Available online at www.rsu.ac.th/rjsh
RJSH Vol. 5, No. 2, July-December 2018, pp. 33-54

ISSN 2286-976X / Online: ISSN 2539-5513

Safe Harbor and Copyright Infringement on the Internet: A Need to Update the Paradigm

Bruce Weeks

International College, Rangsit University, Pathum Thani, 12000 Thailand
Email:bruceweeks@gmail.com

Submitted 4 November 2018; accepted in final form 5 December 2018

Abstract

Copyright law is to encourage the creation of artistic, intellectual, and scientific content, granting to creators exclusive rights to exploit their creations. Internet intermediaries such as websites, search engines and other on-line platforms commonly host third party content which can infringe on the creator's copyright. Safe harbor laws insulate Internet intermediaries from claims of infringement. This paper discusses copyright infringement and safe harbors in instructive jurisdictions addressing the underlying rationale used by legislators and courts and then comments on contemporary issues addressing the vitality of safe harbor protection. The methodology includes a survey of leading safe harbor regimes in the United States, the European Union, Canada and Australia, supplemented with case law that interprets the application of safe harbor rules for intermediaries plus important commentaries on the application of safe harbor rules are explored. Given the rapid changes in the sources of third party content, the swift revolution in the types of internet intermediaries and the difficulty in determining the effects of altering safe harbor principles, the widest application of safe harbor protections are preferable to ensure the continued dynamism of the Internet for all stakeholders.

Keywords**:** *technology, the Internet, copyright infringement, safe harbors*

1. Introduction

It is axiomatic to observe the Internet is central to the way people live today. People get their information on the Internet, people are entertained on the Internet, people do business on Internet, people even develop their social relationships on the Internet. Instead of driving to the supermarket, the bank, or a government agency, people click several buttons on a computer or swipe a smart phone to do business, communicate with government agencies, or settle their finances. For business the Internet, a market of global reach, has significantly lowers costs of entry (Elkin-Koren & Salzberg, 1999). Who provides the platform for these activities? As a simple definition an Internet service provider primarily delivers Internet access or services to customers. Recently the characterization of "services on the Internet" has exploded in range to include Facebook (social media) Google (mailbox providers, online advertising technologies, search engine, cloud computing, software), YouTube, (video-sharing website), Amazon (electronic commerce and cloud computing) Twitter (online news and social networking service) (Fletcher, June 29, 2018).

Importantly, the world of ISPs has evolved to become the "hosting" of data by "Internet intermediaries" which are the primary foundation of commercialized Internet activities. Take the most famous examples: The world's largest accommodation provider (Airbnb) owns no real estate and the world's largest taxi company (Uber) owns no taxis. The most popular media platform (Facebook) creates no content. The world's most valuable retailer (Alibaba) has no inventory. And the largest software vendors don't write applications (Apple, Google, Facebook) (Kennedy, November 25, 2005).

In tandem with the Internet's unprecedented growth in reaching most aspects of the economy and society, are the role of Internet intermediaries that provide the infrastructure that collects, hosts, organizes evaluates and disperses information originated by third parties. These providers support a mass of activities that provide platforms for innovative, inexpensive products and services rapidly delivered. This facilitation of market processes aggregates supply and demand creating network externalities: the effect that one user of a service has on raising the value of that service to other consumers. Internet intermediaries stimulate employment and entrepreneurship by lowering the entry barriers for small businesses. Long-tail retail offerings not previously possible, whereby businesses can sell a large number of unique items, each in relatively small quantities can now reach consumers. Online e-commerce intermediaries, such as Amazon

and Alibaba have liberated consumer with greater information, facilitating product and price comparisons which have lowered the costs to consumers. Search engines such as Google and participative networked platforms such as Wikipedia have enabled access to an unparalleled wealth of information. Online advertisers increasingly play an important role enabling intermediary platforms to provide ever more sophisticated content and services at no monetary cost to users. Facebook, Twitter and Match.com have provided opportunities for new and innovative social dealings (Perset, 2010).

Importantly there is sometimes tension between various functions of Internet intermediaries as their services can be used for both legal and illegal purposes, in particular with copyrighted material. Courts addressing safe harbor issues are facing increasing difficulties in interpreting the applicable statues and court case in adapting them to a new economic and technical landscape that involves new kinds of online intermediaries unprecedented levels of online copyright piracy. This paper will first explore various safe harbor regimes what have been adopted in countries around the world to protect intermediaries. This survey will include various cases which have arisen in these jurisdiction and the rationale used to resolve this disputes will be surveyed. Next, the new intermediaries which have evolved will be defined and the issues of copyright infringement these new technologies present will be identified. Finally, recommendations will be submitted on how to preserve the essential goals of copyright law while at the same time recognizing and incorporating the oftentimes conflicting rights and responsibilities of the emerging actors in the online landscape.

2. Methodology

The methodology employed in the instant research is literature review. Publications addressing the issues explored in this paper include peer-reviewed research papers relevant to the topic, the most authoritative legal cases from the highest appellate courts which are recognized for establishing principles under discussion herein, and official government publications and websites which announced or explained government policy on the topics explored in this writing plus recent commentary exploring issues addressed in the instant paper.

The safe harbor regimes in four countries are emphasized: the United States as it has the most comprehensive level of safe harbor protection; the European Union as recent legislative proposals have been launched to change the safe harbor setup, so the various arguments for change, both pro and con have been addressed; Canada because its “notice and notice” safe harbor system is novel and has had success in its practical application and finally Australia where lean legislative language has empowered courts to actively define theories of liability and the parameters of safe harbor protections. The inclusion standards used for sources used is research paper that are peer-reviewed, legal cases that have been found to be the most enduring precedents and articles including recent commentary on the emerging issues between rightsholders, content providers, intermediaries and users in the development in this dynamic area of the Internet which encompasses technology, the interchange of ideas, and emerging commercial practices.

3. Discussion

3.1 Copyright Law

As the topic of the instant paper is Internet intermediaries and copyright law introductory observations about copyright law are warranted. Copy rights are original artistic creations defined by statue such as songs and lyrics, movies, books and computer programs. Typically copyright grants an exclusive right in the copyright creator during the creator’s life plus some period of time, currently 70 years is common. The goal of copyright law is to encourage the creation of artistic, intellectual, and scientific content, granting to creators exclusive rights to exploit their creations. This fairness in copyright is based on the premise that the law ought to give authors what they deserve, hard work should be rewarded and authors should retain control of the fruits of their labors (Sag, 2018). The philosophical underpinnings in the can be found in the writings of John Locke. Locke posits that in order to incentivize society to the value labor should be rewarded. Specifically Locke's propositions recognized that society should strive for the optimal productive use of resources, such as ideas that the production of ideas requires one’s labor and that these ideas are appropriated from a "common" which is not significantly devalued by the idea's removal (Hughes, 1988). Describing this tread for justification for copyright in the United States William M. Landes and Richard A. Posner explained

that copyright law should "maximize the benefits from creating additional works, minus both the losses from limiting access and the costs of administering copyright protection" (Landes & Posner, 1989).

3.2 Copyright Infringement

A creator of an original work is given a set of exclusive rights to copy, distribute, and perform their works for a limited period of time. The type of protected works are defined in the copyright statue and include such works as books, plays, music, movies, photographs, paintings, sculptures, digital files, and web pages. (UConn Library, n.d.)

Using copyright-protected work without permission is infringement. If something is protected by copyright, it commonly cannot be made available to the public in any format, digital or otherwise, without permission of the copyright owner. As an example in the United States copyright ownership gives the copyright holder six exclusive rights:

The right to reproduce and make copies of an original work;
The right to prepare derivative works based on the original work;
The right to distribute copies to the public by sale or another form of transfer, such as rental or lending;
The right to publicly perform the work;
The right to publicly display the work, and
The right to perform sound recordings publicly through digital audio transmission.
17 US Code sections 107 through 122

Direct copyright infringement requires (1) ownership of a valid copyright, and (2) copying of the copyrighted material. Knowledge or intent is irrelevant in a direct infringement action. The infringed material must be original, must show sufficient creativity, and must be fixed "in a tangible medium of expression". In copyright, direct infringement occurs when a person without authorization reproduces, distributes, displays, or performs a copyrighted work, or prepares a derivative work based on a copyrighted work. 17 U.S.C. § 106.

