but what matters most in rendering the appellant liable is the contents

---

156 See issues for determination of the District Court above.
that gave rise to the suit. The Court of Appeal illustrated this point by stating that the name www.TheDirty.com does not necessarily mean the contents are altogether dirty, just as the name www.Apple.com, might not necessarily mean that it is a website dealing with the fruit called Apple. On a final note the Court of Appeal concurred with the District Court and held that the award of punitive damage to the plaintiff Sarah Jones is justified.

As discussed earlier the Jones case raises issues bothering on the freedom to express one’s self anonymously, and the right of safeguarding one’s reputation and/or privacy against invasion. Both the Kentucky District Court and the Sixth Circuit Court of Appeal re-emphasized that the right to post comment anonymously inherently exists under the CDA and the First Amendment to the U.S constitution. The two courts cited Shiamili v. The Real Estate Group of New York, Inc., et al.\textsuperscript{158}, wherein the following remarks were made; “Creating an open forum for third parties to post content—including negative commentary—is at the core of what section 230 protects.”\textsuperscript{159}

Against this background freedom of expression in the U.S is generally protected by the First Amendments to the U.S constitution.\textsuperscript{160} The First Amendment protection also extends to ISPs in freely distributing accurate speech on matters of public interest.\textsuperscript{161}

\textbf{5.3 The impacts of the Good Samaritan Doctrine on the freedom of expression.}

Admittedly, all speech that takes place on the Internet is enabled by online intermediaries- the ISPs. ISPs have the technical ability to block anonymous content providers who might tend to

\textsuperscript{158} 2009 NY Slip Op 09403 [68 AD3d 581].
\textsuperscript{159} Ibid. See also Pierce, Alan J. "New York's Appellate Courts Wrestle with Significant Issues in Internet Defamation Cases." (2013).

\textsuperscript{160} The First Amendment reads "Congress shall make no law...abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."
\textsuperscript{161} Reno v. A.C.L.U 521 U.S. 844, 885 (1997). The Supreme Court described an anonymous content provider as “a town carrier with a voice that resonates farther than it could from any soapbox.”
unleash harm on innocent parties. Though, filtering tools or software can block potentially obscene or vulgar language, these tools cannot verify with precision whether the blocking of content is a violation of freedom of expression or not. The bone of contention is that even if ISPs were to screen and block offensive contents, ISPs would be unable to determine the legal implication of their conduct unless interpreted to them through a legal action.

Hence the Good Samaritan is considered as a promoter of the freedom of expression on the Internet, by providing a legal shield for ISPs against the liability of disseminating third party contents. It must be noted that even though the CDA through the Good Samaritan Doctrine might have shielded ISPs from the liability of disseminating [offensive] third party contents, the legislation did not preclude the possibility of issuing ISPs with subpoena for disclosing identity of anonymous offenders. Disclosing the identity of anonymous offenders is tantamount to the denial of freedom of expression, and by implication ISPs will likely be accused of being biased against content providers. To this effect Kreimer maintained that ISPs obligation towards freedom of expression is delicate.\(^{162}\)

5.4. ISP Neutrality and anonymity within the context of the First Amendment.

Unlike in the offline world where offensive contents are rarely published; because newspapers and book publishers are guided by professional ethics and transparency, the internet has eroded the decorum of the offline publishing world, and in its place vulgar and obscenity are freely disseminated -worse still the authors are simply elusive. Neutrality for ISPs means the right to operate networks that involves the management of functions as well as the right to determine who qualifies for access into their networks and on what terms and conditions. More succinctly put, ISP neutrality suggests that;

“ISPs and governments alike are to treat all traffic and data flow on the Internet equally, without discrimination, regardless of the nature of the sender, user, type of data, content and platform. In addition, ISPs and governments are also prohibited from prioritising the transmission of data, from blocking content or from slowing down access to certain applications or services.”

ISP neutrality within the context of the First Amendment requires an assessment of whose rights to protect when interests of anonymous third party clashes with the interest of aggrieved parties. Numerous courts cases have reinvigorated the protection of anonymous speakers under the First Amendment. In other words anonymity on the Internet has heralded massive defamation suits and notices of copyright infringements against ISPs. More precisely ISPs were subpoenaed to reveal the identity of its customers/users in copyright and defamation suits.

Nonetheless anonymity has the advantage of preserving privacy, a guarantee against fear of retaliation and harassment. According to Justice Stevens;

“Anonymity is a shield from the tyranny of the majority..... It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society...”

