COMPARATIVE ANALYSIS OF COPYRIGHT ENFORCEMENT IN THE CLOUD UNDER U.S AND CANADIAN LAW: THE LIABILITY OF INTERNET INTERMEDIARIES

BY

DAVID BENSELEM

A thesis submitted in conformity with the requirements for the Master degree (LLM) Faculty of Law University of Toronto

© Copyright by David BENSELEM (2012)
Abstract

Through an empirical comparison between U.S and Canadian copyright law, this paper examines how lawmakers in both countries should deal with copyright liability issues in the cloud while maintaining a proper balance between content owners and Internet intermediaries. This paper proposes to answer this question throughout the study of the liability of Internet intermediaries. Drawing on copyright statutory provisions, case law and scholars articles, this paper examines the issue of online piracy, defines cloud computing and identifies the copyright liability issues posed by the cloud. It then compares U.S and Canadian copyright laws and discusses the new reform proposed in both countries in relation with the liability of Internet intermediaries. It concludes that new statutory reform might not be necessary except for clarification purposes. Indeed current copyright laws deal efficiently with copyright liability issues in the cloud while maintaining a proper balance between content owners and Internet intermediaries.
Acknowledgment

This paper would not have been possible without the support of many people. The author wishes to express his gratitude to his supervisor, Prof. Ariel Katz who was abundantly helpful and offered unique assistance, help and assistance.

The author would also like to convey thanks to the University of Toronto, Faculty of Law for providing the financial means and facilities.

Finally, The author wishes to express his gratitude to Julia Hall, Sahar Gh, Daniele Bertolini, W. & K. Blagui and to his beloved families especially S. Boussen; for their kindness & endless love, through the duration of his studies.
COMPARATIVE ANALYSIS OF COPYRIGHT ENFORCEMENT IN THE CLOUD UNDER U.S AND CANADIAN LAW: THE LIABILITY OF INTERNET INTERMEDIARIES

PRELIMINARY SECTION

A. IS THERE A PROBLEM OF PIRACY IN THE DIGITAL AGE? 3
   1. PIRACY AS A FORM OF SAMPLING 4
   2. PIRACY MAY HAVE A NETWORK EFFECT 4
   3. PIRACY MAY HELP LOCKING CUSTOMERS IN 5
   4. THE NEGATIVE ELEMENTS OF “PIRACY” ARE NOT UNDENIABLE 6

DEFINITION OF CLOUD COMPUTING AND INTERNET INTERMEDIARIES 7

A. DEFINITION OF THE CLOUD 7
   1. NSIT DEFINITION 7
   2. CLOUD COMPUTING FEATURES 7
B. CLOUD COMPUTING DEPLOYMENT MODELS 10
C. THE DIFFERENCE BETWEEN INTERNET AND THE CLOUD 12
D. ISSUE OF COPYRIGHT ENFORCEMENT IN THE CLOUD AND THE LIABILITY OF THE INTERNET INTERMEDIARIES 13

COMPARISON BETWEEN U.S AND CANADIAN COPYRIGHT LAW REGARDING THE LIABILITY OF INTERNET INTERMEDIARIES 14

A. U.S COPYRIGHT LAW REGARDING THE LIABILITY OF INTERNET INTERMEDIARIES 15
   1. STATUTORY LIABILITY: A GENERAL OVERVIEW OF THE LIABILITY OF INTERNET INTERMEDIARIES: THE SAFE HARBOR SHIELD 15
      a. Overview of the secondary liability doctrine under U.S law 15
      Vicarious liability 16
      Contributory infringement 16
      b. The Digital Millenium Copyright Act (DMCA) 17
      ISP’s Safe Harbor 18
      Caching provider Safe Harbor 18
      Hosting and UGC providers Safe Harbor 18
      Search Engines and linking providers Safe Harbor 18
   2. FAIR USE HARBORS 21
      a. Statutory provision 21
      b. Application of the fair use doctrine by U.S courts 24
   3. HOW COPYRIGHT CASES AFFECTING THE LIABILITY OF CLOUD PROVIDERS HAVE BEEN ADDRESSED BY U.S COURTS 27
      a. MAI Systems Corp. v. Peak Computer Inc.: the identification of copyright in the cloud 27
      b. Cartoon Network v. Cablevision: The existence of copyright infringement in the context of digital video recorders 29
      c. The Capitol Records Inc. v. MP3tunes, LLC case 32
B. CANADIAN COPYRIGHT LAW REGARDING THE LIABILITY OF INTERNET INTERMEDIARIES 36
1. **General Overview of the Secondary Liability of Internet Intermediaries under Canadian Law**
   a. Liability of ISP, Hosting Providers and Referral Services 42
   b. Liability of ISP under current Canadian Copyright law: the statutory “Common Carrier” exception explained by the courts 42
   c. The judicial safe harbor granted to hosting providers 43
   d. The existence of a judicial safe harbor granted to referral services 45
   e. Crookes v. Newton: hyperlinks are content neutral 45

2. **Fair Dealing under Canadian Law**
   a. Fair dealing under Canadian doctrine 49
   b. Application of the doctrine of fair dealing by the Supreme Court of Canada 50

SOPA and Bill C-11: The Solution to Address the Liability of Internet Intermediaries While Maintaining a Balanced Copyright Law? 55

A. The Impact of SOPA on the Liability of Internet Intermediaries 55
   1. Overview of SOPA 55
   2. Impact of SOPA and PIPA on Cloud Intermediaries 56
   3. Impact of SOPA/PIPA on Internet Intermediaries: A Bill that Will Chill Innovation by Weakening Safe Harbors Protections 57

B. The Effects of Bill C-11 on the Liability of Internet Intermediaries 59
   1. Bill C-11 Confirmed the Safe Harbors Recognized by Case Law 59
   2. The Redundancy of the User Generated Content Provision? 64
   3. The Enablement Right Do Not Target Internet Intermediaries 65
   4. The “Notice and Notice” Regime v. The “Notice and Take Down” Regime 68
      a. Overview of the “Notice and Notice” Regime 68
      b. Is the Notice and Notice Regime Comparable to the Notice and Take Down Regime? 69

Conclusion 73

Bibliography 75
Today, when you use your computer, your telephone or your Ipad, you will probably use cloud computing (the “cloud”). The cloud is a generic word describing remote services or programs. Put it differently, the cloud is a fancy world to describe the new reality of the digital age that is services, contents and data that are not physically present on your local disk but somewhere in the cloud. Almost all computer and Internet users, use method of cloud computing in their day-to-day activities. To illustrate this point, the top five websites by visits, consist of two search engines/portals and three sites that can readily be considered examples of cloud computing: Facebook, the social networking site and number one website by traffic; Yahoo! Mail, the number one webmail provider by accounts; and YouTube. 

Comparatively, a user with no presence “in the cloud” would be severely limited as he will only be able to use software located on his own computer, use e-mail, that is hosted and operated on servers that he controls, and he would be abstained to use any interactive Internet sites, especially social networking sites. To sum up, nowadays, it’s pretty difficult to use Internet without using the cloud. Cloud computing is the prevailing business model.

With the growth of cloud computing, it became simple to exchange (upload or download) music, video, software or any other data. The main legal question in relation with this technological trend is whether the lawmaker is able to address the new copyright issues in the cloud?

Governments have been lobbied systematically by content industry to target Internet intermediaries, contending that Internet intermediaries are technologically

and commercially well positioned to assist with copyright enforcement. This raises a fundamental question as to whether copyright law shall impose liability on innovators of technologies used to copy, manipulate, disseminate or facilitate copyrighted content. As observed by Dotan Oliar, intellectual property is to promote both authorship and invention/innovation. Normally, these goals can be pursued independently, sometimes they may conflict. As the U.S Supreme Court noted, imposing copyright liability on technology companies would promote authorship but chill innovation, whereas immunizing technology companies from liability would stimulate innovation but chill authorship.

How should the lawmaker deal with copyright liability issues in the cloud while balancing these two interests? We propose in this essay to answer this question throughout the study of the liability of cloud/Internet intermediaries in U.S and Canada.

We will (Preliminary Section) first examine whether there is a problematic of online copyright piracy, i.e. to what extent the digitalization of many goods has increased piracy and what are the ultimate consequences of such phenomenon? (Section 1) We will then attempt to define the very notion of cloud computing and to identify the copyright issues posed by the cloud. (Section 2) We will also compare U.S and Canadian copyright law in order to consider how they balance authorship and innovation through the liability imposed to Internet intermediaries. (Section 3) Ultimately, we will consider whether statutory copyright reforms are necessary respectively in U.S and Canada.

---

5 MGM Studios Inc. v. Grokster Ltd, 545 U.S. 913, 928 (2005); Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984) (observing that the purpose of copyright law’s “staple article of commerce” doctrine is to “strike a balance between a copyright holder’s legitimate demand for effective—not merely symbolic—protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce”).
Before addressing the issue of copyright enforcement in the cloud we have to question whether there is a problem of online piracy.