An early case of internet intermediary liability for copyright violation was Playboy Enterprises, Inc. v. Frena. A well-known gentlemen's magazine, Playboy brought actions for copyright infringement against the operator of a bulletin board service. The defendant's bulletin board service contained unauthorized uploaded copies of photographs that were originally published in plaintiffs magazine. The defendant argued that he himself did not post those pictures, but his subscribers did and that as soon as he received notice, he removed them. The court found access and substantial similarity had been established and held that Frena violated Playboy's exclusive distribution and display rights. As the BBS was only available to those who paid a monthly fee, the court found that the purpose of Frena's use was commercial. (Playboy Enterprises, Inc. v. Frena, 1993)

3.3 Contributory Copyright Infringement

A defendant is contributory liable for copyright infringement if he (1) "knew or should have known" about the infringing conduct, and (2) "induced, caused or materially contributed to the infringing conduct of another." One who intentionally and purposefully participates in infringing actions, but does not actually commit the infringing actions himself, is contributory liable. One who "induces, causes or materially contributes to the infringing conduct of another," may be liable for contributory infringement. Unlike direct infringement, contributory infringement requires knowledge of infringing activity. (Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 1971). In Sega Enterprises Ltd. v. MAPHIA, the defendants owned and operated a computer bulletin board service which users of the bulletin board service uploaded and downloaded various Sega copyrighted video games. With defendants' knowledge and encouragement, the defendants profited from this activity. Sega brought an action against the defendants, charging them with copyright infringement. Sega established the concept that creating an online portal constitutes secondary infringement once the operator has knowledge of the infringement. (Sega Enterprises Ltd. v. MAPHIA, 1994)

An early technology case mapping out the jurisprudence of on-line vicarious liability was Religious Technology Center v. Netcom On-Line Communication Servs., Inc. In this case defendant Erlich was charged with copyright infringement by the Church of Scientology when he posted online copyrighted writings of the

Church. The Church also sued Netcom On-Line Communication Services, Inc. (Netcom), the Internet service provider for the Bulletin Board System (BBS) containing the alleged infringing postings, and Tom Klemesrud, the operator of the BBS which Erlich used to transmit his postings. The Court found that Klemesrud and Netcom were not liable for direct infringement because the copying that occurred between the computers on the internet was incidental to Erlich's intentional copying of the documents to the internet likening Klemesrud and Netcom to a photocopy machine where the public can make copies. The Court noted that to find Klemesrud and Netcom liable would create a huge pool of defendants as every computer connected to the internet copies data from other places on the internet, so the total number of potential infringers would be unreasonably large. The Court defined vicarious copyright infringement as where a defendant has the right and ability to control an infringer's acts, and receives direct financial benefit from the infringement. The Court found that there was evidence to show that Klemesrud and Netcom had the ability to control Erlich's postings. However, the Court found that there was no evidence that Erlich's infringement gave any financial benefit to Klemesrud or Netcom. (Religious Technology Center v. Netcom On-Line Communication Servs., Inc., 1995).

The Netcom decision does have a significant footnote in the development of safe harbor protections as it influenced the United States Congress to add the notice and takedown provisions to the Digital Millennium Copyright Act. (Asp, 2018)

Although the doctrines of contributory and vicarious liability have different tests and rationales, particularly as they are applied in the on line context no strict dichotomy exists between them. As one US Court stated: “The lines between direct infringement, contributory infringement, and vicarious liability are not clearly drawn.”. (Universal City Studios, Inc v Sony Corp, 1979) The doctrines have significant overlap, as a secondary infringer could often conceivably be either vicarious or contributory in its infringement. (Allweiss, 1999)

3.4 Internet Intermediary

Typically, intermediaries are objects, things or people that act as a link between other objects, things or people. The connotation of an online intermediary has come to signify more than simply the interests of two parties, linked together as a “go-between.” Specifically, online intermediaries provide an infrastructure that allows people to access, create, share, or manipulate information on the Internet. Accordingly, they have to balance the interests of many involved parties, like end-users, content-providers, buyers, sellers, advertisers, or regulators all occupying a central place with expanding functions both social and economic. Because of the increased potential for new functionality, online intermediaries may also possess their own political, economic, social, and technological interests, and are therefore no longer acting as “intermediaries” in the traditional sense of the term. The connotation of the term intermediary is constantly changing in the online world (Gasser and Shultz, 2015).

An Internet intermediary provides the basic infrastructure of the Internet such as digital services and platforms. Internet service providers (ISPs) are companies that provides provide their customers with the ability to communicate with the Internet providing an entry using several technologies, such as dial-up, DSL, cable modem, wireless or dedicated high-speed connections. Individual customers pay ISPs for Internet access while ISPs are interconnected to one another at network access points until transmissions reach a Tier 1 carrier, which is an ISP capable of reaching every other network on the Internet (Edwards, 2010).

Internet access providers (IAPs) are web hosts and cloud providers, and online platforms for the creation and exchange of content such as YouTube, WordPress, and Facebook. Individual websites that allow for user interaction) are also Internet intermediaries. Many public institutions such as schools, universities, libraries, galleries and museums provide Internet access and host content. ISP’s, IAPs or simply internet intermediaries risk infringing copyright when their users infringe as transmit infringing items with computers and software operated by Internet intermediaries. For example IAPs reproduce (temporarily, or for longer periods) and communicate (transmit or make available) copyright material. Their liability arises from common activities essential to the Internet, including: “traditional” web hosting/cloud hosting, hosting user-generated or user-created content or operating a search engine (Edwards, 2010).

3.5 Safe Harbors

A safe harbor is a shelter during a storm. A safe harbor is a provision (as in a statute or regulation) that affords protection from liability or penalty (Black's Law Dictionary, 2004). A safe harbor is a provision of a statute or a regulation that specifies that if certain conduct is observed the actor will not be deemed not have to violated a particular rule. The concept of a "safe harbor" denotes to a legal principle to to reduce or eliminate liability in certain situations as long as certain conditions are met. Various arrears of the law recognizes this defense against liability. For example, a safe harbor can be found in tax law when assets are sold and then leased back to the seller (Slovin et al., 1990). In the United States safe harbor provisions exist under rules of the Securities and Exchange Commission to protect management from liability for making financial projections and forecasts in good faith (Olazabal, 2011). This paper discusses issues surrounding safe harbors used by Internet intermediaries to find protection from claims of copyright infringement.

A vast array of commercial cultural and policy predilections shape Internet laws around the globe yet when addressing safe harbors for copyright infringement by Internet intermediaries the fundamental principles of most statutes share the same themes. Common underlying premises requires intermediaries - the two most board categories being carriage service providers that provide access or hosting services - to act passively and neutrally. Generally no requirement puts on a duty to monitor content that is either hosted or transmitted, by intermediaries, nor is there an obligation to make important endeavors to prevent copyright-infringing material from being located or passed on by their systems. The conventional standard is to create and maintain passive-reactive systems that call for action against third-party communications on a system only upon receiving allegations of copyright infringement from a rightsholder. With some exceptions which will be addressed herein, this approach exists in the laws of Australia, Canada, the European Union, Japan, Singapore, South Korea, and the United States. Some provisions are general in defining the actors, their duties and liabilities while, others spell out in great precision the expectations upon intermediaries. Some of the disparity has created difficult disagreements between rightsholders and Internet intermediaries in the establishment of safe harbors and raised calls to update safe harbor law in response to technological and commercial advancements (de Beer, J & Clemmer, 2009).

The architecture common to many on-line intermediaries is premised on unmoderated user contributions from third parties. These contributions, posts, links, images or videos are often shifting and unpredictable and challenge ISPs IAPs and other internet intermediaries in monitoring such user-generated content. For instance, million of notices are posted to the craigslist system each month, Google seeks to organize billions of unique URLs, while YouTube has thousands of video uploaded every minute. Site like Facebook or Twitter, are designed for immediate social interaction and it would be challenging for a site's administrators to instantly review in a meaningful way all the social conversations taking place on the site. Therefore, safe harbors for internet intermediaries were created to encourage the development of internet services unencumbered by the constant threat of liability for copyright infringment from third party contributors (Bramble, 2013).

Safe harbor legislation balances the interest of two major on-line actors: the content industry and online service providers. In 1997 prior to the implementation of a copyright law overhaul in the United States online service providers such as ISPs and search engines began lobbying the US Congress for a safe harbor from secondary liability which could arise from their customers' copyright infringement. This tension between copyright holders and service providers has only increased as time has gone on (Imfeld, 2005).

3.6 Safe Harbor Law in the United States

In the United States the Digital Millennium Copyright Act (DMCA) became law in 1998. DMCA was the U.S. implementation of the 1996 WIPO Copyright Treaty (WCT) directive to "maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information" while updating copyright norms for the digital age. In the context of safe harbors and Internet intermediaries, the law attempts to strike this balance by immunizing ISP's for copyright liability stemming from their own acts of direct copyright infringement (as primary infringers of copyright), as well as from the infringing acts of their users (as secondary infringers of copyright), provided that ISP's comply with general requirements protecting the rights of authors (Tarleton, 2004).

The US Congress sought to update copyright law "to make digital networks safe places to disseminate and exploit copyrighted materials." The act is divided into five titles, addressing different aspects of digital copyright law. Title I, implements the World Intellectual Property Organization Copyright Treaty, specifying protection for copyright owners and "creates the legal platform for launching the global digital on-line marketplace for copyrighted works." Title II articulates the liability of Internet service providers (ISPs) for copyright infringements transmitted over their networks. Title I and Title II work collectively to "make available via the Internet the movies, music, software, and literary works that are the fruit of American creative genius," while limiting the liability faced by ISPs in order to ensure that "the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will expand" (Bell Atl. Corp. v. Twombly, 2007).

The first safe harbor, set out in section 512(a), indemnifies service providers from copyright infringements for providing transmission, routing, connection services, and material storage while providing such services. In this definition the material is initiated by a third party, the services is an automatic process and the provider does not select the recipients of the material as part of the automatic response to a request of another. Finally the material must be is transmitted without modification of its content.

The second safe harbor, set out in section 512(b), indemnifies service providers for copyright infringement for the "intermediate and temporary storage of material" on a system or network which the providers control. The conditions are that the material is made available by an automatic technical process and the material is transmitted without modification to its content. The third safe harbor, set out in section 512(c), indemnifies a service provider for copyright infringement for storage, at a user's direction, of the user's material on the provider's system or network. The last safe harbor, set out in section 512(d), indemnifies a service provider for referring linking users to an online location containing infringing material or infringing activity.