Negatively, granting legal protection to anonymous speakers will stimulate reckless and unguarded speech on the Internet. Remaining anonymous, individuals are never held accountable for their speech or action. For instance in the famous WikiLeaks website case, Judge White...

---

163 Defending freedom of expression and information available at www.article19.org/
commented that “we live in an age when people can do some good things and people can do some terrible things without accountability necessarily in a court of law.”

Based on these facts Judges have formulated a test which is aimed at balancing the freedom of expression and the right to seek redress against anonymous offenders. In this regard the case that set the precedent in providing solutions to problems caused by anonymous speech was *MacIntyre v Ohio Election Commission.* In the case one Margret McIntyre distributed some pamphlets regarding an election in violation to the Ohio Code 3599.09, which forbade the distribution of anonymous campaign literature. The Supreme Court held that the Ohio Code was a violation of the freedom of expression and as such unconstitutional. Noting that;

“[t]he decision in favour of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one’s privacy as possible.”

Ideally in the U.S, a party who has been aggrieved by offensive third party content which has been posted anonymously, must contact the ISP concerned (through a notice) for a disclosure of the identity content owner. The utmost cooperation of ISPs is required in enforcing a subpoena seeking for the identity of John Does. Having been served with a subpoena, an ISP can still maintain its neutrality and stay clear from liability through the following options;

i. *Refusal to Act:* obviously an ISP may simply opt to do nothing and expect a subpoena to follow. Where an ISP does nothing and is subpoenaed, the immunity offered by section 230 of the CDA ceases to exist and under this circumstance the ISP would be treated in a

---

168 Ibid at page 331 as per Justice Stevens.
169 John Doe is actually a name given to anonymous and/or fictitiously-named defendants.
legal action as if it were the provider of the offensive content. However, the ISP is still having the usual defences that any publisher of information would have under the common law. In addition, the ISP would be entitled to an accelerated hearing of a motion to strike the action. Also an ISP might plead that it correctly believes the material in question is a protected speech. Similarly, an ISP can prove that the legal action was not carried out in good faith, but maliciously instituted. \(^{170}\)

ii. \textit{An order against legal action:} the second option available to ISPs confronted with a complaint from an aggrieved party for the conducts of anonymous posters is, to apply for a restraining order against legal action. The restraining order will strengthen the immunity currently available under section 230 of the CDA. However in order to be entitled to an immunity, the ISP is required to contact the anonymous poster and offer the opportunity to remove the posting within an agreed period of time for instance 10 days.

If on the one hand; the anonymous poster consents and removes the offensive contents, or if the ISP by virtue of the Good Samaritan Doctrine decides to remove the offensive contents, then no legal action will follow. On the other hand, if the anonymous poster refuses to remove the offensive content or the ISP is not very keen in acting as a Good Samaritan, then the ISP is obliged to cooperate with a subpoena or order of a court and reveal the identity of the poster. The ISP will still be immune from any liability resulting from any action for violating the right to anonymous speech under the First Amendment.

Broadly speaking, there are three tests propounded by courts in balancing the right to remain anonymous on the Internet, and the right to seek redress against anonymous offenders. These tests are:

a. *The motion to dismiss test*: The motion to dismiss test was formulated in the case of *Columbia Insurance Co. v. Seescandy.com.*\(^{171}\) It is so called motion to dismiss because as a precondition for disclosing the identity of John Doe, the test requires an initial claim which is powerful enough to withstand a motion to dismiss. Similarly, under this test courts are not interested with the actual content of the speech instead the identity of the speaker is what matter to the courts. A plaintiff relying on the test must:

i. provide sufficient evidence to support the fact that a real person or an existing entity is there to be sued,

ii. proffer the means by which to locate the defendant,

iii. prove that the suit will survive any motion moved for its dismissal and,

iv. file for a discovery\(^ {172}\) request accompanied by sufficient reason justifying the discovery.

b. *The Legitimate good faith test*: The test was developed following the ruling of *In re: Subpoena Duces Tecum to America Online Inc.*\(^ {173}\) The plaintiff in this application subpoenaed America Online Limited (AOL) for the true identity of certain John Does, and AOL declined from cooperating with the subpoena, arguing that the subpoena infringed upon the John Does' rights to speak anonymously. The Court required the plaintiff to adduce evidence or plead that there is legitimate good faith basis for the claim, and that the success of the claim is dependent upon revealing the true identity of the defendant.\(^ {174}\) What the

---

\(^{171}\) 185 F.R.D. 573 (N.D. Cal. 1999).