A. IS THERE A PROBLEM OF PIRACY IN THE DIGITAL AGE?

Nowadays, it is commonly accepted that the Internet has made digital piracy of copyrighted works a serious global problem. The U.S. copyright industry claimed that piracy had cost billions of dollars in revenue while threatening the loss of hundreds of thousands of jobs worldwide. For instance, piracy is estimated to cost the U.S. and Canadian entertainment software industries more than $3.5 billion annually. 6 Besides, an Ipsos / Oxford Economics report released in 2011 by the Canadian Motion Picture Distributors Association (CMPDA) estimated that more than $1.8 billion and 12,600 full-time equivalent jobs were lost across the entire Canadian economy in 2009-10 as a result of movie piracy. 7

It is therefore no surprise that the copyright industries have been aggressively pursuing legal actions and lobbying for stronger protection throughout the world.

The reality seems to be more complex than the situation reported by the content industry for there are various cases where piracy may increase demand for a digital item. 8

---

6 The Entertainment Software Association of Canada (ESAC), Piracy, online ESAC <http://www.theesa.ca/?page_id=170>.
1. **Piracy as a form of sampling**

First, it has been claimed that piracy can be regarded as a form of sampling, and that sampling can encourage the diffusion of digital medias.\(^9\) The main argument is that digital products are experience products, which value cannot be reasonably measured without trying them. In the absence of legal samples, consumers may turn to pirated goods so as to assess whether they like it and eventually purchase it. It has also been argued that some publishers may have spread some music sample, considering that it would help them sell more digital goods.\(^10\)

2. **Piracy may have a network effect**

Piracy may have a positive effect on demand when there is a high network effect in a relevant market.\(^11\) For instance, network effects are especially strong in the software industry.\(^12\). Some scholars contend that, in the presence of network externalities (where the value a user derives depends on the size of the user base), the utility of the software increases with piracy because it increases the number of other individuals using it. The utility of product consumption increases with the total number of individuals using it.\(^13\) Using innovation diffusion models, they suggest that piracy provides word-of-mouth advertising for the software product and thus represents an efficient form of “sampling” that leads to a future purchase.\(^14\)

---


\(^11\) Supra note 1.


\(^13\) Supra note 8.

In a nutshell, these scholars argue that the value of owning a software increase with the numbers of other consumers owning the same software. Let’s take for example Microsoft Office. The possibility for consumer to exchange Word or Excel files with other consumers creates value to the product. The value of such product increases with the numbers of users in the Office network. This implies that if piracy increases the size of the network, it can increase the value of possessing a digital item, thus the demand for the legal item.

As mentioned by Ariel Katz, In the face of network effects that exist in many software markets, a “cross-sectional price discrimination”, in which the lower tier of customers 'purchases' illegal versions for a zero price, achieves the most expeditious and widest dissemination of software, maximizes the value of the network, and may also accelerate a tipping of the market in favor of the more dominant publisher. As a result, publishers are able to increase their profits compared to those earned in a smaller and less valuable network”. 15

Other studies have analyzed the impact of illegal download of music on legal sales of music. They concluded that, similarly to the software industry illegal file sharing creates network effect through word-of-mouth advertising for good songs, which increase sales. 16

3. Piracy may help locking customers in

Lock in to specific software or operative system is increased when the costs of swapping to a new technology are significant. Besides if the alternative software, operative system does not have an important pool of users, and if there is an absence of complementary products, this may inhibit any decision to switch to the alternative offer even if the alternative technology is technically better. This

15 Ibid. at 157.
supports that when a software, OS or other product is competing with another for standard of the industry, companies may be willing to tolerate or even bolster piracy, considering that it will enhance the network effects, induce switching costs and locking customers in.  

4. The negative elements of “piracy” are not undeniable

A recent study show that the fashion industry, which produces a significant variety of creative goods without strong copyright protection. Some scholars have suggested that the lack of intellectual property rights for fashion design has not quashed innovation, as the orthodox account would predict, and that it may have actually promoted it. These scholars question whether the positive effects of piracy in the fashion industry are present in other creative industries such as music and film.

Moreover, a recent study by a Swedish sociologist of law explains that the very conception of piracy as theft is problematic as the key element of stealing is that one stolen from loses the object, which is not the case of online piracy since the object is not taken from something but copied. The author also argues that one of the obvious problems is that every “stolen copy” is considered as a lost sale whereas people who downloaded illegally a file may not have ultimately bought it.

Recent studies have evaluated what the academic literatures can tell us about the impact of piracy on sales. This is outside of the scope of the present paper for we solely advocate that the negative consequences of online piracy are not that clear and are at least the subject of serious doubts. Again, this paper does not pretend to

---

19 Ibid. at 1776.
address this question but to stress that parliament should take into consideration this unclear situation in order to tackle the liability of Internet intermediaries in the cloud.

DEFINITION OF CLOUD COMPUTING AND INTERNET INTERMEDIARIES

A. DEFINITION OF THE CLOUD

1. NSIT definition

According to the National Institute of Science and Technology:

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployments models”.

Put it differently, cloud computing describes a global technological infrastructure in which the user of a computer can access and use data and software located in the cloud, that is, outside the user’s computer. 22

2. Cloud computing features

The National Institute of Standards and Technology (“NIST”) has developed a series of definitions. 23 These definitions, consisting of “five essential characteristics, three

---

service models, and four deployment models,” provide useful element to the present analyze. The “essential characteristics” defined by the NSIT are the following:

- **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as applications, server time and network storage, as needed automatically without requiring human interaction with each service’s provider.

- **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

- **Resource pooling.** The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

In the framework of the current analyze of copyright in the cloud, on-demand self-service and broad network access—are the most important.

---

**Self-service** characteristic raises a fundamental liability issue; i.e. whether the user or the system is committing and thereby liable for copyright infringement. As NIST defines it, the on-demand self-service characteristic means that, a "consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider". 24

The need for human monitoring, from the provider perspective, can play an important role in the analysis of provider liability. 25 While copyright act(s) are generally understood to be and are applied as a strict liability statute, U.S and Commonwealth courts have found a distinction in recent years where the defendant's system is automatically making the potentially infringing copies. The “self-service” characteristic of cloud computing speaks to this very question of volitional conduct.

As it will be discussed in the subsequent sections, 26 recent United States and Canadian case law suggests that copies created in the cloud by user will not normally transfer liability to the ISP, even where the system making the copies was created and is owned and maintained by an ISP.

Broad network access suggests the basis of the “issue” from copyright owners perspective. It is the characteristic that allows users to access and share their, or other users’, cloud-based files and systems from virtually anywhere, and from diverse client platforms, notably laptops, mobiles phones and personal digital assistants (PDA) thanks to broadband connections. This ability to access and distribute instantaneously content from anywhere and through different devices is a key issue of copyright enforcement in the cloud. Moreover, broad network access involves several parties in the transmission of the data, increasing the ISP’s and

---

24 Ibid.
25 Ibid.
26 Infra. section II.
other intermediaries’ responsibility for transmitting data, eventually creating automatic temporary copies as part of this transmission process. This again can raise the problem of Internet intermediaries’ liabilities with respect to copyright infringement.27

Resource pooling suggests the necessity for cloud service providers to monitor the use of resources. For instance when a user upload a photo or a video on Facebook, Facebook will not allocate a dedicated server to each user. These file are only allocated a specific amount of space available among the provider large pool of data storage, space. The cloud provider may control the allocation of the storage pool without any intervention of the end user who does not have knowledge about the physical resource he is using and where his data is stored.28

Rapid elasticity is *ipso facto* linked to resource pooling. While resource pooling has for result to exclude the user from knowing the resource used, rapid elasticity require that the cloud provider to scale up instantaneously to user request/need and to scale down just as fast to keep the maximum free space for other users.

**B. CLOUD COMPUTING DEPLOYMENT MODELS**

The NSIT also defines various deployment models.

Cloud computing refers to a set of approaches to diffuse computing power across more than one physical computer.29 These approaches are generally divided into

---

27 *Supra note 23.*


29 *Supra note 23.*
three services models, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

In SaaS, the cloud provider(s) controls most of the software stack. Figure 1 illustrates how control and management responsibilities are shared. In the center, the figure depicts a traditional software stack comprising layers for the hardware, operating system, middleware, and application. The figure also depicts an assignment of responsibility either to the cloud provider, the cloud subscriber, or both.  

SaaS is the most common model. The classical example is the web-based email, where the user/consumer is using the provider’s applications, servers, and infrastructure to send and receive emails but with almost no abilities to set up its own preferences. It’s a sort of bargain where the web mail provider is free but where the service offered is limited. Social networking sites, Facebook, LinkedIn, etc. are also SaaS. Taking into account the limited options offered to the U.Ser under this model, copyright owners may claim that SaaS providers have technically the ability to monitor their systems and thereby control infringing copyright contend uploaded/transmitted on their systems.

---


11
For the most part, the other deployment models are outside the scope of the present study. Basically the other platforms, that is, the Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) allow users to stack their software on the top of a cloud platform, providing the user more control over his information. In such service model configuration, PaaS and IaaS can counter copyright infringement liability by contending that they are not able to control every bite of data that crosses their servers. At the end of the day, these types of models are the exception and will not therefore be discussed further.