The policy behind the Digital Milinium Copyright Act in providing a safe harbor from liability for copyright infringement was set out in the initial report behind the legislation. Congress intended that Section 512(a) provide a safe harbor to large internet service providers. The statute allows service providers that transmit, route, or provide connections without liability for secondary copyright infringement as part of a connection between users. For this safe harbor to apply, any copies made must be of a transient nature. (Senate Report, 1998, p. 20). Section 512(b) protects companies that cache data while providing connections to customers. Caching speeds up access to content accessed by more than one user by copying the data returned by a user's request for data from a remote server. While caching, the service provider may infringe copyright because the service provider reproduces copyrighted material, yet it simply allows the server to provide data to a subsequent user without transferring duplicate data over the Internet. Section 512(b) increases the efficiency of the Internet. (Senate Report, 1998, p. 41). The third provision, section 512(c), protects companies from liability arising from material posted by a user by providing a safe harbor when a service provider would otherwise be liable for an "infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider." (Senate Report, 1998, pp. 42-43) Finally, section 512(d) protects companies that index, refer to, and link to websites that infringe copyright. Search engines commonly index content without verifying the legality of linked content. Congress recognized the importance of indexing the Internet through search engines. (Senate Report, 1998, p. 49).

Section 375 (b) stipulates that the provider does not receive a financial benefit directly attributable to infringing activity. All the safe horror provisions require first, that the provider must not have actual knowledge that the material is infringing, or facts or circumstances from which infringing activity is apparent, and second, the provider acts expeditiously to remove or disable access to the material one having notice. Regarding the issue of financial benefit In A&M Records, Inc. v. Napster, Inc., the court held that copyrighted material on Napster's system created a "draw" for customers which resulted in a direct financial benefit because Napster's future revenue was directly dependent on increases in user-base (A&M Records, Inc. v. Napster, Inc., 2001). Conversely, in Ellison v. Robertson, the court held that AOL did not receive a direct financial benefit when a user stored infringing material on its server because the copyrighted work did not "draw" new customers. AOL neither "attracted [nor] retained [nor] lost…subscriptions" as a result of the infringing material (Ellison v. Robertson, 2002).

For an intermediary to be liable for "contributory infringement," the intermediary must have actual or constructive knowledge of the direct infringement and make a "material contribution" to the direct infringement as well (Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 2005). Essential definitions are the nature of "knowledge" and what sort of contribution is "material". With respect to knowledge, ignorance of direct infringement is not a defense to an intermediary to a claim of secondary liability under the "willful blindness" rationale for situations in which a defendant "should have" known of a direct infringement, but purposefully turned a blind eye or act upon facts or circumstances that indicated a direction of infringement. The court observed in In re Aimster observed that "Willful blindness is knowledge, in copyright law (where indeed it may be enough that the defendant should have known of the direct infringement" (In re Aimster, 2003).

In the case Perfect 10 v. Visa International, credit card companies were claimed to have infringed on copyrights with knowledge in processing payment transactions for infringing material. Plaintiffs argued that defendants had chosen to continue to process credit card payments to the infringing websites, despite having knowledge of ongoing infringement (Perfect 10 v. Visa International, 2007). An analogy was drawn from Fonovisa v. Cherrry Auction, where the defendant, who hosted "swap meets" where infringing activity was allowed was found liable for infringement. In Fonovisa the court held that the infringers and the swap meet providers were in a mutual enterprise of infringement which constituted material contribution and inducement. Perfect 10 argued that Visa was the cyberspace equivalent of such an illicit marketplace by the material contribution of Visa's payment process system. The court ruled the alleged infringing activity was not a material contribution. The court decided that infringement rested on the reproduction, alteration, display, and distribution of Perfect 10's images over the Internet Visa's payment processing services (Fonovisa v. Cherrry Auction, 1996)

Two seminal case cases clarifying contributory infringement for online intermediaries are the Sony and Grokster litigations. In Sony Corp. of America v. Universal City Studios the issue was a technology that may involve facilitating copyright infringement (video recorders), but may also be used in non-infringing ways. The court reasoned that constructive knowledge of possible infringement should not be imputed to the intermediary in this instance the makers of video recorders. The Sony case established the "substantial non-infringing uses" test, for intermediary technologies that only make direct infringement possible rather than certain (Sony Corp. of America v. Universal City Studios, Inc., 1984). The Grokster case expanded this theory, holding that simply because an OI's technology was merely capable of substantial non-infringing uses did not categorically immunize the OI from liability, and that contributory liability may still be found if there is clear evidence of an OI's intent to induce and facilitate infringement. This has become known as the Grokster "inducement rule." The court observed: "Thus, where evidence goes beyond a product's characteristics or the knowledge that it may be put to infringing uses, and shows statements or actions directed to promoting infringement…will not preclude liability" (Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 2005).

Viacom v. YouTube was a series of trial and appeals in a copyright infringement lawsuit originally filed in 2007 by Viacom, Paramount Pictures, and other media companies against YouTube a popular video sharing service On April 18, 2013, a federal district court judge again granted summary judgment in favor of YouTube dismissing claims of secondary infringement. Plaintiffs averred YouTube infringed copyrighted movies, television shows placed on YouTube while the Internet site defended claiming § 512(c) "safe harbor" protection as YouTube acted as a service provider, with no knowledge of infringing materials, and when informed promptly removed any infringing materials. Originally the trial court ruled in favor of YouTube's owner, Google, on a summary judgment, finding safe harbor principles protected YouTube (Viacom Int'l Inc. v. YouTube, Inc., 2013). On appeal the court remanded the case back to the trial court to determine whether YouTube had knowledge or awareness of any specific infringements, whether YouTube had not willfully blinded itself to specific infringements or if YouTube did had the "right and ability to control" infringing activity. In 2013, the trial court again granted summary judgment to YouTube on all three issues finding that the plaintiffs had not proven that YouTube knew or was aware of specific infringements, and claims of willful blindness "give at most information that infringements were occurring with particular works, and occasional indications of promising areas to locate and remove them." The court additionally ruled that "knowledge of the prevalence of infringing activity, and welcoming it, does not itself forfeit the safe harbor. To forfeit that,

the provider must influence or participate in the infringement." The court found no evidence that YouTube induced its users to submit infringing videos or "otherwise interacted with infringing users to a point where it might be said to have participated in their infringing activity." In 2014 Viacom and YouTube finally settled after 7 years of litigation (Stempel, March 18, 2014).

3.7 European Union Safe Harbor Discussion

Under the E-Commerce Directive (ECD) safe harbors are available to 'information society services', which are defined in the Information Society Services Directive (Directive (EC) 98/34 of the European Parliament and of the Council, of 22 June 1998, laying down a procedure for the provision of information in the field of technical standards and regulations [1998] OJ L204/37.) and the Conditional Access Directive.(Directive (EC) 98/84 of the European Parliament and of the Council, of 20 November 1998, on the legal protection of services based on, or consisting of, conditional access [1998] OJ L320/54.)

The motivation behind the EU Directive on electronic commerce is to develop information society services to ensure legal assurance and create consumer confidence for the proper functioning of the internal market, in order to create a legal framework to ensure the free movement of information society services between Member States. (Baistrocchi, 2002)

The definition of an information society services includes any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of a service. The ECD defines three types of online intermediary activities: 'mere conduit' (Article 12 ECD), 'caching' (Article 13 ECD) and 'hosting' (Article 14 ECD). The three types of intermediary activity (mere conduit, caching and hosting) that are exempted from liability correspond to activities of classical physical network providers, Internet Access Providers, and Internet hosting providers. Recital 42 of the ECD emphasizes the passive and technological nature of intermediary activities that are exempted from liability: The exemptions from liability [...] cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored. For an internet access provider to qualify as a conduit the internet access provider cannot initiate the transmission of information, select the receiver of information, or select or modify the information. Intermediary liability for caches or acting as conduits is limited when these intermediaries are in no way involved with the information transmitted. (van der Sloot, 2015).

Regarding hosting, the service provider is not liable for the information stored at the request of a recipient of the service if the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent and the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. Article 15 of the e-commerce Directive also establishes that member states shall not impose on ISSPs a general obligation to monitor third party content, or actively to seek facts or circumstances indicating illegal activity (OECD, 2011).

The hosting exemption is of general application however, there is a question whether the hosting exemption is only available to a hosting service provider that does no more than enable users to store data in a technical sense. For example, if a website owner publishes an editorial incorporating user content would the website be able to benefit from the hosting defense? In addition there is a case to be made that Recital 42 of the Directive supports an interpretation that a publisher benefiting from advertising revenue arising out of hosting third party content would not be able to benefit from any immunity from liability. (Leonard, December, 2010)

In L'Oreal v eBay, L'Oreal argued that eBay was not taking sufficient steps to stop the sale of counterfeits on its online marketplace. One question was whether eBay was entitled to rely on the liability exemption set out in Article 14(1) of the Ecommerce Directive in relation to the hosting of information provided by its various sellers. The case arose in the context of eBay's practice of assisting sellers, in some cases, to enhance their offers for sale, and promote and increase their sales (for example through display of

advertisements through use of Google keywords). The OEU held that in relation to a marketplace like that of eBay: '[T]he mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability provided for by Directive 2000/31 ... Where, by contrast, the operator has provided assistance which entails, in particular, optimizing the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31.'103 (L'Oreal SA and Others v. eBay International AG and Others, 2011).

A major distinction in the scope of the safe harbors between the US and the EU is the source and manner of the overall laws which govern intermediary liability. The US has a cumulative approach to the laws, for example the DMCA safe harbors codified in 17 U.S.C. § 512, are part of the Copyright Act and thus limit liability whether direct, contributory or vicarious arising from copyright infringement alone. Other laws which create intermediary liability on different issues spring from different laws. Juxtaposed to this is the EU "horizontal" approach where the law does not to focus exclusively on copyright, but addresses ISP liability in drafting a safe harbor to cover intermediaries' liability for any kind of unlawful content provided by their users, whether it is copyright infringement, trademark infringement, defamation, unfair competition, hate speech or illicit material. As the service provider is carrying out a similar technical activity be it transmitting, caching or hosting third-party content and the intermediary's actions are neutral and passive with regard to the content the logical is to establish a single set of rules covering all fields (Peguera, 2009).