\(^{172}\) A discovery request is an application for the disclosure and production for inspection of any relevant material in the possession of one party by the other.

\(^{173}\) 52 Va. Cir. 26 (2000).

\(^{174}\) This does not contravene the requirements of the First Amendments.
ruling means is that an application for the disclosure of the identity of an anonymous speaker can only be made when the speech is actionable per se.

c. **The summary judgments test:** One of the early cases that directly address the issue of subpoena on ISPs was *Dendrite International, Inc. v. John Doe*\(^\text{175}\). In this case the court denied Dendrite’s attempt to discover the true identity of a poster on a Yahoo! message bulletin about stock trading, holding that Dendrite did not prove a probable cause of action resulting from the defamatory posting. The court instead recommended the manner in which subpoena is to be served on ISPs seeking for the identity of anonymous posters. The recommendation is that a trial court must first of all;

1. consider and decide an applications for a subpoena by striking a balance between First Amendment protected right to speak anonymously, and the right of the plaintiff to assert recognizable claims against *John Doe*.

2. thereafter, the following four-part thong test for serving subpoenas on ISPs are to observed by the courts;

i. the plaintiff must make efforts to notify John Doe that he is the subject of a subpoena or application for an order of disclosure. The court will normally withhold action to afford John Doe a reasonable opportunity to file and serve an opposition to the application for a subpoena.

ii. the plaintiff must clearly and sufficiently identify the exact actionable statements purportedly made by John Doe,

iii. the plaintiff must prove that a prima facie case exist by adducing cogent evidence to support each element that forms the cause of action. This must be done prior to the grant of a court order seeking for the disclosure of the identity of John Doe. If the plaintiff have satisfied all these requirements then,

\(^{175}\) 775 A.2d 756 (2001).
iv. the court may order for the disclosure of the identity of John Doe and then allow the plaintiff to properly proceed with the action.

In addition to those requirements, the court in Solers, Inc. v Doe\textsuperscript{176} set forth a fifth requirement for courts to follow in enforcing or quashing a subpoena that inquires the identity of anonymous posters of offensive contents. Specifically, “courts must determine that the information sought is important to enable the plaintiff to proceed with his lawsuit.”\textsuperscript{177}

The Dendrite test was upheld in Independent Newspapers, Inc. v. Brodie.\textsuperscript{178} In this case Zebulon Brodie filed a defamation suit against Independent Newspapers and other anonymous posters. By way of response Independent Newspapers filed a motion requesting the court to quash the plaintiff’s request for the disclosure of the identity of anonymous posters. The court denied the defendants motion, and ordered for the disclosure of the anonymous posters. On appeal, the decision of the lower court was reversed based on the grounds that the Plaintiff Brodie did not plead a prima facie case of defamation against the anonymous posters\textsuperscript{179}. The court stated;

“[W]e believe that a test requiring notice and opportunity to be heard, coupled with a showing of a prima facie case and the application of a balancing test—such as the standard set forth in Dendrite— most appropriately balance a speaker’s constitutional right to anonymous Internet speech with a plaintiff’s right to seek judicial redress from defamatory remarks.”\textsuperscript{180}

In summary the test provided for in SeeScandy.com and Dendrite has provided the right balance between the First amendment rights of anonymous speech, and the right to seek redress against anonymous offenders especially cases involving defamation on the Internet. However, ISPs disseminating speech which is illegally obtained cannot be protected by the CDA and the

\textsuperscript{176} 07-CV-159 (D.C. Cir. Aug. 13, 2009)
\textsuperscript{177} Ibid
\textsuperscript{178} 966 A.2d 432, 407 Md. 415 (Md. App. 2009)
\textsuperscript{179} Ibid at page 447
\textsuperscript{180} Ibid at page 456.
First Amendment.\textsuperscript{181} Likewise it is imperative to state that freedom of expression generally goes along with duties and responsibilities, conditions and penalties. Put differently, 

"[t]he right to communicate anonymously is not absolute... and that the protection granted to right to communicate anonymously must be balanced against the need to assure that those persons who choose to abuse the opportunities presented by this medium can be made to answer for such transgressions."\textsuperscript{182}