C. THE DIFFERENCE BETWEEN INTERNET AND THE CLOUD

In the early days of the Internet, for the most part, websites offered minimal interaction for the user; they were static, read only and unidirectional. Web 2.0 technology, changed the Internet realm as it offered users easy to use interfaces to contribute and generate content through interactive applications that operate on networks versus software that users used to install and use an their individual hard drive. Pre-cloud, Internet was mainly used to transport data from one computer to another computer. In comparison, with cloud computing, the user can upload and download data on external servers that the user does not own and does not know the exact location. The reason explaining the growth of cloud computing is the worldwide increase of Internet speed. In fact, the use of cloud storage is practical

31 Chatrooms, MUDs, MOOs, and Usenet groups were early exceptions, operating in text-only and DOS-based formats that required intermediate to advanced user skills to navigate.

32 “Web 2.0 is a concept that takes the network as a platform for information sharing, interoperability, user-centered design, and collaboration on the World Wide Web. A Web 2.0 site allows users to interact and collaborate with each other in a social media dialogue as creators (prosumers) of user-generated content in a virtual community, in contrast to websites where users (consumers) are limited to the passive viewing of content that was created for them. Examples of Web 2.0 include social networking sites, blogs, wikis, video sharing sites, hosted services, web applications, mashups and folksonomies”, Wikipedia, Web 2.0, online <http://en.wikipedia.org/wiki/Web_2.0>.


34 The Use of classical webmail requires solely Internet speed of 56Kbps whereas streaming services and video-on-demand as Netflix requires broadband connection. For instance Watching a single two hour movie could consume anything between 1.5GB to 5GB (GigaBytes) of data, ISP Review, UK Comparison of Broadband Movie Download and Web Streaming Services, (April 12, 2012) online:
only if the user Internet connection is sufficient to allow large amount of data transfer. At some point, the progression of Internet speed reached a threshold, marking Internet user’s ability to access services (storage, software, media streaming) as easily than using the same service on their computer. To sum up, the cloud can be described as the latest stage of the development of the Internet where users are offered more interaction capabilities.

D. ISSUE OF COPYRIGHT ENFORCEMENT IN THE CLOUD AND THE LIABILITY OF THE INTERNET INTERMEDIARIES

Following the growth of cloud services, and the lack of success of legal actions against end users and P2P providers, the music and other copyright right holders have turned to an indirect strategy consisting in seeking ISP’s cooperation or liability of Cloud/Internet intermediaries. Again, this paper does not pretend to address this issue but to stress that parliament should take into consideration this unclear situation in order to tackle the liability of Internet intermediaries in the cloud.

Nowadays, the content industry claims that infringing music, video, film and e-book is broadly available from cloud intermediaries. For instance a user may upload an infringing content on various user generated content as Youtube, Dailymotion etc. Infringing data/content is also widely available for download. These data are stored in cloud/hosting intermediaries’ servers. Furthermore, search Engines such as Google have become crucial actors. Contents aggregators became also an important

digital actor as they offer aggregate content from a variety of linked sites. The issue is that these aggregators can make a link to infringing content. In these examples, the intermediaries are not directly engaged in the infringing endeavor. However, rightholders will argue that they facilitate such infringing endeavor.

Ultimately, the question arising from the development of cloud computing is whether special duties should be imposed on and or immunities from liabilities removed concerning Internet intermediaries. We will analyze herein whether U.S and Canadian courts/lawmakers are struggling to balance rules establishing new liabilities for Internet intermediaries and recognizing in the same time the essential role that intermediaries play in the digital realm. Put it differently, we propose to analyze whether US and Canadian courts are struggling to maintain a tradeoff incentivizing authorship and incentivizing innovation through the analysis of the liability of Internet intermediaries.

We acknowledge that the present analysis has solely focused on this tradeoff whereas other actors such as end users may also be affected by the development of cloud computing. In the following section we will compare U.S and Canadian copyright law in order to determine how they are balancing authorship and innovation through the liability imposed to Internet intermediaries.

COMPARISON BETWEEN U.S AND CANADIAN COPYRIGHT LAW REGARDING THE LIABILITY OF INTERNET INTERMEDIARIES

One may legitimately question why we choose to compare U.S and Canadian copyright law. Actually, U.S is the pioneer in copyright enforcement as most of the big fifty cloud/internet companies are based in the U.S. In addition, U.S is the first commercial partner of Canada and U.S copyright law and new technologies

---

38 Supra note 4, section IV.A, pp. 1014.
companies have an incontestable influence in Canada. Finally both countries
drafted new copyright laws recently and the comparison between these laws may
help identifying the same issues faced by U.S and Canadian lawmaker in their
attempt to seek new liabilities to cloud providers.

A. U.S COPYRIGHT LAW REGARDING THE LIABILITY OF INTERNET
INTERMEDIARIES

1. Statutory Liability: a general overview of the Liability of Internet
intermediaries: the safe harbor shield

The purpose of this section is not to study in full detail the liability of Internet
intermediaries in United States but to stress the general principles of secondary
liability of internet intermediaries and the safe harbor provisions that can benefit
internet intermediaries so as to limit /exclude liability. This analysis will allow us to
first analyze how U.S lawmaker and courts balanced the interests of the content
industry with the interests of the Internet intermediaries and then to compare the
U.S and Canadian approach.

a. Overview of the secondary liability doctrine under U.S law

Section 106 of the U.S Copyright Act stipulates that the owner of copyright has the
exclusive right “to do and authorize” any of the rights of copyright. There is a debate

Subject to sections 107 through 122, the owner of copyright under this title has the exclusive rights
to do and to authorize any of the following:
(1) to reproduce the copyrighted work in copies or phonorecords;
(2) to prepare derivative works based upon the copyrighted work;
(3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other
transfer of ownership, or by rental, lease, or lending;
(4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion
pictures and other audiovisual works, to perform the copyrighted work publicly;
(5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial,
graphic, or sculptural works, including the individual images of a motion picture or other audiovisual
work, to display the copyrighted work publicly; and
(6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital
audio transmission.
as to whether this section 106 constitutes the statutory basis for secondary liability. Having said that, under U.S copyright law, there are two different theories of secondary liability that is, ‘vicarious liability’ and ‘contributory infringement’.

**Vicarious liability**

This theory is based on the principle tort of vicarious liability. Ultimately, the rule means that when the right and ability to supervise mingle with an obvious and direct financial interest in the exploitation of copyrighted materials, even in the absence of actual knowledge that the copyright monopoly is being impaired, the purposes of copyright law may be best effectuated by the imposition of liability upon the beneficiary of that exploitation. Most of the litigation regarding vicarious liability against Internet intermediaries are related to actions against developer of P2P software and are therefore beyond the scope of the present analysis.

**Contributory infringement**

In case a party “with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another”, this party may be held liable as “contributory infringer”. U.S courts have embraced a quiet broad view of contributory infringement for this principle is based on the tort theory of “enterprise liability” or “joint enterprise”. Content rightholders had some success in applying contributory infringement to Internet intermediaries as P2P providers. Thus, Napster was found to be liable for contributory infringement, finding that Napster had materially contributed to the infringement by providing the support services that enabled Napster users to find and download music.

---

43 Supra notes 40, 41.
44 Gershwin Publishing Corp. v. Columbia Artists Management, Inc. 443 F.2d1159, 1161 (2d Cir. 1971).
46 Supra note 41, at 1022.
b. The Digital Millenium Copyright Act (DMCA)

The extent judicial approach towards contributory infringement urged Internet and telecom players to lobby Congress so as to enact the Online Copyright Infringement Liability Limitation Act, which is part of the DMCA. The safe harbor defense (Section 512) provides limitation of liability defense for Internet intermediaries. It also comprises a safe harbor defense against direct and secondary copyright infringement. 47 In fact, section 512 (a) stipulates:

“A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, (…)”. 48

This immunity is not absolute and is granted provided that the service provider interacts with the infringing content/material to the extent utterly necessary for the transmission to occur, following a request by a third party to that third party's designated recipients, not storing copies of the content/material transmitted for longer than the strictly necessary. 49 One can read behind the lines of this provision and find that U.S Congress tried to foster innovation by granting immunity to Internet intermediaries. However this immunity is not absolute, otherwise it would have granted a property rules in innovators /Internet intermediaries, allowing them

47 17 U.S.C § 512.
48 Id. 7 U.S.C § 512(a).
49 Id. 7 U.S.C § 512(a) (1) to (5).
to produce technologies that are harmful to the content industry and to actively promote their use for infringement.\textsuperscript{50}

\textbf{ISP’s Safe Harbor}

The safe harbor refers to service providers who provide transmission, routing, and connection services.\textsuperscript{51} This definition encompasses ISP’s such as AOL or Verizon.

\textbf{Caching provider Safe Harbor}

The second safe harbor refers to service providers who provide “intermediate and temporary storage of material” on a system or network, which the providers control, that is, system caching.\textsuperscript{52}

\textbf{Hosting and UGC providers Safe Harbor}

The third safe harbor refers to service providers who provide hosting services, i.e. “the storage at the direction of a user material that resides on a system or network controlled or operated by or for the service provider”.\textsuperscript{53}

As it will be discussed herein, this section is of the utmost importance for Web 2.0 service providers,\textsuperscript{54} who offer user generated content services (UGC) (e.g. Youtube or DailyMotion) as they are facing a considerable amount of lawsuits from rightholders since Web 2.0.