Safe harbor remedies can vary in different jurisdiction. The DMCA and the e-Commerce Directive are different in their nature as the DMCA is a federal statute that creates a direct right of action while the EU e-commerce Directive sets forth a framework that member states must incorporate in domestic laws. The e-commerce Directive lacks some detailed procedural rules of the DMCA such as specific notice and takedown procedures, and measures for injunctive relief which are detailed and circumscribed in the DMCA. Although Recital 45 of Council Directive 2000/31/EC states that "The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it." Specific injunctive relief under the e-commerce Directive refers to national law for their procedure and scope where broader principles of fairness, equitability and proportionality regulating compensation under general principles of law often apply (Peguera, 2009).

3.8 Canadian Safe Harbor Discussion

The Canadian system differs in two major ways with its U.S. counterpart. First, the Canadian "Notice and Notice" procedure does not provide a direct duty for Internet intermediaries to take down allegedly infringing content. Second, Internet intermediaries are granted a safe harbor independently from their compliance with the Notice and Notice system. Under § 31.1 of Canada's Copyright Act, ISPs are "exempt from liability when they act strictly as intermediaries in communication, caching and hosting activities" In Canada, the Copyright Act merely states that "a person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate that work or other subject-matter to the public." The Notice and Notice procedure begins with a notice of claimed infringement sent by a copyright owner to a service provider. Sections 41.25 provides that a notice must identify the work of claimed infringement, the electronic location and the infringement claimed. Under Section 41.26(1)(a) upon receipt of a notice, the service provider is not required to remove the alleged infringing content, but rather forward the notice to the alleged infringer while retaining a record for six months (for one year if a court action has been initiated) on the identity of the alleged infringer. If a service provider fails to comply with any of these duties under the Notice and Notice procedure, the right owner is entitled to statutory damages under Section 41.26(3). The broad and less specific nature of the Canadian system is a recognition of industry practice that was going on for a number of years. In a 2010 submission on copyright

reform, major Canadian telecommunication companies explained that they had been collaborating with rights owners since the early 2000's by forwarding, at their own expense, "millions of copyright infringement notices to subscribers who are alleged to have infringed copyright" (Berkeley Technology Law Journal, March 2, 2014).

Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Providers, the Supreme Court of Canada held that the Copyright Act specifies that neutral intermediaries enjoy immunity from liability. This immunity is enjoyed "[s]o long as an Internet intermediary does not itself engage in acts that relate to the content of the communication, i.e., whose participation is content neutral, but confines itself to providing 'a conduit' for information communicated by others . . . ."The court also observed "[t]o the extent [that Internet service providers (ISPs)] act as innocent disseminators, they are protected by [§]2.4(1)(b) of the Act." The opinion found an analogy to owners of telephone wires who were "utterly ignorant of the nature of the message" and thus not accountable for the content of the transmissions. As a result, although Canada does not have an explicit list of requirements for immunity from liability for transitory communications, the effect of the general provision is similar to other jurisdictions' more detailed schemes (Society of Composers, Authors & Music Publishers of Canada v Canadian Assn of Internet Providers, 2004).

Because it provides an expeditious and effective method to remove infringing material the US notice and takedown regime is cited for effectiveness in curtailing copyright infringement on the Internet. On the other hand commentators on this regime contend that it creates an incentive for ISPs to remove alleged infringing content from their network even in circumstances that the material might not be infringing. The result is this situation can lead to violations of free speech in commenting on issues of public importance, restrictions on creativity, the deterrence of technological innovation, and decrease access to creative works by Internet users. For instance, works like parodies, which are generally not infringing under the fair use defense, are traditionally at risk under common notice and takedown practice. Possibly the less onerous Canadian notice and notice procedure is preferable than the US notice and takedown process the perspective of Internet intermediaries. (Berkeley Technology Law Journal, March 2, 2014).

3.9 Australian Safe Harbor Discussion

Australian's Copyright Act 1968 deals with the exclusive rights of copyright owners and infringement of those rights in separate provisions. In the case of works 'literary, dramatic, musical and artistic', the exclusive rights to do certain 'acts' are set forth in s 31(1) and include the exclusive right to reproduce the work , to publish it, to perform it in public, communicate it to the public, and adapt it. Separate and more limited, exclusive rights are conferred on sound recordings (s 85), films (s 86), broadcasts (s 87) and published editions (s 88). These rights are infringed by anyone 'who, not being the owner of the copyright, and without the license of the owner of the copyright, does in Australia or authorises the doing in Australia of, any act comprised in the copyright' (ss 36(1) and 101(1)). Australian copyright law therefore defines infringement of a copyright in two ways: directly, by the infringer, or indirectly, by authorising another party (the direct infringer) to commit the infringing act. (Pappalardo, 2014).

Australia's safe harbor regime is of limited force in today's emerging technology field. Safe harbors provisions only apply to commercial Internet Service Providers (ISPs) such as Telstra, iiNet and Optus and not to all providers of Internet services particularly search engines. In Australia IAPs which merely providing Internet access face little exposure for infringement by their subscribers even if they take no action to notify or educate infringing customers. Yet, web hosts, cloud computing platforms, online platforms supporting user-generated content, and search engines face risk of direct infringement through communication or reproduction initiated by their users (Weatherall, 2018). Compared to the broad protection offered by the United States and the European Union Australian has comparatively weaker protections in the statutory scheme. Yet, recently a large inequity was address with the passage of Copyright Amendment (Service Providers) Regulation amended Copyright Regulations to extends safe harbor protections to schools, universities, libraries, cultural institutions and technology platforms (Universities Australia, 2018).

A method of attacking infringers is by asserting the direct liability of intermediaries. This claim is established by pleading the doctrine of vicarious liability with employees or agents acting on behalf of principals. The authorization or permission to do the act in question can be implied from the surrounding circumstances as a question of fact drawing inference from the conduct of the defendant. For example in

Falcon v Famous Players Film Co Ltd., a person who had entered a hiring agreement with the proprietor of a picture theatre who hired out the their theatre to exhibit a film, was held to have authorized its exhibition. (Falcon v Famous Players Film Co, 1926). In Twentieth Century Fox Film Corporation and Another v Newzbin Ltd. the defendant operated a search website for the Usenet news system allowing users to locate copies of films online for downloading and was held to have infringed the copyright. Despite the fact defendant denied it promoted the downloading of unlawful content in fact the system was designed to search newsgroups promoting the downloading of illegitimate and unauthorised copies, and to provide its own equivalent of a web hyperlink to such files. A key requirement is some ability on the part of the alleged authorizer, to control or prevent the infringing act (Twentieth Century Fox Film Corporation v Newzbin Ltd., 2010).

Quite distinct from the liability for authorization is the possibility of liability arising as a joint tortfeasor in the acts of infringement committed by another party. This is closely related to what is termed under the law of the United States law as 'contributory infringement'. Mirroring a similar rationale found in patent infringement law in copyright infringement cases activities are actionable by principles of joint tortfeasorship: aiding, abetting, facilitating and inducing the commission of infringing acts. But these activities must be underpinned by a 'common design' with the direct infringer, ie that both parties are engaged in some common enterprise or are acting 'in concert' in committing the tort'. Advertising a product in such a way as to suggest that it can be used for infringing purposes will not be sufficient, in the absence of showing some common design between supplier and infringer to infringe (Thompson v Australian Capital Television Pty Ltd., 1996).

Internet providers were given a broader protection in *Roadshow v iiNet*. The court held that Internet access providers are not liable for authorising infringements by their customers engaged in using BitTorrent to download films and television shows. Plaintiff rightsholders presented evidence that BitTorrent sharing by ii Net customers violared copyright and ii Net of infringements. The notice included a demand that under ii Net's. By its Customer Relationship Agreement iiNet should terminate and customers engaged in illegal conduct. iiNet did nothing claiming that it had no obligation to act. The court held ii Net not liable, for two key reasons. First, iiNet provided neither the BitTorrent software nor content and only had limited and indirect power to prevent customer infringements via BitTorrent. Second, in the circumstances of that case, issuing warning notices to customers, suspending or terminating their accounts were not reasonable steps. The court observed that "[i]n general, in the absence of any positive steps that actively incite infringement, [ISPs] that provide Internet access (as opposed, for example, to hosting services) will not be liable for authorising copyright infringements committed by their subscribers (or those using their accounts)" (Roadshow Films Pty Ltd. v iiNet Ltd., 2011).

The issue of direct liability for infringement by intermediaries with emerging technology can be seen in National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd. The case was brought by the AFL, NRL and Telstra against Optus finding that Optus breached copyright law by showing live or pre-recorded free-to-air AFL and NRL games on its TV Now service. The issue was the direct liability of service providers engaged in commercial activity involving copying and communication of content online, as opposed to non- carriage service providers (as defined under Australian law which enjoy a statutorily created safe harbor. Optus created a cloud-based system to enable its mobile Internet customers to record (on Optus' servers using Optus developed and maintained software) and then watch free-to-air television. The court held that although Optus' automated copying system only responded to a user's command to make a copy, Optus was a joint maker of any resulting copies and thus afoul of copyright law (National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd., 2012).

The trend in Australian to target targeting aggregators and disseminators of infringing content is best illustrated in the case Pokémon Company International, Inc. v Redbubble Ltd. I the case, Pokémon Company International (Pokémon) won in their Federal Court pursuit of copyright infringement claims against Redbubble Ltd. the operator of an online marketplace for "print on demand" products based on artwork submitted by independent artists or designers. Redbubble is an online marketplace for "print on demand" products where users can upload artwork and can place orders for products, such as a T-shirts, to which the artwork is applied. These products are manufactured and then supplied to consumers by third parties fulfillers, not by Redbubble directly. Pokémon is the owner of copyrighted art work which was displayed on the

Redbubble site, by third parties, and Pokémon claimed this was a violation of its copyright. It alleged specifically that Redbubble had infringed its copyright by making the infringing works available on the Redbubble website and communicating them to the public and thus authorising the reproduction of the infringing works (Pokémon Company International, Inc. v Redbubble Ltd., 2017).