5.5 \textbf{limitations to anonymous speech under the first amendments.}

Undeniably, restriction on anonymous speech is evaluated by the courts based on whether there is suppression of the speech or denial of access to the medium that hosted the speech. Furthermore, under the First Amendment restriction on the freedom of expression also extends to restriction on the right of speech anonymously. Consequently, restrictions of anonymous speech on the Internet based on the First Amendment are divided into:

a. \textit{content based restriction}: Exemplified in the in \textit{Mac Intrye} case (supra), it basically deals with issues involving:
   i. any speech that may incite violence and lawlessness
   ii. speech in violation of copyright,
   iii. Obscenity and,
   iv. Child pornography.

b. \textit{Time, place or manner restriction}: so called because this kind of restriction allows for the regulation of any speech which contravenes legitimate interest such as state secret, administration of justice and the maintenance of public order. According to the court in \textit{Ward v. Rock Against Racism}\textsuperscript{183}, time, place, or manner restrictions to the First Amendment must:

\begin{itemize}
  \item \textsuperscript{181} Bartnicki v. Vopper 532 U.S. 514 (2001)
  \item \textsuperscript{182} In re:Subpoena Duces Tecum to America Online Inc., No. 40570, 2000 WL 1210372, (Va. Cir. Ct. Jan. 31, 2000)
  \item \textsuperscript{183} 491 U.S. 781 (1989)
\end{itemize}
i. be content neutral,
ii. be narrowly tailored to serve a significant governmental interest and,
iii. leave open ample alternative channels for communication.

Hence by virtue of the First Amendment, any restrictions on anonymous speech on the Internet must reflect the principles of ISP neutrality. Similarly, any technical means of restricting the ability to post comments anonymously on the Internet must be transparent and adhere to due process. Due process means it must be legally prescribed and subject to a competent judicial review process. The judicial review must be implemented in the most cost effective and speedy manner. In other words it must be accessible to all litigants. The remaining discussions such as answers to the central research questions and recommendations are dealt with in the last chapter of this thesis.
Chapter six: Conclusion

6.1 Summary.

The impunity by which ISPs operate in the U.S has left the courts grappling on how to interpret the law, and on how to administer justice by striking the right balance between conflicting constitutional rights. To ameliorate the situation the Congress enacted the CDA in 1996 and the DMCA in 1998 in order to regulate ISP liability in the U.S.

The CDA was specifically enacted to serve the twin purpose of immunizing ISPs against the liability of disseminating defamatory and obscene contents, and to promote free speech on the Internet. Based on the CDA, ISPs are immune from legal action when they act as Good Samaritans, in screening and blocking offensive third party contents on the Internet. The purpose of the Good Samaritan Doctrine is to foster self-regulation on the Internet by curtailing unnecessary litigation against ISPs for disseminating offensive third party contents.

However case law has proved that; the CDA contrary to its name has neither promoted decency on the Internet, nor did it facilitate the freedom of [anonymous] expression on the Internet. Furthermore, it has been established through case law that screening and blocking is not an effective means of deterring defamation on the Internet. Stripping ISPs of the immunity granted by section 230 of the CDA is not called for, as this would lead to more litigation against ISPs for taking any action in good faith to control abuse on the Internet. After 18 year of its enactment, the CDA seems so frail and there is every need to refurbish it.

The DMCA was enacted in a similar fashion to the U.S Copyright Act 1976; following guidelines issued by the WIPO to regulate online copy right infringements in the U.S. The DMCA mainly sanctions online copyright infringement through a detailed and responsive notice
and take down procedure. The principal provision of the DMCA is section 512 which provides a safe harbour for ISPs against the liability of disseminating third party contents. Similarly, the provision has embedded some checks and balances against; abuse of notice for taking down unauthorized contents, and the possibility of issuing subpoena seeking for the disclosure of the identity of anonymous infringers of copyright materials. Accordingly, the DMCA has justified it purpose when measured against other legislations such as the E-CD of the EU.

The EU settles ISP liability through the E-CD which adopts a horizontal approach in dealing with ISP liability, and which (by virtue of Articles 12-14) provides a special immunity for ISPs serving as; mere conduit, caching, or hosting of third party contents under certain conditions. The E-CD has also given Member States the free hand to regulate ISP liability. This means that Member States can compel ISPs (by way of an ex post measure) to, disclose the identity of infringers of Intellectual property rights, and authors of illegal contents for instance child pornography. Disclosing the identity of anonymous offenders is reaffirmed by the provisions of EU General Data Protection Directive of 1995 and the e-Privacy Directive of 2002.