\textbf{Search Engines and linking providers Safe Harbor}

The last safe harbor refers to service providers who are “referring or linking users to an online location containing infringing material or infringing activity, by using

\begin{footnotesize}
\begin{itemize}
\item [\textsuperscript{50}] Supra note 4, pp.955.
\item [\textsuperscript{51}] Id. 7 U.S.C § 512(a).
\item [\textsuperscript{52}] Id. 7 U.S.C § 512(b).
\item [\textsuperscript{53}] Id. 7 U.S.C § 512(c).
\item [\textsuperscript{54}] Supra note 37.
\end{itemize}
\end{footnotesize}
information location tools, including a directory, index, reference, pointer or hypertext link”.55 This last safe harbor refers to hyperlinking providers, that is, search Engines and hyper linkers (e.g. content aggregators price aggregators or comparison sites like RSS, Google News and Yahoo).56 This safe harbor is very important as it deals with the new actors of Web 2.0. Similarly to UGC, these Internet service providers face nowadays several lawsuits for copyright infringement.

The Internet/cloud service providers can benefit from the above-mentioned safe harbors provided that they comply with the conditions provisioned under section 512 (i):

“i) Conditions for Eligibility
(1) Accommodation of technology. — The limitations on liability established by this section shall apply to a service provider only if the service provider
(A) has adopted and reasonably implemented, and informed subscribers and account holders of the service provider’s system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers; and
(B) accommodates and does not interfere with standard technical measures”.

55 Id. 17 U.S.C § 512(d).
56 A content aggregator is an individual or organization that gathers Web content (and/or sometimes applications) from different online sources for reuse or resale. There are two kinds of content aggregators: (1) those who simply gather material from various sources for their Web sites, and (2) those who gather and distribute content to suit their customer’s needs. The latter process is called syndication, Search SOA, content aggregator, online: <http://searchsoa.techtarget.com/definition/content-aggregator>.
Although subsection (a) dealing with ISP’s liability and (b) dealing with system caching do not condition the immunity on lack of knowledge of infringement, subsection (c) addressing hosting and UGC providers liability and subsection (d) addressing search engines and linking providers entail that the cloud /Internet service provider lack “actual knowledge” that the content hosted or hyperlinked may infringe the copyright of rightholders. 57

Subsection (d), addressing search engines and hyperlinking providers’ liability seems to implement a blend of secondary liability doctrine. In fact, it provides that the service provider shall lack actual or constructive knowledge (vicarious liability) and shall also not receive a direct financial benefit from the infringing content. 58

Subsection (c) provides a ‘notice and take down’ (NTD) obligation. The NTD obligation means that, when a service provider receives a notice of infringement from a right/content holder, it must respond in a timely manner to remove or disable access to the material. 59 The service provider shall also publicly design an agent so as to receive all the notifications of alleged infringement. 60

In conclusion, the safe harbors provision is an essential doctrine of the U.S copyright law. Without this provision, the secondary liability of Internet intermediaries may have been engaged in several instances and the development of innovators like Google, Yahoo, and YouTube may have been compromised. Having said that, although nobody challenged the importance of the DMCA, its conditions as applied and interpreted by U.S courts have been criticized.

57 17 U.S.C § 512 (c), (d) providing that service providers should not be liable of they do not have any actual knowledge of infringing content hosted and/or linked.
58 17 U.S.C § 512 (d)(1), (2); Supra note 28.
59 17 U.S.C § 512 (c)(1)(C).
60 17 U.S.C § 512 (c)(2).
Indeed there is a controversy as regards the exact meaning of the “right and ability to control” an infringing activity\textsuperscript{61}, what comprises a “direct financial benefit”,\textsuperscript{62} and what is the definition of knowledge described in section 512 (c). For instance, though it is agreed that “apparent knowledge” shall be considered both subjectively, that is whether the cloud/Internet service provider was aware of the infringing content and objectively, i.e. whether a reasonable person placed in the same circumstances would have been aware of the infringing contend, the issue is how the test will be practically applied?

There are two approaches as to how to interpret such “ambiguity”. The first approach would be to deplore it as neither internet intermediaries nor content owners would be able to predict precisely how it will be interpreted by the courts in any eventual litigation. The second approach is to see in this “ambiguity” a sort of flexibility. The new technology sector evolves so rapidly that the lawmaker or the courts cannot reasonably keep up. One may therefore consider that the best method to deal with this constant technological change is to enact general principles to be clarified on a case-by-case basis by the courts. The DMCA safe harbor seems to offer this kind of flexibility allowing U.S courts to cope with new copyright issues on a case-by-case basis.

2. Fair use harbors

\textit{a. Statutory provision}

As a preliminary remark, it has to be mentioned that it has been contended that fair use works at “the periphery of copyright enforcement in the cloud”\textsuperscript{63} for it is an exception to the primary act of infringement and not a separate defense against

\textsuperscript{62}Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th. Cir. 2007).
\textsuperscript{63}Supra note 28.
secondary liability infringement claims. We will see in this section that this is not always correct for fair use can feature prominently.\footnote{Infra note 70.}

Section 17 U.S.C. § 106 of U.S Copyright Act enumerates a bundle of rights provided by the possession of a valid copyright on a specific work.\footnote{Ibid.} The United States Copyright Act provides also a list of limitations where copyright infringement is established but where the defendant can escape liability.\footnote{17 U.S.C. §§ 107-22.}

In fact, section 17 U.S.C § 107 provides:

“Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include

(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

(2) the nature of the copyrighted work;

(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

(4) the effect of the use upon the potential market for or value of the copyrighted work.
The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors”.

The various factors and purposes are not exhaustive, they are just illustrative. In *A.V v. iParadigms*, the Fourth Circuit considered that “Section 107 contemplates that the question of whether a given use of copyrighted material is ‘fair’ requires a case-by-case analysis in which the statutory factors are not “treated in isolation but are weighted together, in light of the purposes of the copyright”’. The U.S doctrine of fair use only stipulates overall legislative recommendations and mainly leaves to courts the mission of elaborating what could be considered as a fair use defense on a case-by-case basis. When the court asserts that the factors enumerated by Section 17 U.S.C. § 106 are weighted together it means for example that though the commercial purpose weights against the establishment of a successful fair use defense, such element is not dispositive. Actually, the courts will use four factors to assess whether fair use defense may be successfully used. Its essential to note that these factors are only guidelines that courts are free to adapt in a specific case.

It is clearly the intention of the U.S. Congress to leave fair use open to interpretation and new technology/cloud computing based upon a court's consideration of any particular case before it. A court must consider all four criteria set out in the Act in making its determination. These four factors are Congress' attempt to codify common law fair use. Professor Leaffer opined that these factors are broadly stated, overlapping, and vague, and the legislative history provides little insight as to their meanings, what weights to give them, or how they interrelate. He argues that, “legal developments, both at home and abroad, driven by technological change and the push toward the international harmonization of legal norms, threaten the very survival of fair use. Given these realities the doctrine will, of necessity, be

---

67 *A.V v. iParadigms, LLC*, 562 F.3d 630 (4th Cir. Apr. 16, 2009).

reconceptualized”. 69

b. Application of the fair use doctrine by U.S courts

In order to illustrate how fair use case law has operated in relation with the liability of Internet intermediaries we propose to analyze two decisions of U.S courts.

Sony Corp. of America v. Universal City Studios

Sony Corp. of America v. Universal City Studios 70 also known as the “Betamax case” was not a decision involving Internet intermediaries but is relevant for the present analysis as it the first time the Supreme Court contemplated the indirect liability of a new technology company. In this case the Supreme Court considered whether Sony was liable for manufacturing the Betamax videotape recorder (VTR). Universal Studios sued Sony for contributory infringement, alleging that Sony provided end-users with a tool to make unauthorized copies of movies.

The essential question was whether the extent of owner’s copyright exclusive right/control covered this innovative technological use. The Supreme Court had for the first time to arbitrate between the interest of copyright owners and the interest of new technologies companies. The Court observed that whilst some consumers used VTR for illicit purpose, other used them for “time shifting”, recording and watching their favorite shows at a later time. According to the court, such use constitutes a non-infringing fair use. 71 As to whether Sony could be described as "contributing" to copyright infringement, the court stated:

The staple article of commerce doctrine must strike a balance between a copyright holders legitimate demand for effective - not merely symbolic - protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of

---

69 Ibid. at 849, 850.
71 Ibid. at 447-55.
commerce. Accordingly, the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial non-infringing uses. 72

As time shifting was the VTR’s prevalent use, the Court did not find a contributory liability. The Court stayed intentionally vague regarding the exact meanings of “capable” and “substantial” for the VTR cleared the test. 73

A scholar has observed that "the Sony decision is the most significant legacy of Justice Stevens in the field of intellectual property law and its significance is likely to continue in mediating disputes between copyright industries and creative information technology developers and users of information technology”. 74 Other authors contended that the contour of Betamax safe harbor remain fuzzy and even arbitrary. 75

Now, we suggest discussing whether Betamax decision was a balanced decision, i.e. if it promoted innovation without chilling the content industry. Dotan Oliar claimed that Betamax decision was very permissive as the standard to qualify for the safe harbor was low. To qualify as technology had only to be capable of a substantial non- infringing. 76 Dotan Oliar concludes that such standard is close to a property rule in innovators, in other word, that it would induce some technologies companies to market harmful technologies and invest perversely in harming copyright owners.