The court found that Redbubble hosted the website containing the infringing material, making the work available online, controlled the website content and made the arrangements with the artists for products that were ordered through the website. While those responsible for uploading the artworks were also involved, this did not obsolve Redbubble liable for communicating the relevant works to the public. Further due to correspondence from Pokémon, Redbubble was on notice of claim of infringement. Finally the court found that Redbubble authorised the infringement of copyright, as it had the ability to prevent the infringement. It was immaterial that the system including the website operated automatically as Redbubble had developed that system in the first place. Further, Redbubble had no automated software, such as using keywords for tags or descriptions of the work or efforts to block content. Redbubble considered using an automatic approach to remove possibly infringing conduct, did not on commercially considerations. Although prevailing Pokémon was limited in its recovery. The court upheld the demial of a pre-trial injunction and awarded only $1 in nominal damages (Pokémon Company International, Inc. v Redbubble Ltd., 2017).

3.10 The Change in Internet Use: The Rise of Applications

Hosting as originally defined is the storing of third-party information on an intermediaries' system. When many jurisdictions enacted safe harbors immunizing hosts from liability for copyright-infringing content on their systems, hosting services typically offered were by the same telecommunications companies that provided carriage services or by smaller companies that specialized in Web hosting. Quickly new classes of online intermediaries emerged which were much different from those services that existed when the original immunity laws were in the late 1990s, such as the EC Electronic Commerce Directive (ECD) and the US Digital Millennium Copyright Act (DMCA) were debated and then promulgated in the late 1990s. The various immunity provisions or safe harbors were in the main designed to address straightforward situations of transmission and hosting of 3rd party content.

Roughly 20 years after the Internet came into widespread use – from 1995 on - fundamental changes in the paradigm of how people use the Internet and who generates on-line content came about. Originally the Internet was the World Wide Web (epitomized by "www."). The Web used Hypertext Markup Language (HTML) or JAVA as a standard language for creating web pages. But an important change predating existing copyright laws is that the users of today have shifted away from open HTML content and use different software to create the substance of what is seen and used on the Internet of today. The driver of this change was the creation of the iPhone model of mobile computing and its mobile phone-based progeny which use application software. Having achieved great popularity these dedicated platforms are grounded in the use of application software or apps. A mobile application is designed to run on a mobile devices such as a smartphone or tablet (Anderson and Wolff, 2010). Beginning in 2008 App software was widely popularized by Apple Inc. with its App Store and Google and with its Android Market which was later renamed to Google Play (Pogue, 2009).

The decline of HTML data and rise of application data has changed how and what is used on the Internet. Now applications account for more of the Internet's traffic including peer-to-peer file transfers, Skype calls, online games, iTunes, and Netflix movie streaming. Whereas in 2000 the sites with the largest traffic included Ebay, AOL.com, Geocities.com, americangreetings.com today the most popular are Google, Youtube, Facebook, Baidu and the lone HTML site is Wikipedia (Gray, April 10, 2017).

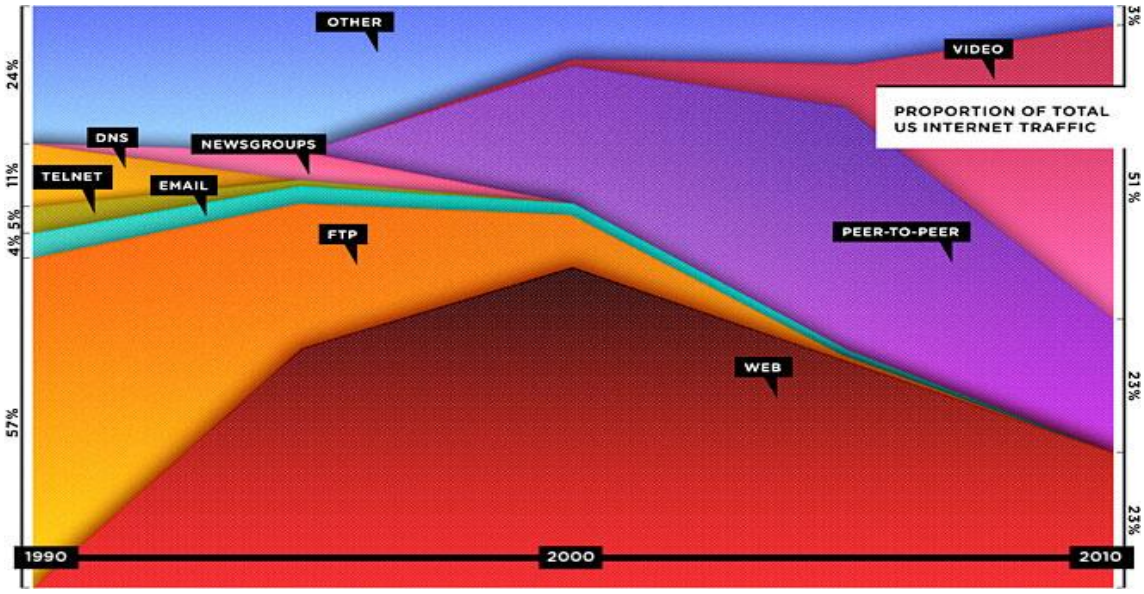

Figure 1: Increase in Web-based Applications (Anderson and Wolff, 2010, p 31)

The newer applications are most often closed, often proprietary, networks. For example both Apple and Android have restrictive guidelines for developers who which to write apps for the iOS and Android platform. Newer technologies such as Peer-to-peer (P2P) file sharing software programs, such as Napster and BitTorrent, video hosting such as Youtube, or Vimeo, commerce sites such as Ebay, Amazon or Craigslist, service sites such as AirbNb or Lyft, social media sites such as Facebook or Line plus payment systems such as Paypal and Bitcoin and all serve up a panoply of issues causing to bring in to question the viability of safe harbor laws.

Mobile operators are today in an almost monopolistic position as they "own" the mobile delivery channel as well as relationships with customers. Of course mobile platforms need to be innovative lest they end up like Internet service providers where technology, such as switching costs, has made barriers to entry low competition and advantage is often based only on price, while the cost of acquiring customers is high as few have developed a relationship with their customers. Mobile operators have sought to develop "walled garden" portals to force content creators to be controlled in the products produced and the interactions with end-customers. The value chain which is defined as creating profits through a linked chain of activities explains the "walled" aspect of mobile platforms. The digitization of both content and the value chain requires a fresh perspective that recognize the new relationships and the underlying power structures (Peppard & Rylander, 2006).

The supplier to the mobile delivery system is the application developer a key in the success of this model, as it fills the market with applications to be acquired. Fostered by low entry barriers to developers multiple profiles of application providers coexist, ranging from amateur developers to large enterprises. These actors provide applications, which are defined as native, installable pieces of software, developed using the platform APIs and guidelines, and provisioned through the market. IN theory the application store is an open market, where every competitor has equal chances to succeed. However, it must be noted that active markets are enormously competitive, with tens of thousands of competing applications. These factors greatly increase the importance of the functions related to discovery, marketing and recommendation of applications (often controlled by the mobile platform), as they play a fundamental role in application success (Cuadrado & Dueñas, 2012).

Take gaming for example. A prevalent myth is that the app economy and the vast number of mobile devices have radically changed the games industry from a simple dual relationship between dominate games studios to one where small companies or individuals can access app platforms and gain success. Rather, Apple's App Store is an example that demonstrates the increasing concentration of visibility and success by

a small segment of the developers offering games in the App Store. The challenge of network control and achieving attention by new entrants in a massive marketplace means that already dominant players are evident and at an obvious advantage. While there are still examples of small entrants achieving great success will be small as a result, 'the role of Apple in the value network is all encompassing and pervasive' (Nieborg, 2016).

3.11 Safe Harbor Takedowns are Too Broad

In the United States the 512 takedown process has incurred considerable disapproval for a variety of reasons. One critique is that the take down process was likely to impact and deter other permissible activities on the Internet such as the use of peer-to-peer networks which usually result in the termination of a the target's Internet access. Also, the take down process often does involve a clarity in legal issues, rather the alleged offendor's activity does not clearly fall into prohibited conduct which are not clear cut are simply. Urban and Quilter found that thirty percent of notices demanded takedown for claims that presented an obviously litigable question for example a clear fair use argument, or complaints about claims over uncopyrightable material. Often take down notices include statutory flaws that render the notice unusable, for example, failing to adequately identify infringing material. Also companies often engage in anticompetitive practices against competitor by using take down notices, for example over half of the notices sent to Google to demand removal of links were sent by businesses targeting apparent competitors (Urban and Quilter, 2005).

The safe harbor scheme in the United States seems to provide motivation for ISPs to replace wrongfully or mistakenly targeted material. Section 512(g) allows users to request replacement of material believed, in good faith, to have been removed or disabled as a result of mistake or misidentification of the material. If a third party content provider objects to the implementation of a takedown notice in a "counter notice" under Section 512(g) ISPs are required to notify targets that they will place the material back on-line unless the ISP receives notice that a legal action was filed. Specifically, the OSP must first notify the complainant that it will reinstate the content within ten business days after receipt of a counter notice; and then the OSP must "replace ... and cease disabling access" to the material within fourteen days after receipt of a counternotice. Also Section 512(f) provides a cause of action to users where the copyright owner knowingly makes material misrepresentations during the notice and takedown/putback process. This provision allows end-users to bring an action against those who knowingly misrepresent the infringment of a particular use. This provisions is designed to create liability for "knowingly false allegations to service providers in recognition that such misrepresentations are detrimental to rights holders, service providers, and Internet users." The reason for Section 512(f) was the protection of third parties whose material would be taken down. The law seems to place power back in the hands of content providers when in fact ISPs limit their liability with their terms of service. The actual result is that while the statute seeks to encourage put back by providing a safe harbor against liability for wrongful takedown, in practice ISP service contracts limit the legal or financial incentives for ISPs to do so (Urban and Quilter, 2005).