However the E-CD has some major short comings that create a lacuna and a general legal uncertainty in the system. These shortcomings are, the vagueness in the wordings of Article 15; ‘no obligation to monitor shall be imposed on ISPs by member states’ is in conflicts with the right to issue injunctions on ISPs. Also is no common standard set by the E-CD which guides Member States in enforcing monitoring obligation on ISP’s, and this leads to implementation differences. Again the special liability regime for ISPs designed by Articles 12-15 of the E-CD has some shortcomings is considered to be lacking in clarity as such difficult to rely on. Above all, the E-CD did not provide for the procedure of taking down and also an obligation for
restoring contents on the Internet. Neither did it provide for a safeguard against abuse of notice for taking down contents on the Internet.

In sum numerous court cases were analysed and a comparison was made between the EU ISP liability regime and the U.S ISP liability in order to appreciate the *strength and weakness of the Good Samaritan Doctrine in providing legal shield to ISPs against liability for third party contents*. In the process of analysing the Good Samaritan Doctrine, the central question posed was; what is the effect of screening and blocking third party content on the Internet, and on what basis should ISPs be held accountable for third party contents?

### 6.2 What is the effect of screening and blocking third party content on the Internet?

ISPs relying on legal shield provided by the Good Samaritans Doctrine will screen and block third party contents in a bid to steer away from incurring liability. The implication of screening and blocking contents on the Internet will lead to the suppression of freedom of expression of users of the Internet. By extension, access to related sites suspected of disseminating offensive contents will be denied. In essence the provision of the provisions of the First Amendments to the U.S constitution will be violated and ISP neutrality will become a myth rather than a reality.

### 6.3 On what basis should ISPs be held accountable for third party contents?

ISPs are susceptible to legal action for disseminating offensive third party contents, because apart from having the technical control over those offensive contents, ISPs are visible rather than the content providers. Going by the series of court decisions that interprets the Good Samaritan Doctrine; screening and blocking of offensive contents posted by third parties absolves ISPs from liability. Similarly, where ISPs do not deliberately promote the posting of defamatory contents, or do not derive financial benefit from that content they are not accountable.
However, ISPs are not exempted from liability, and should be held accountable for negligently disseminating content or hosting a site that;

   i. will corrupt public morals, established norms, and conventions. For example allowing child pornography to flourish on the Internet will leads to a slippery slope in reinforcing the subculture of child abuse. In addition, child pornography will be used for priming youngsters in illicit sexual conducts.

   ii. Is active in promoting extreme political views and hate speech, which will surely incite public violence and total breakdown of law and order.

   iii. specializes in providing recipes for making bombs and other noxious items.

6.4 Recommendations.

ISPs connect Internet user with the world, territorial boundaries are eroded and a regionally based ISP liability law such as the CDA, DMCA and the E-CD will be ineffective in regulating liability for third party contents. If ISPs screen and blocks a content in the U.S for instance, those contents can still be assessed from may be Nigeria or North Korea. Hence a recommendation will be to have an international standard that regulates ISP liability preferably an international treaty coordinated by the United Nations. The treaty should provide for a hybrid solution that encourages both self-regulation and co-regulation drawn from the principles of the CDA, DMCA and the E-CD. An example of such a treaty is the WIPO treaty on intellectual property which has been acceded to, and accepted by many countries.

Having a harmonised international standard on ISP liability is necessary in the light of the various loopholes identified under the EU ISP liability regime as contained in some provisions of the E-CD, while discussing the drawbacks of the E-CD in chapter three. For example, the vagueness and ambiguity on what constitute actual notice for implementing a NTD, and the lack
of a detailed NTD procedure itself. Similarly a harmonised international standard will provide clarity and legal certainty for the special liability regime contained in Articles 12-14 of the E-CD. Furthermore a harmonised international will ameliorate the conflicting Interpretation of the Good Samaritan Doctrine contained in section 230 of the CDA. Essentially the hesitant attitude of the court in attaching a publisher or distributor liability on ISPs for disseminating third party content would be settled. Once again, ISPs will not be liable for developing or complementing third party content by simply exercising their editorial functions as discussed in cases such as, *Stratton Oakmont, Inc. v. Prodigy Services Co* (supra) and *Jones v. Dirty World Entertainment Recordings LLC* (supra).

Consequently, the harmonised international standard should employ the following technical means of restricting access to or the availability of defamatory contents on the Internet;

1. removal of search links and cache copies relating to any subject of defamation.