72 Ibid. at 442.
73 Ibid.
75 Supra note 4, at 961.
76 Ibid at 995.
77 Ibid.
In practice, the Betamax decision was not that harmful for the content industry, in contrary, rather than destroying the movie industry, videotape sales became gradually important to their income. By the mid 90’s more than half of Hollywood’s film industry revenue came from home video compared to less than a quarter from movie theaters. By 2001, the VCR was not anymore "arguably believed to be the death knell of the movie business. Instead it became arguably its savior" because consumers much preferred buying or renting films to recording their own onto blank tapes.

Although Dotan Oliar is right to mention the Supreme Court set a low safe harbor standard to qualify for the safe harbor and that the exact meanings of “capable” and “substantial” are not clear, I believe that this decision is not arbitrary. One has to remember the context of the decision. Indeed in 1984, it was the very beginning of new technologies companies. The court had to protect rightholders but had also to make sure that its decision will not discourage innovation. The VCR technology was revolutionary at that moment. I believe that the court has to set a low standard in order to not chill innovation and to remain fuzzy so as to keep a sort of flexibility in the absence of any statutory provision or judicial precedent.

**Perfect 10, Inc. v. Amazon.com, Inc**

In *Perfect 10, Inc. v. Amazon.com, Inc*., the court ruled that Google’s framing and hyperlinking as part of an image search engine constituted a fair use of Perfect 10’s images because the use was highly transformative, overturning most of the district court’s decision. The court noted that Google made available to the public the new and highly beneficial function of "improving access to information on the Internet."

---


80 *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007).
This had the effect of recognizing that, "search engine technology provides an astoundingly valuable public benefit, which should not be jeopardized just because it might be used in a way that could affect somebody's sales." The court also mentioned the importance of analyzing fair use flexibility in light of rapid technological changes. Indeed, the Court insisted that the dispositions of the Statutes should not be frozen in time of rapid technological change.

*Perfect 10, Inc. v. Amazon.com, Inc.* shows that despite the criticism about its vagueness, fair use is a flexible doctrine that evolved continuously with the development of new technologies. It is because the foregoing four factors are only guidelines that can be adapted by courts that the fair use doctrine can survive and adapt to the development of new technologies. Since the article of Professor Leaffer, i.e. in 2001, fair use has not been threaten or disappeared, in contrary it has adapted rapidly thanks to its flexibility.

### 3. How copyright cases affecting the liability of cloud providers have been addressed by U.S courts

#### a. MAI Systems Corp. v. Peak Computer Inc.: the identification of copyright in the cloud

*In MAI Systems Corp. v. Peak Computer, Inc.*, is one the most significant decisions dealing with the identification of copyright in the digital area.

---

81 *Ibid*, at 15471 § 12, "We conclude that the significantly transformative nature of Google's search engine, particularly in light of its public benefit, outweighs Google's superseding and commercial uses of the thumbnails in this case. In reaching this conclusion, we note the importance of analyzing fair use flexibly in light of new circumstances. *Sony*, 464 U.S. at 431-32; *id.* at 448 n.31 (" '[Section 107] endorses the purpose and general scope of the judicial doctrine of fair use, but there is no disposition to freeze the doctrine in the statute, especially during a period of rapid technological change.' ") (quoting H.R. Rep. No. 94-1476, p. 65-66 (1976), U.S. Code Cong. & Admin. News 1976, p. 5680)). We are also mindful of the Supreme Court's direction that "the more transformative the new work, the less will be the significance of other factors, like commercialism, that may weigh against a finding of fair use." *Campbell*, 510 U.S. at 579".

82 *Ibid*.

83 *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993).
In this decision, the U.S Court of Appeals for the Ninth Circuit addressed the question of whether or not the loading of a software program into RAM by a computer repair technician makes a copy of the software that is a potential violation of copyright law.

The court ruled that a copy of a program made from a hard drive into RAM for purpose of executing the program was a copy under the Copyright Act. The judges utilized the criteria set forth by 17 U.S.C. § 101, which states that a work is "fixed" in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.'

17 U.S.C. § 117 allows copies made as an essential step in utilizing the software to be made without permission of the copyright holder by the owner of a copy of the software. Nonetheless, the court believed that this clause did not apply because end users of MAI's software were mere licensees. The court also considered two additional facts: Peak had unlicensed copies of MAI's operating system at Peak's headquarters and the unlicensed loaning of computers featuring MAI's operating system to Peak's customers.

Based on the above facts, the court found that Peak was guilty of copyright infringement.

*MAI Systems Corp. v. Peak Computer, Inc* does not deal directly with the liability of Internet intermediaries. However this decision is significant, as it is the first U.S judicial decision identifying copyright in the digital age. Besides, as it will be considered in the following sections, other U.S courts84 have challenged the conditions of copyright liability established by *MAI Systems Corp. v. Peak Computer, Inc*. 

---

84 *Cartoon Network, LP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008).
b. Carton Network v. Cablevision: The existence of copyright infringement in the context of digital video recorders

Carton Network v. Cablevision is among the most recent and important decisions impacting cloud based storage providers. Cablevision, a cable television provider, wanted to create a hosted DVR (Digital Video Recorder) service. Precisely, Cablevision revealed plans in March 2006 to sell a “remote storage DVR system” ("RS-DVR") to allow subscribers without a DVR to record cable programs on central hard drives Cablevision maintained at a “remote” location. A consortium of copyright holders in the television and film industries sued for direct copyright infringement on the grounds of unlawful copying and public performance.

The United States Court of Appeals found that:

a) the copying of streaming content for the purposes of buffering did not itself constitute unlawful copying.
b) the automated copying of content at user request did not constitute direct infringement,
c) Time shifting, or replaying content to the original audience, did not constitute public performance,

and

a) As to whether the creation of RAM copies are infringing and more precisely concerning content buffering, the court noted that the Copyright Act requires two conditions for a work to be "fixed" and hence infringing:

   o **Embodiment requirement**: the work must be both "embodied in a copy or phonorecord",

___________________________

85 Ibid.
o **Duration requirement**: the work must be perceivable "for a period of more than a transitory duration."

The court considered that the district court relied too heavily on the embodiment requirement and did not properly consider the duration requirement. In this, the Circuit Court noted the lower court's reliance on *MAI Systems Corp.*, which held the creation of RAM copies to be infringing. The Circuit Court found that this case is missing an important element, as it did not address the duration requirement. Indeed, the alternative interpretation, as the court points out, would read the "transitory duration" language out of the Copyright Act. The Circuit Court thus held that while the data was embodied in the buffer, the duration was sufficiently small to be considered transitory.

b. The second claim overturned by the court was that Cablevision was liable for direct copyright infringement for copying programs to the hosted service RS-DVRs. The court contended that Cablevision did not evince the required "volitional conduct" that actually instigated the copy to be made and established that Cablevision's conduct in designing, hosting, and maintaining a system can not be seen as direct infringement.

c. The third and possibly the most debated claim overturned by the appeals court was that the transmission of programming from the RS-DVR to subscribers who requested playback violated the public performance right. Here, the court considered Cablevision claim as pertinent, i.e. that, "because each RS-DVR transmission is made using a single unique copy of a work, made by an individual subscriber" only one subscriber is capable of receiving the transmission of that particular work, hence the performance can not be considered as "public".

The holding in the Cablevision case that individualized copies of content specifically streamed to subscribers from remote DVRs constitute private, as opposed to public, performances presents a kind of ambiguity regarding the rights necessary for cloud-based transmissions of content. Put it differently, the question remains as to whether streaming of legally obtained content to an end-user from the cloud (e.g.,
MP3 music/video stored in a digital locker like iCloud, etc.) involves the public performance right.

This decision has been widely criticized for that, cloud providers are allegedly left considering whether further authorization is required from copyright holders, and in the absence of such consent, whether there is a potential risk that another U.S. tribunal could later disagree with the Second Circuit’s holding in the Cablevision Case. It has also been contended that the application of the holding in the Cablevision Case (that individualized copies of content specifically streamed to subscribers from remote DVRs constitute private, as opposed to public, performances), does not permit to understand the copyright liability of hosting/cloud providers. ⁸⁷

On the other hand, some authors argued that Cartoon Network is aligned with Betamax decision for both decisions bolster innovation. ⁸⁸ Besides, it has been contended that this ruling seems to protect service providers allowing them to conduct their Internet business without any risk of infringement, even secondary.

It seems to me that the criticisms of Cartoon Network v. Cablevision are not justified for it is a highly significant decision for cloud computing providers. Indeed this case stopped Cablevision being rendered liable for any copyright infringing material stored in the clouds. Despite the claim that this decision does not permit to understand the liability of cloud provider, it actually cleared the way for Cablevision to deploy its RS-DVR commercially. It also led to additional incremental investment in U.S. cloud computing companies that ranged from $728 million to nearly $1.3 billion over the two-and-a-half years following the decision. ⁸⁹

⁸⁷ Supra note 84, at 43, § 19.
In the other hand, it is difficult to assess the impact of this decision on Carton Network and the entertainment industry. We can however compare Carton Network v. Cablevision with Betamax decision and assume that Sony and Cablevision technologies are almost similar except that Cablevision offered a remote storage DVR system. We can therefore presume that the effect of both technologies is comparable. As discussed hereabove, the Betamax decision was not that harmful for the content industry, in contrary, rather than destroying the movie industry, videotape sales became gradually important to their income. We can anticipate that Cablevision decision will have comparable positive effects on the content industry. At the end of the day, I believe that the court did find a well balance in Carton Network v. Cablevision as it has promoted innovation without harming the content industry.