The practice of notice and takedown/putback procedures also disadvantage end-users in the incentives build into the law. Because the safe harbor shields an ISP from liability to a rightsholder, takedown notices incentivized ISPs to immediately take down content without any investigation. If they comply with a counter-takedown notice, the ISP has further disincentive to investigate a takedown notice because § 512(g) immunizes the ISP from liability to the end-user. All presumptions in the notice and takedown/putback procedure favor the copyright holder. The statutory scheme grants even greater protection to a copyright owner than the owner would have in court as in a trial a rightsholder would be required to show that the material is infringing their copyright. Under the takedown procedure the user's material is "assumed illegal on the bare say-so of the copyright holder (Pollack, 2006).

3.12 Takedown Enforcement is Too Punitive

Although Internet Intermediaries control the technical means for both preventing and facilitating infringement, all too often they find a profit in the encroachment on copyright monopoly of ownership through increased traffic that can be exploited commercially. But the risk in increasing the involvement of Internet intermediaries in copyright law enforcement involves the risk of creating a heavy economic burden and therefore of threatening the vitality of e-commerce. A European survey in 2015 showed that Internet

users "are most likely to have paid (either by subscription or per item) to access or download e-books (46%), followed by video games (34%), audio-visual content (30%), music (29%), and sports (19%)" (European Union, 2015). Larry Lessig has argued on the changing perceptions of the normative values of intellectual property and downloading observing that the widespread peer-to-peer and remix activities of young people need to be decriminalized; his argument is practical in that young people don't respect or abide by copyright law, therefore in some aspect copyright law should be changed (Lessig, 2008). As it can be reasonably assumed that a substantial proportion of free online content accessed by consumers constitutes copyright infringement. What follows is that both technically and realistically, the prosecution of a large proportion of the population is not a realistic strategy. Not only would the political cost be high as such enforcement measures would be highly unpopular, but also the legal system would be burdened of massive prosecutions. The intermediaries' safe harbor is justified in the concept that the burden of control should not be disproportionately borne by the private e-commerce sector, which should remain as unburdened by unregulated as possible to meet the needs of the consuming public and remain vigorous in the creation of new commercial models which benefit wider society. The copyright system is not unique in tolerating small scale infringements at the edges that do not, in aggregate, have a significant deleterious effect. An analogy is the parallels between copyright violations and speeding offences under driving laws. In both cases, violations are individual acts that increase individual utility but are believed in the aggregate to lower overall societal utility. Both involve individual acts that seem hard to detect. For that reason, each law has huge amounts of non-compliance. And, just as with speed limits, it may be that non-compliance with copyright law is widespread, but not severe (Hughes, 2010).

Consumers access the internet in new ways which have made the categories in section 512 obsolete in practice. Websites of today frequently use multiple methods to store and process data. For instance, many websites covered by section 512(c) 07 also use system caching as described in section 512(b)108 to improve run times and to allow content to load faster. The DMCA requires that websites using multiple categories of services enumerated in the statute must comply with each category's specifications. These conflicting obligations makes it problematic for websites to follow the DMCA's complex safe harbor provisions. Moreover, the DMCA's limiting categories fail to include some sites that engage in the most blatant forms of copyright infringement, including peer-to-peer ("P2P") hosting services. (Asp, 2018)

The breadth of safe harbor protections can reach potentially unexpected quarters. In the recent decision Sony v McFadden the European Court of Justice held that providers of open Wi-Fi are not liable for copyright violations committed by others, but can be ordered to prevent further infringements by restricting access to only registered users with passwords. In Sony v McFadden a German shopkeeper's free, open, wireless network was allegedly used to infringe copyright. McFadden (a member of Germany's Pirate Party) received a demand from Sony Music after a user shared music from his network. McFadden argued he was a service provider under the national implementation of the E-Commerce Directive and a 'mere conduit' for his users' traffic shielding him from direct liability for his users' copyright violations. The court rejected this argument and found liability on a German principle of Störerhaftung - a type of vicarious liability attaching to any party in a position to 'terminate or prevent' the infringements. Germany's Federal Supreme Court in 2010 held that the private operator of a wireless network can be required to use password protection in order to prevent abuse by third parties. In ruling that freedom of information is not prejudiced by an injunction which orders the provider to password protect network access as a means to identify intellectual property infringements the European Court of Justice balanced the fundamental rights under the European Charter against the right of freedom of expression. (Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, 2016).

3.13 Takedown Trolling Punishes Content Providers

Takedown notice trolling is another recent phenomenon which abuses the protections of safe harbor for ISPs as illustrated in the US case of BMG v Cox Communications. BMG is a music rights management corporation (a company which collects music royalties for rightsholders) who employed Rightscorp to enforce its music catalog copyrights on the Intenet. Rightscorp would send takedown requests to ISPs, with a settlement offer hoping that the ISPs would pass those notices on to subscribers accused of infringing. In many cases Rightscorp flooded on-line intermediaries with numerous take down requests. Cox

Communications refused to pass on the settlement letters. Cox does have a method to process claims of infringement as copyright owners are able to log one complaint per subscriber per day, and Cox considers terminating a subscriber's access after the thirteenth notice of alleged violation, subsequent to a series of escalating responses. Cox never automatically terminates a subscriber. Cox claimed the ISP had violated the safe harbor provisions, specifically the complaint alleged that the Internet service provider contributory liable for infringement of BMG's copyright catalog by Cox's subscribers. The case considered two questions in the ongoing battle over digital piracy: first what responsibility do providers have to police the infringing activities of their subscribers for safe harbor protection, and second, is negligence alone sufficient to prove contributory copyright infringement? (Brown, 2018).

The court denied Cox's safe harbor defense reasoning that although it was clear that the ISP had implemented a system to process copyright complaints, the facts indicated that Cox seemed to have no intention of implementing a repeat infringer policy. The court found that the company had failed to implement its own policy "in any consistent or meaningful way." Cox's hesitance to terminate service to alleged infringers and repeated re-activation of their accounts suggested that the company was more concerned with retaining paying subscribers than policing infringement (BMG v. Cox, 2018).

3.14 Takedown Requests Continue to Proliferate

When Google acquired YouTube in 2006 major media companies, particularly film studios and record labels, asserted that the platform facilitated widespread copyright infringement and called for a legislative response, despite the fact media rightsholders agreed in 1998 to safe harbor rules. In response to commercial pressure from content industries, Google developed Content ID, a system for proactive filtering (in Internet vernacular "bots") that often lets rights holders remove allegedly infringing content without even having to send a DMCA takedown request. Content ID allows rightsholders to submit large databases and YouTube scrutinizes new uploads for potentially matching content. Rights holders can choose to have YouTube automatically remove or they can review the content and decide the contents place in YouTube with the eye to monetize the videos. On balance to protect innocent third party uses of content there is an appeals process. Content ID changed YouTube and obtained the company the support of big content owners, many of which have forged lucrative commercial deals with YouTube (Tassi, Dec 19, 2013).

According to the researchers Urban, Karaganis, and Schofield in their review of more than 108 million of Google's web search takedown requests, more than 28%, were found to be "questionable." Nearly a third of takedown requests (28.4%) raised clear questions about their validity, while some had multiple potential issues. Among the "questionable" takedown requests are those that target websites that have been shut down calling into question the checks done to keep automated algorithms accurate. Other questionable notices were improperly formatted, included a subject matter inappropriate for DMCA takedown, or had potential fair use issues. The result of the high number of "questionable" takedown notices is that Google likely removes more content than it should. As the company currently acts in response to 97.5% of the takedown requests, the vast majority of the questionable notices are honored. Given the risk of high statutory penalties if a service rejects a valid notice, most if not all Internet intermediaries err on the side of takedown, categorically taking down 100% of the requests they receive (Urban et al., March 22, 2017).

The number of URL copyright removal requests sent to Google continues to climb at a rapid rate. During the week of November 19, 2014 Google received 15,659,212 URL takedown requests based on copyright infringement averaging 2.2 million requests per day. In November 2015 Google received 65,122,023 million URL copyright removal requests for 72,207 specified domains from 5,492 copyright owners.

Figure 2: Rise in Google takedown requests
Note: Google takedown requests grew 75 percent between 2013 and 2014. (Gesenhues, November 23, 2015).

The music industry in the United States claims takedown notices are not suppressing infringement, particularly focusing on search engines such as Google. Despite hundreds of millions of takedown notices to Google, rightsholders claim copyright infringing material is still topping many search results. Advocating a "notice and stay down" approach music groups are calling for advanced technologies to ensure that infringing content does not reappear once it's removed. The concepts includes audio fingerprinting technologies, hash-matching technologies, meta-data correlations and the removal of links that point to content which has been taken down already. Also safe harbor provisions are being targeted in that they profit from copyright infringement (RIAA Music Notes Blog, March 31, 2016).