2. graduated response (“three strikes and you are out”) method of terminating the subscription of a content provider who is notorious for providing defamatory content on the Internet.

3. NTD procedure of the DMCA (which is very elaborate), should be adopted in dealing with defamatory contents. In addition the new NTD procedure should consist of the following modifications;

   i. Allow victims of defamation to notify ISPs to take down defamatory content within a stated time. The notice should explain the nature of the defamatory material, and its location (URL), from which IP address it emanates.
ii. Upon receiving notice from a victim of defamation, an ISP must take down the content and in its place post a retraction. Of course ISPs must observe the principles of neutrality in treating a notice to take down.

iii. Due diligence must be observed in carrying out the new NTD. It should not be carried out by ISPs alone instead it must be backed up by a judicial review, and there must reasonable remedies for content providers whose contents were taken down or blocked from the Internet in error. ISPs refusing to take down content should not be held liable automatically, instead each case should be treated on its merit.

iv. While observing Seescandy.Com and Dendrite principle, request for unmasking anonymous offenders on the Internet should be granted by courts in dire needs such as; the administration of justice, in the interest of national security, and for maintaining public order, but not based on politically motivated actions or on commercial basis.
Bibliography

Cases: European Union.


Case C-70/10, Scarlet Extended SA v. Société belge des auteurs compositeurs et éditeurs (SABAM).


Court of appeal of Paris (4th chamber, section A), 6 May 2009, Dailymotion vs. C. Carion, the company Nord-Ouest Production et al.


Google/LVMH (C-236-238/08).


L'Oréal and others v eBay, judgment of 12 July 2011, C-324/09.

Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU Case C-275/06.


Tamiz v Google [2013] EWCA Civ 68.

Telekabel Wien GmbH v Constantin Film Verleih GmbH, Case C-314/12

Vizetelly v. Mudie’s Select Library, [1900] 2 QB.

Cases: United States.


Blumenthal v Drudge and AOL, Inc. (1998) 992 F Supp 44


Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003).


Doe v. Reed, 130 S. Ct.2811 (2010).

Fair Housing Council of San Fernando Valley v. Roomates.com LLC, 521 F.3d 1157 (9th Cir. 2008).


In re: Subpoena Duces Tecum to America Online Inc, 52 Va. Cir. 26 (2000).


JONES v. DIRTY WORLD ENTERTAINMENT RECORDINGS, LLC 840 F. Supp. 2d 1008 (E.D. Ky. 2012)

JONES v. DIRTY WORLD ENTERTAINMENT RECORDINGS, LLC (2013) No. 2:09-CV-219-WOB.


Tiffany (NJ) Inc. v. eBay Inc., -F.3d - 2010 WL 1236315 (2d Cir. Apr. 1, 2010)

UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (2013)


Zeran v America Online, Inc (1997) 958 F Supp 1124 (ED Va)

Books

Benedek & Kettemann 2014

Collins 2011

Cucereanu 2008

Glendon et al 2008

Lessig 1999

Langford et al 2000

Nchi et al 1996.
**Nunziato 2009**

**Price 2013**
Price, Monroe E., ed. *The V-chip debate: Content filtering from television to the Internet*. Routledge, 2013

**Ronald & Winn 2002**

**Susy & McLay 2002**

**Articles & Periodicals**


Barry Sookman, Hyperlinking and ISP liability clarified by Supreme Court in Crooke’s case October 20th, 2011


Gerson & Ryan; A Primer on Internet Exchange Points for Policymakers and Non-Engineers Working Paper, August 11, 2012.


Karolis Vinciūnas, Civil liability of internet service providers for transmitted information: problems and perspectives of legal regulation” Teisės apžvalga Law review No. 1 (8), 2012, p. 57-99.


Paul Ehrlich "Communications Decency Act § 230" (2002) 17 Berkeley TLJ 401;


*Internet*


Article 19, http://www.article19.org
Statutes

Europe

The Directive on the enforcement of intellectual property rights (Civil Enforcement Directive) 2004/48/EC.


Federal law Relating To Telecommunications (TKG) Austria 1997.

General Data Protection directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The Defamation Act of the United Kingdom 2013.


United States


Others

Eric Schmidt, ‘’we’ve listened- and this is how we’ll halt this depravity’ Google executive chairman on child pornography: mail online 18 November 2013.


AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS 1994(TRIPS).