**c. The Capitol Records Inc. v. MP3tunes, LLC case**

Another recent and ongoing United States case eventually affecting Internet intermediaries especially digital locker and cloud providers is Capitol Records, LLC et al. (“EMI”) v. MP3tunes, LLC. (“MP3Tunes”)91

This is a case filed by EMI, Inc. against cloud-storage service MP3tunes as well as its executive Michael Robertson. In fact, multiple record companies affiliated with EMI have claimed, diverse copyright infringement against MP3tunes, which operates two separate online services—specifically, MP3tunes.com and Sideload.com.

MP3tunes.com allows users to store their music collections in online digital lockers, which they can access from any computer or mobile device from Internet. Sideload.com is a music search engine site that permits users to search for links on the Internet to downloadable music that can be uploaded (or “sideloaded”) to an MP3tunes digital locker. Once music is placed in an end-user’s digital locker,

90 Section II.A.3.c
91 Capitol Records, Inc. v. MP3tunes, LLC, 07 Civ. 9931.
the music becomes available for transmission to any IP-enabled device at the end user’s direction.

EMI has alleged several direct and secondary copyright infringement claims against MP3tunes, including claims that MP3tunes has lost its eligibility under the DMCA safe harbor provisions for its illegal conduct in deliberately providing the means for end-users to violate EMI’s copyrights via Sideload.com and failing to reply to take down notices.

Whereas a thorough analysis of the merits of EMI’s DMCA and contributory liability theories is outside the scope of this analysis, the district court, did find that the MP3tunes was entitled to the DMCA protections, but further addressed a significant issue emerging in the cloud. Precisely, following the reception of a valid takedown notice from EMI, the court ruled that MP3tunes had a duty to not only delete links to infringing materials publicly displayed on Sideload.com, but also a duty to remove songs stored in users’ personal lockers which were downloaded from such links. In its defense submissions, MP3tunes contended that it was solely required to remove the URL links on Sideload.com because only those links were listed on EMI’s takedown notices and that users might sue MP3tunes if it actually removed personal property from users’ digital lockers. 92

The court rejected this argument, referring to the DMCA’s immunity provisions for service providers acting on valid takedown notices 93 asserting that:

“Where service providers such as MP3tunes allow users to search for copyrighted works posted on the internet and store those works in private accounts, to qualify for DMCA protection, those service providers must (1) keep track of the source and web address of stored copyrighted material, and (2) take content down when copyright owners identify the infringing sources in otherwise compliant

92 Supra note 91, at 14, 15.
93 17 U.S.C. 512(g)
notices... [Accordingly,] MP3tunes was obligated to remove specific works traceable to users' lockers .. because MP3tunes keeps track of the source and web address for each sideloaded song in each user's locker and EMI's notices gave sufficient information for MP3tunes to locate copies of infringing song in users lockers. 94

In addition to the foregoing claims, EMI also stressed that MP3tunes infringes the right of public performance by allowing end users to stream music from their online lockers to their personal devices. Relying in part on the holding in the aforementioned Cablevision case, EMI proclaimed that MP3tunes violates the public performance right because it uses a “single master” to play songs to multiple users, as opposed to Cablevision which maintained a separate copy of each program for each subscriber who recorded it.

The district court considered that MP3tunes does not use a “single master” system, but rather a standard algorithm known as “Content-Addressable Storage” to store music files.95 Still, this does not address EMI’s infringement claim regarding the right of public performance as the court’s holding solely relates to the nature of the specific file storage technology employed by MP3tunes.

This decision can be compared with the Betamax and Cablevision decision. In fact, the court considered that MP3tunes is entitled to claim DMCA safe harbor protection. MP3tunes offered to its client similar hosting services. The difference is that in Betamax and Cablevision decisions, end-users were solely recording original copyrighted programs whereas in MP3tunes, end users were able to access and eventually store infringing copyrights songs. Following Betamax and Cablevision decisions, companies were allowed to offer storage services to end-users.

In MP3tunes, The court had for the first time the opportunity to delimitate the liability of cloud providers offering search and storage services, especially the contour of the notice and take down obligation provided under the DMCA.

94 Supra note 91 at 15.
95 Ibid.
This decision was observed by other cloud providers as Google, Amazon, and Apple who were launching cloud music services. It was viewed by Internet/cloud intermediaries as "a victory for cloud music" and a first step in "granting music locker services a firm legal foundation" for it recognized DMCA safe harbor protection for cloud services, possibly permitting them "broad immunity from copyright liability".

Here, the district court stressed that “this case turns in large part on whether Mp3Tunes is eligible to safe harbors created by the DMCA” and added that “the DMCA seeks to balance the interests of copyright owners and online service providers by promoting cooperation, minimizing copyright infringement, and providing a higher degree of certainty to service providers on the question of copyright infringement”. It appears to me that this decision is a half victory for cloud providers for it allowed them to invoke DMCA safe harbors and a half victory for the content industry for it toughened the notice and take down obligation by requiring cloud providers to delete not only infringing links but also illicit content stored on personal lockers of customers. I believe that the court had to reach a difficult balance for it did not want to chill innovation and discourage cloud service investment but it did not want also to harm the content industry.

I conceive that such balance was not that simple to reach as in Cablevision and MP3tunes, cloud-services, whether overtly or implicitly, implicates many of the exclusive rights afforded to copyright holders and stakeholders. It has been argued that the liability of cloud providers for providing cloud services is still imprecise, as the law in the U.S has not yet addressed the contours of cloud services

---

98 Ibid.
99 Supra note 91 at 7; ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 625 (4th Cir. 2001).
100 Supra notes 84 and 91.
and the corresponding responsibilities. This criticism may be grounded, however, one has to remember that in such changing environment as the online environment, courts have to be very cautious in delimiting the liability of internet intermediaries and are compelled to maintain a flexible rules even if they can sometimes be perceived as imprecise.

Following the study of copyright enforcement issues faced by the U.S, the question at this stage is whether Canadian lawmaker and courts faced similar problems in balancing the interests of the content industry with the interests of the Internet intermediaries.

B. CANADIAN COPYRIGHT LAW REGARDING THE LIABILITY OF INTERNET INTERMEDIARIES

Similarly to United States, copyright requires fixation under Canadian law. So far, there is no Canadian case law addressing the question as to whether a temporary copy or a virtual programs created in the cloud constitutes copyright infringement.

As stated in Theberge v. Galerie d’Art du Petit Champlain, the fixation singularizes works that may attract copyright from general idea that are the common idea of humanity although conceptually the question of fixation in the context of when is a work protected is distinct from the question of when such work is infringed. Put in differently, copyright exists as soon as the work in question is written or recorded in a permanent form. Therefore, if the work is not permanent or fixed sufficiently, there is no copyright. Applying this general principle of copyright to the cloud leads to question how permanent or fixed is the cloud and the work in the cloud?

Before tackling this question, it is necessary to recall the exclusive rights of copyright under Canadian law, section 27. (1) of the Copyright Act provides that:

\[101\] Ibid.

“It is an infringement of copyright for any person to do, without the consent of the owner of the copyright, anything that by this Act only the owner of the copyright has the right to do”.

Section 3 (1) describes what the owner of the copyright has the right to do. 103

Actually, copyright is a negative right to prevent others from exercising the right available to the author under the Act. 104 The issue with the cloud is that reproductions/copies may exist everywhere at a specific time and then disappear, as can the infringer, user.

In *Apple Computer Inc. v. Mackintosh Computers Ltd.*, 105 computer programs encoded on chips as a series of circuits were “copied” by copying the chips directly and without copying the written form of the programs. It was held that a copy made of a reproduction in a different form from the original, was still an infringement of

---

103 3. (1) For the purposes of this Act, “copyright”, in relation to a work, means the sole right to produce or reproduce the work or any substantial part thereof in any material form whatever, to perform the work or any substantial part thereof in public or, if the work is unpublished, to publish the work or any substantial part thereof, and includes the sole right

(a) to produce, reproduce, perform or publish any translation of the work,

(b) in the case of a dramatic work, to convert it into a novel or other non-dramatic work,

(c) in the case of a novel or other non-dramatic work, or of an artistic work, to convert it into a dramatic work, by way of performance in public or otherwise,

(d) in the case of a literary, dramatic or musical work, to make any sound recording, cinematograph film or other contrivance by means of which the work may be mechanically reproduced or performed,

(e) in the case of any literary, dramatic, musical or artistic work, to reproduce, adapt and publicly present the work as a cinematographic work,

(f) in the case of any literary, dramatic, musical or artistic work, to communicate the work to the public by telecommunication,

(g) to present at a public exhibition, for a purpose other than sale or hire, an artistic work created after June 7, 1988, other than a map, chart or plan,

(h) in the case of a computer program that can be reproduced in the ordinary course of its U.Se, other than by a reproduction during its execution in conjunction with a machine, device or computer, to rent out the computer program, and

(i) in the case of a musical work, to rent out a sound recording in which the work is embodied, and to authorize any such acts.