3.15 The European Union Moves in the Wrong Direction

At the time of this article's publication the European Parliament is deliberating on a law that would force platforms like Google and Facebook to introduce automated upload filters to block copyright-protected content from being illegally posted online. The directive seeks to find a balance between the fee received by authors and performers and the profits made by Internet platforms when they make rightsholder's works accessible. This difference has been called "the value gap". The proposed change targets online service providers who offer access to a large amount of copyright-protected content uploaded by users, as these platforms organize, index, categorize, and promote content for profit. Internet access providers, cloud services businesses that upload content for their own use, or online marketplaces that do not give access to copyright protected content as a business model. non-for-profit websites, scientific or educational repositories, or open source software developing platforms are not included in the proposal. (Council of the European Union, March 25, 2018)

The proposal aims to address a longstanding objection by rightsholders that certain large intermediaries do not pay equitable value for content industry posted on platforms. (Danbury, 2016). The proposal has received wide support from rightsholders, for example Paul McCartney, James Blunt, Placido Domingo and more than 1,300 recording artists signed an open letter to the European Parliament in support of the new copyright law (Roxborough, July 4, 2018).

The EU proposal also aims to change the legal framework for the online use of news, by creating a new exclusive right for press publishers as Recital 31 of the new law states "[a] free and pluralist press is essential to ensure quality journalism and citizens' access to information". The subject matter is defined very broadly, covering professional publications, blogs and websites with the intention to make aggregators, search engines and social media pay to publishers for news posted on their platforms (Danbury, 2016).

A common objection to the proposed rules is they are universally applicable and EU-wide laws where rightsholders (both media groups and news organizations) are seeking to gain more of the profit from their copyrights. The fear is that free expression in society and smaller on-line startups will suffer harming the vitality of the commercial marketplace to the detriment of consumers. While intending to govern only licensed content, the proposed regulations target all types of content and all platforms regardless of licenses

or copyright infringement activities. The proposal aims to address a grievance by rightsholders that certain large platforms do not pay enough for content. The desire is to force intermediaries into licensing agreements. Yet small platforms and innovative startups that do not have the market power and resource to negotiate possibly thousands of licensing agreements will suffer (Koschwitz, November 21, 2017).

Filtering itself is technically ineffective and in practice comparatively expensive. Filtering is effective with some types of content, and ineffective with others. Audio files are comparatively straightforward in recognizing infringing content and systems can block text and links, more technologically complex filtering technology will raise the cost of launching commercially beneficial startups in Europe. Crowdfunding platforms 3D printing marketplaces, or e-commerce site all present different infringement issues and would need to develop different types of filtering systems. Even if filtering were to work properly across all formats, it would price many innovative ideas out of the European market (Engstrom & Feamster, March 2017).

3.16 The Lost Voice: Consumers

Currently, the notice and takedown‖ provisions of safe harbor regimes favors copyright holders and internet service providers over end-users. An Internet user may provide a counter-notice to the ISP if he believes a provider mistakenly removed or disabled access to his work. 17 U.S.C. § 512(g)(3). Whether copyright infringement actually occurred or not, the law imposes a mandatory ten-day waiting period on an service provider before restoring access 17 U.S.C. § 512(g)(2) C). Critics argue that this creates - impermissible restrictions on free speech by effectively granting temporary restraining orders prior to any determination by a court (Blom, 2009).

The current notice and takedown system significantly obstructs a consumer's ability to contest an unjustified takedown. Consider Reddit a social news aggregation website. Registered members submit content to the site such as links, text posts, and images, which are then voted up or down by other members. (Nicol, July 19, 2018). In 2016, Reddit received approximately 3294 copyright removal requests. Reddit was required to remove content in response to 610 requests, 19% of the total. Yet, no counter notices were received from any users and as such no content was required to be restored. The same was true in 2015. In practice consumers do not seem to understand the ability to challenge takedown requests in a meaningful way (Reddit, n.d.).

Another common appraisal against the notice and takedown procedures is about incentives. Internet intermediaries have no incentive to authenticate the authenticity of any notices for take down receive. The prudent course of action given the potential liability is to respond by treating all complaints of infringements as actual infringements. This is particularly true of there is not subscription relationship between search engines and alleged infringers. The search engines would be more likely than other types of service providers to take down any allegedly infringing content. As search engines generally have no subscribers, there is rarely an economic incentive for a search engine to remove purportedly infringing links. (Blom, 2009)

Although notifying consumers of a content takedown is a part of the process, the statute describing the US procedure is imprecise. As it is written, section 512(g)(2)(A) merely requires ISPs to "take[] reasonable steps [to] promptly . . . notify the subscriber that it has removed or disabled access to the material." Although there have been many cases addressing the notice required to initiate a proper takedown notice, there has been a notable absence of cases that discuss what ISPs are required to tell consumers. This lack of clarification creates a wide range of notifications a consumer can receive if his or her content is taken down. Consumers can be denied information about who is bringing a claim and what specifically about their content was infringing, and what they can do to assert their rights. This denial of basic information makes it very difficult for consumers to know what process is available to challenge an unfair takedown (Asp, 2018).

4. Conclusion

Internet intermediaries provide an infrastructure that allows people to create and share information free from the threat of claims for infringement on the Internet a greater balance between the interests of the parties involved must be found. The number of actors who are protected by safe harbors, the technology that creates these new intermediaries and the novel commercial uses continues to grow in way that are unimaginable when the original safe harbor laws were passed. In order to increase the space for innovations,

existing or not yet conceivable, safe harbors should be given an expansive reading to avoid unintended consequences which can restrict the inventive characteristics of the Internet which benefit third party contributors, intermediaries and rightsholders. The current system of internet safe harbors laws are in need of an update. The users of internet services are the largest group impacted by current policy, yet they receive little consideration in the drafting of safe harbor rules. Takedown activities under safe harbor laws have proliferated, yet the evidence seems that it is overly broad. The latest European Union proposals greatly expand the entitlements of copyright holders while placing great demands on internet intermediaries that could stifle the creativity that has driven innovations on the internet. The normative values of intellectual property need to be shifted with more emphasis placed on consumers versus rightsholders. Also, intermediaries need additional space to develop novel innovation that benefits not only rightsholders, but the providers and consumers of internet commerce.

5. References

A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (2001)

Allweiss, D. (1999). Copyright Infringement on the Internet: Can the Wild, Wild West Be Tamed? *Touro Law Review, 15*(3), Article 9. Retrieved from http://digitalcommons.tourolaw.edu/lawreview/vol15/iss3/9

Anderson, C, Wolff W., (2010, August 17) The Web is Dead Long Live the Internet. *Wired*. Retrieved from https://www.wired.com/2010/08/ff-webrip

Asp, E. Section 512 of the Digital Millennium Copyright Act: User Experience and User Frustration. *Iowa Law Review, 103*(2), 751-783. Retrieved from https://ilr.law.uiowa.edu/print/volume-103-issue-2/section-512-of-the-digital-millennium-copyright-act-user-experience-and-user-frustration/

Baistrocchi, P. (2003). Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce. *The Santa Clara High Technology Law Journal, 19*(1). Retrieved from http://digitalcommons.law.scu.edu/chtlj/vol19/iss1/3

Bell Atl. Corp. v. Twombly, 550 U.S. 544, (2007).

Berkeley Technology Law Journal (2014, March 2) Canada's Approach to Intermediary Liability for Copyright Infringement: the Notice and Notice Procedure, (BTLJ Blog Post) Retrieved from http://btlj.org/2014/03/canadas-approach-to-intermediary-liability-for-copyright-infringement-the-notice-and-notice-procedure/

Blom, A. (2009). Search Engines and § 512(D) OF THE D.M.C.A. *Case Western Reserve Journal of Law, Technology & the Internet, 1*(1).

BMG v. Cox, Nos. 16-1972, (4th Cir. Feb. 1, 2018).

Bramble, N. (2013). Safe Harbors and the National Information Infrastructure, *Hastings Law Journal, 64*, 325-342.

Brown, O. Ed by Doug Stephens D. (2018, Feb 21) BMG v. Cox: Court of Appeals Denies DMCA Safe Harbor in Landmark Copyright Case, (Jolt Digest Blog Post) Retrieved from https://jolt.law.harvard.edu/digest/bmg-v-cox-court-of-appeals-denies-dmca-safe-harbor-in-landmark-copyright-case

Council of the European Union. (2018, March 25). *Copyright rules for the digital environment: Council agrees its position* [Press Release] Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2018/05/25/copyright-rules-for-the-digital-environment-council-agrees-its-position/

Cuadrado, F., & Dueñas, J. (2012). Mobile application stores: success factors, existing approaches, and future developments. *IEEE ASSP Magazine Communications Magazine, 50*(11), 160-167.

Danbury, R. (2016). Is an EU Publishers' Right a Good Idea?, Centre for Intellectual Property and Information Law Cambridge University, 1-83. Retrieved from https://www.cipil.law.cam.ac.uk/projectscopyright-and-news-research-project-2014-16/working-papers

De Beer, J., & Clemmer, C. (2009). Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?, *Jurimetrics Journal, 49*(4), 375-409.