Applying this to the cloud, a virtual infrastructure, platform, software or other work that is reproduced in a cloud, in a different form from the original, could be infringing. But it must be a substantial (quality vs. quantity) part of the work and the material must still be the proper subject matter of copyright.

As seen in the foregoing section, U.S. and Canadian courts struggled to identify whether copyright liability exist in the cloud. When this question has been answered, the main problem is to identify the entity that should be liable for infringing work posted in the cloud. As here above mentioned, clients are increasingly using the cloud to either store their contents (media, music, documents) or to download contents from the cloud. In the same time, rightholders increased the pressure on Internet intermediaries by suing them for copyright infringement and on the legislature so as to enact new rules implementing tougher secondary liability of online/cloud intermediaries for the infringing conduct of their users. Therefore as in the U.S, Canadian lawmaker and courts had to find a balance between the interests of innovators and content owners while addressing copyright enforcement issues in the cloud.

1. General overview of the secondary liability of Internet intermediaries under Canadian law

Section 3 of Canadian Copyright Act provides that rightholders have the exclusive right to produce or reproduce the work, to perform it, to publish it and to authorize such acts”. Section 27 of the Copyright Act states that constitutes an infringement

106 Daniel Seng, Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries, online: WIPO Online Website, at 36
107 Copyright in works
"3. (1) For the purposes of this Act, “copyright”, in relation to a work, means the sole right to produce or reproduce the work or any substantial part thereof in any material form whatever, to perform the work or any substantial part thereof in public or, if the work is unpublished, to publish the work or any substantial part thereof, and includes the sole right
for anyone to do any act that the Copyright Act reserves only to rightholders, including the right of authorization. As here above mentioned, it can be observed that Canadian “authorizing infringement” principle is regarded as a kind of vicarious liability under U.S. copyright law.

The meaning of the Canadian “authorizing infringement” principle has been explained in *CCH Canadian Ltd. v. Law Society of Upper Canada* (“CCH”),. Essentially, the Supreme Court of Canada considered that the fact that the Law Society of Upper Canada provided self-service photocopiers in its library did not amount to authorizing copyright infringement. The Supreme Court accepted that the act of authorization has to be determined on a case-by-case basis and that such act could be deduced from acts that are not necessarily direct and positive, including a sufficient degree of indifference. Nevertheless, the Supreme Court held that a person does not authorize infringement by authorizing the mere use of equipment(s) that may eventually be used to infringe copyright. According to the Supreme Court, there is a presumption of lawful authorization. However this presumption can be rebutted if it is proved that a relationship or degree of control

---

(a) to produce, reproduce, perform or publish any translation of the work,
(b) in the case of a dramatic work, to convert it into a novel or other non-dramatic work,
(c) in the case of a novel or other non-dramatic work, or of an artistic work, to convert it into a dramatic work, by way of performance in public or otherwise,
(d) in the case of a literary, dramatic or musical work, to make any sound recording, cinematograph film or other contrivance by means of which the work may be mechanically reproduced or performed,
(e) in the case of any literary, dramatic, musical or artistic work, to reproduce, adapt and publicly present the work as a cinematographic work,
(f) in the case of any literary, dramatic, musical or artistic work, to communicate the work to the public by telecommunication (…).

108 Section 27(1).
109 Ibid.
111 Ibid, at para 46.
112 Ibid at para 38.
113 Ibid at para 43.
114 Ibid at para 38,43.
existed between the supposed authorizer and the primary author of the copyright infringement. ¹¹⁵

Following CCH, the Society of Composers, Authors & Music Publishers of Canada (SOCAN) sought before the Canadian Copyright Board to impose royalties on all entities involved in the Internet chain, comprising the backbone service providers, for the act of communication of downloaded contents (music), but then restricted their claim to ISP’s located in Canada for they providing access to contents providers and end users. ¹¹⁶ SOCAN contended that Canadian ISP’s were liable for authorizing infringement. In Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers (“SOCAN”), the Supreme Court assessed that although the “knowledge of the content available on the Internet”, especially free contents, “are powerful inducements for end-users to sign up with access providers, and content providers with operators of host services”, ¹¹⁷ nonetheless, there were also “massive amounts of non copyrighted material” accessible to Internet end-users. ¹¹⁸

In view of CCH, the Supreme Court reassessed the presumption of lawful authorization and concluded that “knowledge that someone might be using neutral technology to violate copyright is not necessarily sufficient to constitute authorization, which requires a demonstration that the defendant did give approval to, sanction, permit, favor, encourage, the infringing conduct”. ¹¹⁹

What is essential for the purpose of the present analysis is that the Supreme Court concluded that the participation of the ISP’s on communicating copyright works is

¹¹⁵ Ibid at para 38.
¹¹⁷ Ibid at para 121.
¹¹⁸ Ibid at para 123.
¹¹⁹ Ibid at para 127.
content neutral. However the court considered that in case an ISP’s is aware of an infringing material posted in its system and do not take any positive action such as require the end-user to remove the contended infringing material over a take down notice, it may not be seen anymore as a content neutral actor. In other words, the Supreme Court contemplates that in case an ISP’s has general knowledge of an infringing content and do not take positive step(s) to take down such content, this ISP’s may be held liable for copyright infringement. The Supreme Court would have preferred a statutory notice and take down notice regime as the DMCA. In the absence of such statutory regime, it did not provide any further guidance except the fact that the existence of “authorization” should be decided on a case-by-case basis.

In CCH, the Supreme Court insisted on the fact that the exceptions in the Copyright Act must be interpreted liberally in order to ensure that the Act’s purpose – which is to maintain a balance between copyright owners’ rights and users’ interests – can be fully achieved.

In SOCAN, the Supreme Court also suggested a broad notice and take down regime similar to the DMCA (even if the court ruled that this NTD regime has to be implemented by the legislature). The Court maintained the same flexibility as U.S case law, by stating that the existence of “unlawful authorization” by Internet intermediaries will be decided on a case-by-case basis.

---

120 Ibid at para 92, 124.
121 Ibid at 110, 124.
122 Ibid at para 127.
123 Ibid at para 128.
124 Supra note 110, at 48.
125 Ibid.
a. Liability of ISP, Hosting Providers and Referral Services

The essential question to be addressed here is how, in the absence of DMCA safe harbor, Canadian courts tackled the liability of Internet intermediaries and how they balanced the interests of Internet intermediaries and content owners.

It has been previously mentioned that Internet intermediaries became very important actors since Web 2.0 i.e. the expansion of cloud computing. It has also been stated that since 2004, rightholders took multiple legal actions against Internet intermediaries claiming that they facilitate or benefit from infringing endeavor.

b. Liability of ISP under current Canadian Copyright law: the statutory “Common Carrier” exception explained by the courts

Section 2.4(1) of the Canadian Copyright provides:

“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.”

Known as the “common carrier exception”, this provision was originally intended to ensure that providers that “serve as an intermediary between the signal source and a retransmitter whose services are offered to the general public” would not be held liable. 126

In SOCAN, 127 the Supreme Court of Canada explained the meaning of this provision in relation with the liability of Internet intermediaries:

---

126 Sub-Committee on the Revision of Copyright of the House of Commons Standing Committee on Communications and Culture, A Charter of Rights for Creators (1985), at 80.
127 Supra note 116.
"Section 2.4(1)(b) shields from liability the activities associated with providing the means for another to communicate by telecommunication. “The ‘means’”, as the Board found, “. . . are not limited to routers and other hardware. They include all software connection equipment, connectivity services, hosting and other facilities and services without which such communications would not occur” (…). I agree. So 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, then it will fall within s. 2.4(1)(b)”. 

The Supreme Court connected ISP’s role with those of owners o telephone wires, in that they lack tangible information as regards the infringing content transmitted through their infrastructure, and considered that its unrealistic from a law and economic prospective to monitor the vast amount of material moving through the Internet”. Interestingly, The Supreme Court referred several times to international safe harbor instruments and pronounced that it’s interpretation of section 2.4(1)(b) is consistent with the European E-commerce Directive Preamble, which stipulates that the exemption of liability concerns solely the neutral activity of ISP’s, that is, when their act as a mere conduit.

c. The judicial safe harbor granted to hosting providers

In the absence of statutory safe harbors in the form similar to the DMCA, the Supreme Court considered in SOCAN that section 2.4(1)(b) of the Copyright Act safeguarded Internet intermediaries providing host server services from liability. The Court agreed with the Copyright Board in not imposing liability on host server

---

128 Ibid, para 96.
129 Ibid, para 101.
130 Ibid, para 98.
providers. It is implicit from the Court’s decision that in performing such functions, they generally act as mere conduits without the requisite degree of knowledge of infringement to make them liable.

However, the Supreme Court agreed that that a host provider may be held liable if it failed to response to a notice of infringing content by “taking it down”. In the present case, the Supreme Court did not answer such question as it considered that it was not the question at issue. 131

Remarkably, Justice Binnie noted that following an infringement notice, instead for the provider to assess whether the copyright objection is founded and to choose between contesting a copyright action or potentially breaching its contract with the content provider, “A more effective remedy to address this potential issue would be the enactment by Parliament of a statutory “notice and take down” procedure as has been done in the European Community and the United States”. 132

In the same way as section 7 U.S.C § 512(c) of the Online Copyright Infringement Liability Limitation Act (which is part of the DMCA), the Supreme Court acknowledged a principle of immunity for host providers. However the conditions of such immunity are not explained. The Supreme Court referred to the notice and take down procedure provisioned under European law. According to Justice Binnie, such procedure shall be provided by the legislature. The comment made by Justice Binnie is of the utmost importance as Canadian courts tried to address the liability of Internet intermediaries in the absence of clear statutory provision (except for the general Section 2.4(1) of the Canadian Copyright referred here above). However Justice Binnie seems to consider that there is a limit upon which courts cannot go beyond in addressing such issue. At the end of the day, there is not any notice and take down procedure under Canadian law, unlike United States and European copyright law.