Elkin-Koren, N., & Salzberg, E. (1999). Law and Economics in Cyberspace. *International Review of Law and Economics, 19*(4), 553–581.
Ellison v. Robertson, 189 F.Supp.2d 1051(C.D.Cal. 2002).
Engstrom, E., & Feamster, N. (2017). The Limits of Filtering A Look at the Functionality and Shortcomings of Content Detection Tools. Retrieved from http://www.engine.is/events/category/the-limits-of-filtering-a-look-at-the-functionality-shortcomings-of-content-detection-tools
European Union. (2015). Cross Border Access to Online Technology. https://doi.org/10.2759/353931
Falcon v Famous Players Film Co, 2 KB 474 (1926).
Fletcher, N. (2018, June 29). Faang-tastic five: can US tech giants continue their stellar rise? *Guardian.* Retrieved from https://www.theguardian.com/business/2018/jun/29/faanga-us-tech-giants-facebook-amazon-apple-netflix-google
Fischer, S. (2014). Challenges of the Internet of Services, In W. Wahlster et al. (Eds.), *Towards the Internet of Services: The THESEUS Research Program.* Cognitive Technologies. Springer (pp. 15-27). https://doi.org/10.1007/978-3-319-06755-1_2
Garner, Bryan, Black, Henry Campbell, (2009) *Black's Law Dictionary* 9th Ed St. Paul, MN:West p. 4162.
Gasser, U., & Schulz, W. (2015, February 18). Governance of Online Intermediaries: Observations from a Series of National Case Studies. Berkman Center Research Publication No. 2015-5. http://dx.doi.org/10.2139/ssrn.2566364
Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2nd Cir. 1971).
Gesenhues, A. (2015, November 23). Google Received More Than 65 Million URL Takedown Requests In The Past Month. Retrieved from https://searchengineland.com/google-received-more-than-65-million-url-takedown-requests-in-the-past-month-236763
Gray, A. (2017, April 10). These are the world's most popular websites. *World Economic Forum*. Retrieved from https://www.weforum.org/agenda/2017/04/most-popular-websites-google-youtube-baidu/)
House of Representatives Reports, *United States Congress*, (1998) No. 105-551 (II), 20 -49. Retrieved from https://www.congress.gov/105/crpt/hrpt551/CRPT-105hrpt551-pt2.pdf
Hughes, J. (1988). The Philosophy of Intellectual Property. *Georgetown Law Journal, 77*, 287–366.
Hughes, J. (2011, December 30). How (Dis) respected is Copyright Law?, Retrieved from http://www.mediainstitute.org/IPI/2011/121311.php
In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003).
Imfeld, C., & Ekstrand, V.S. (2005). The Music Industry and the Legislative Development of the Digital Millennium Copyright Act's Online Service Provider Provision. *Communication Law and Policy, 10*(3), 291-312. https://doi.org/10.1207/s15326926clp1003_2
Kennedy, J. (2005, November 25). How digital disruption changed 8 industries forever, *Silicon Republic*. Retrieved from https://www.siliconrepublic.com/companies/digital-disruption-changed-8-industries-forever
Koschwitz, L. (2017, November 21). Filtering Obligations: Don't torpedo startups in Europe, *The Digital Post*. Retrieved from http://www.thedigitalpost.eu/2017/channel-startup-economy/filtering-obligations-dont-torpedo-startups-in-europe
Landes W., & Posner, R. (1989). An Economic Analysis of Copyright Law, *The Journal of Legal Studies, 18*(2), 325-363.
Leonard, P. (December, 2010). Building Safe Harbours in Choppy Waters- Towards a Sensible Approach to Liability of Internet Intermediaries in Australia, *Communications Law Bulletin, 29*(3), 10-23. Retrieved from http://classic.austlii.edu.au/au/journals/CommsLawB/2010/18.html
Lessig, L. (2008). *Remix: Making Art and Commerce Thrive in the Hybrid Economy*, New York: Penguin Press
Lilian, E. (2010). Role and Responsibility of Internet Intermediaries in the Field of Copyright and related Rights, *World Intellectual Property Organization Publication* [Online] Retrieved from http://www.wipo.int/publications/en/details.jsp?id
L'Oreal SA and Others v. eBay International AG and Others C-324/09 139 (2011).
Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd. FCAFC, *59* (2012).
Nicol, W. (2018). What is Reddit? A Beginner's Guide to the Front Page of the Internet Digital Trends Retrieved from https://www.digitaltrends.com/social media/what-is-reddit/
Nieborg, D. (2016). From premium to freemium: The political economy of the app. In T. Leaver & M. Willson (Eds.), *Social, Casual and Mobile Games: The Changing Gaming Landscape* (pp.225-240). London and New York: Bloomsbury Academic
OECD. (2011). The Role of Internet Intermediaries in Advancing Public Policy Objectives, *OECD Publishing* [Online] Retrieved from htttp://www.oecd.org/sti/ieconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm
Olazabal, A. M. (2011). False Forward-Looking Statements and the PSLRA's Safe Harbor. *Indiana Law Journal*, *86*(2), 595-644. Retrieved from http://www.repository.law.indiana.edu/ilj/vol86/iss2/5
Peppard, J., & Rylander, A. (2006). From Value Chain to Value Network: Insights for Mobile Operators. *European Management Journal*, *24*(2), 128-141.
Pappalardo, K. (2014). Duty and Control in Intermediary Copyright Liability: An Australian Perspective, *IP Theory*, *4*(1). Retrieved from http://www.repository.law.indiana.edu/ipt/vol4/iss1/2
Peguera, M. (2009, September 4). The DMCA Safe Harbors and Their European Counterparts: a Comparative Analysis of Some Common Problems. *Columbia Journal of Law and Arts, 32*, 481- 488.
Perfect 10 v. Visa International, 494 F.3d 788 (9th Cir. 2007).
Perset, K. (2010). The Economic and Social Role of Online intermediaries (2010). *OECD Directorate for Science Technology and Industry* [Online] Retrieved from http://www.oecd.org/Internet/ieconomy/44949023.pdf
Playboy Enterprises, Inc. v. Frena (1993) 839 F. Supp. 1552.
Pogue, D. (2009). A Place to Put Your Apps, *New York Times* Page B https://www.nytimes.com/2009/11/05/technology/personaltech/05pogue.html
Pokémon Company International, Inc. v Redbubble Ltd. [2017] FCA 1541.
Pollack, M. (2006). Rebalancing Section 512 to Protect Fair Users from Herds of Mice-Trampling Elephants, or A Little Due Process Is Not Such a Dangerous Thing, *Santa Clara Computer and High Technology Law Journal*, *22*(3), 547.
Reddit Inc. (2016) Transparency Report (n.d.) Retrieved from https://www.reddit.com/wiki/transparency/2016
Religious Technology Center v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).
RIAA. (2016, March 31). 400 Artists, Songwriters, Managers, and Music Organizations Call For Reforms of Broken DMCA Recording Industry Association of America® (RIAA Blog Post) Retrieved from https://www.riaa.com/400-artists-songwriters-managers-and-music-organizations-call-for-reforms-of-broken-dmca/
Roadshow Films Pty Ltd. v iiNet Ltd. 89 IPR 1 (2011).
Roxborough, S. (2018, July 4). Paul McCartney, James Blunt Back New European Copyright Law. *The Hollywood Reporter.* Retrieved from https://www.hollywoodreporter.com/news/paul-mccartney-james-blunt-back-new-european-copyright-law-1124974.
Sag, M. (2018). Internet Safe Harbors and the Transformation of Copyright Law. *Notre Dame Law Review, 93*(2), 499-564.
Sega Enterprises Ltd. v. MAPHIA, 857 F. Supp. 679, 686 (N.D. Cal. 1994).
Slovin, M., Sushka M., & Polonchek, J. (1990). Corporate Sale-and-Leasebacks and Shareholder Wealth. *The Journal of Finance*, *45*(1), 289-299.
Society of Composers, Authors and Music Publishers of Canada v Canadian Assn of Internet Providers, 2 S.C.R. 427 (2004).
Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984).

Stempel, J. (2014, March 18). Google, Viacom settle landmark YouTube lawsuit. *Reuters.* Retrieved from https://www.reuters.com/article/us-google-viacom-lawsuit/google-viacom-settle-landmark-youtube-lawsuit-idUSBREA2H11220140318

Tassi, P. (2013, Dec 19) The Injustice of The YouTube Content ID Crackdown Reveals Google's Dark Side. *Forbes.* Retrieved from https://www.forbes.com/sites/insertcoin/2013/12/19/the-injustice-of-the-youtube-content-id-crackdown-reveals-googles-dark-side/#68d90e0f66c8

Tarleton, G. (2004). Copyright and Commerce: The DMCA, Trusted Systems, and the Stabilization of Distribution. *The Information Society*, 20(4), 239-254. https://doi.org/10.1080/01972240490480938

Telecommunications Act of 1996, Pub. LA. No. 104-104, 110 Stat. 56 (1996).

Thompson v Australian Capital Television Pty Ltd. 169 CLR 574 (1996).

Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, Case C-484/14 (2016).

Twentieth Century Fox Film Corporation v Newzbin Ltd. EWHC 608 (2010).

Urban, J., Karaganis, J., & Schofield, B. (2017). Notice and Takedown in Everyday Practice. UC Berkeley Public Law Research Paper No. 2755628. Accessed at: http://dx.doi.org/10.2139/ssrn.2755628

Urban, J, & Quilter, L. (2005). Efficient Process or Chilling Effects - Takedown Notices under Section 512 of the Digital Millennium Copyright Act. *Santa Clara High Technology Law Journal, 22*(4), 621-694.

Universal City Studios, Inc v Sony Corp 480 F Supp 429 pp. 457-58 (CD Cal 1979).

Universities Australia. (2018). New copyright safe harbour changes to protect universities [Press Release] Retrieved from https://www.universitiesaustralia.edu.au/Media-and-Events/media-releases/new-copyright-safe-harbour-changes-to-protect-universities#.W9WHrHszbIU

UConn Library. (n.d.). University of Conneticut (n.d.). Retrieved from https://lib.uconn.edu/about/policies/copyright/what-is-copyright/#

van der Sloot, B. (2015). Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, *6*(3), 211-228.

Viacom Int'l Inc. v. YouTube, Inc., No 1:07-cv-02103-LLS (S.D.N.Y. Apr. 18, 2013).

Weatherall, K. (2018, February 11). Internet Intermediaries and Copyright: A 2018 Update. *Australian Digital Alliance*. Retrieved from https://www.aph.gov.au/DocumentStore.ashx?id=79110429-08ee-4b3b-8219-85071c8c0cee&subId=563534