131 Supra note 116 at 123, 127-128,
132 Ibid, para 127.
In a nutshell, pre-bill C-11, the Supreme Court of Canada granted a sort of common law DMCA to host providers. By doing so, the Supreme Court protected these Internet intermediaries and *ipso facto* innovation. We will see in the subsequent section how bill C-11 implemented a statutory DMCA in Canadian copyright law.

**d. The existence of a judicial safe harbor granted to referral services**

Referral services refer to Search Engines and hyperlinks portals.  

Search Engines, such as Google, Baidu are significant actors in the realm of navigation and management of Internet resources. The main issue is that contrary to the U.S, in Canadian copyright law pre-bill C-11, there was no statutory provisions dealing with the liability of search engines as the DMCA in the U.S.

In *SOCAN*, the Supreme contended in a *obiter* that the creation of an automatic hyperlink one that instructs a browser that accesses a first website to download a file/document from a second website, as opposed to manual hyperlink, where the user must take some action such as to click on the link to access the information on the second site, may attract copyright liability in authorizing infringement for communicating the work. Nonetheless, the Supreme Court did not make any further reference to the liability of referral services intermediaries providing manual hyperlinks to third party sites either in its review of section 2.4(1)(b) or in its analyze regarding authorizing infringement.

**e. Crookes v. Newton: hyperlinks are content neutral**

In a very recent decision, the SCC ruled that hyperlinks are, in essence references and that, it should never, by itself been seen as “publication” of the content to which

---

133 *Supra* note 116, at 36,

134 7 U.S.C § 512(d).

135 *Supra* note 116, at 25. “Automatic links employ an embedded code in the Web page that automatically instructs the browser, upon obtaining access to the first site, to download a file from a second site. The user does not need to do anything but visit the initial site before information from the second site is “pulled”. A different legal issue may arise where the user must take action, such as to click the mouse button over the hyperlink, in order to obtain access to the information from the second site”.

---
it refers. 136

The SCC ruled:

“The fact that access to (...) content is far easier with hyperlinks than with footnotes does not change the reality that a hyperlink, by itself, is content neutral (highlight added) – it expresses no opinion, nor does it have any control over, the content to which it refers (...)

Making a reference to the existence and/or location by hyperlink or otherwise, without more, is not publication of that content. Only when a hyperlinker presents content from the hyperlinked material in a way that actually repeats the defamatory content, should that content be considered to be ‘published’ by the hyperlinker (...)

In this decision, Justice Abella stressed the importance of the Internet to the flow of information in modern society:

“The Internet cannot, in short, provide access to information without hyperlinks. Limiting their usefulness by subjecting them to the traditional publication rule would have the effect of seriously restricting the flow of information and, as a result, freedom of expression. The potential “chill” in how the Internet functions could be devastating, since primary article authors would unlikely want to risk liability for linking to another article over whose changeable content they have no control. Given the core significance of the role of hyperlinking to the Internet, we risk impairing its whole functioning. Strict application of the publication rule in these circumstances would be like trying to fit

a square archaic peg into the hexagonal hole of modernity”. 137

According to eminent scholars, this decision is amid the most important decision of the Supreme Court on Internet. 138 Whereas this decision concerned defamation, the court’s acknowledgement of the limits of links raises interesting questions about other area of law especially copyright, where some have claimed that linking to purportedly infringing content should itself constitute an infringement. Actually, this case does not rule on that specific copyright infringement issue.

Howard Knopf argued:

"If a link or hyperlink by itself does not constitute ‘publication’ for defamatory purposes, it is difficult to see how it could, by itself, constitute publication or reproduction or any other activity covered by the Copyright Act”. 139

Howard Knopf interpretation makes sense as if hyperlinks are content neutral as ruled by the Supreme Court, they are neutral for all content conveyed viz. copyright infringing contents. If hyperlink are content neutral, therefore the provider of such content i.e. the Search Engine and the hyperlinker may ipso facto be considered as a neutral intermediary.

In a fresh decision, 140 the Federal Court confirmed Howard Knopf interpretation. The facts were pretty straightforward. Free Dominion, was a Canadian-based political news website where users regularly post online articles or link. On 2008, a column by National Post columnist Jonathan Kay was posted online. After the Post complaint, the column was replaced with shorter excerpt that included the same headline along with three full paragraphs and one half-paragraph. A month later, a

137 Ibid. at 136.
138 Michael Geist, Supreme Court of Canada Stands Up for the Internet: No Liability for Linking, (October 19, 2011), online: M. Geist <http://www.michaelgeist.ca/content/view/6069/125/>.
140 Warman and National Post v Fournier, 2012 FC 803.
user posted a link to a photograph that was posted on the photographer’s website. The photograph itself was not posted as only a link was used.

The court’s had to answer whether such link to the photographer website constituted a copyright infringement. The court noted that the photographer authorized the communication of the work by posting it on his own website and was able to remove it if he did not want others to link to it. In other words, the court said that the communication of the work could not be viewed as unauthorized, since the photographer had implicitly authorized others to access the photo by posting it online.

As Michael Geist notes, this decision should definitely eliminate fears that linking to copyright materials may raise potential copyright infringement risks. 141

As seen in this section, Canadian courts filled a legal void by granting a judicial safe harbor to search engines and hyperlink portals.

Having said tat, it seems that the liability of the Internet intermediaries is stronger and clearer under U.S copyright law for there is a statutory safe harbor provision whereas no such statutory provision exist under Canadian law. However, we observed hereabove that Canadian courts have filed the void in various decisions such as CCH, SOCAN, Crookes v. Newton.

Besides, it has been argued that, Canada has been a laggard on embracing cloud computing for confidentiality, security, and jurisdictional issues. 142 I do not agree with this interpretation as I appreciate that Canadian copyright law pre Bill C-11 has dealt efficiently with copyright issues referred to courts. It’s correct that Canadian courts did not address explicitly the liability of user-generated contents. However, this is due to the fact that Canadians courts did not have the opportunity to deal particularly with such questions. I also appreciate that the conditions of liability of

141 Michael Geist, All the News That’s Fit To Post and Link: Federal Court Clears Up Legal Risks, (July 03, 2012), online: <http://www.michaelgeist.ca/content/view/6573/135/>.
Internet intermediaries remain vague under Canadian law. We observed in the foregoing section that similar comments have been made regarding U.S case law. The same response can be made here, that is, that the contended “vagueness” could be regarded a sort of flexibility. Indeed courts may have an interest in defining general principles to be outlined on a case-by-case basis, especially when dealing with new technologies.

Ultimately, I appreciate that, as judged by Justice Binnie the judicial authority cannot reasonably replace the lawmaker, however, I do no consider that the judicial authority would have overlapped with the prerogatives of the lawmaker by enforcing a notice and take down procedure for Internet intermediaries. I advocate that, Canadian copyright law pre-Bill C-11 was able to keep up with the digital age and to address the liability of Internet intermediaries while maintaining a balance the interests of content owners and innovators.

2. Fair dealing under Canadian law

The purpose of this section is not to study in details the fair dealing doctrine but to broadly stress its elements and its evolution through Canadian case law. This will permit to compare the fair dealing and fair use doctrines and ultimately to analyze under which conditions Internet intermediaries in Canada can raise this defense to escape liability.

a. Fair dealing under Canadian doctrine

Fair dealing is a statutory exception to copyright infringement. It is a defense against copyright infringement claim. The plaintiff therefore has the burden of establishing infringement with the burden of proof upon the defendant. To qualify under the fair dealing exception, the dealing must first be for a purpose listed in sections 29, 29.1 or 29.2 of the Copyright Act (research, private study, criticism, review or news

---

See Section III.A.
reporting), and the dealing must also be fair. It is usually contended that Canada’s fair dealing provisions do not provide an open ended defense for dealing that can be considered as “fair”; the fairness of a particular dealing is relevant to the extent that it is undertaken for the limited specific purpose. According to Michael Geist, this situation is changing due to the expansive approach by the Supreme Court of Canada.

b. Application of the doctrine of fair dealing by the Supreme Court of Canada

The first stage of faire dealing evolution: CCH

The 2004 ruling by the Supreme Court of Canada in CCH has interpreted extensively the concept of fair dealing in Canada. In considering fair dealing the Court observes:

144 Research or private study
s.29 Fair dealing for the purpose of research or private study does not infringe copyright.

Criticism or review
s.29.1 Fair dealing for the purpose of criticism or review does not infringe copyright if the following are mentioned:
(a) the source; and
(b) if given in the source, the name of the
(i) author, in the case of a work,
(ii) performer, in the case of a performer’s performance,
(iii) maker, in the case of a sound recording, or
(iv) broadcaster, in the case of a communication signal.

News reporting
s.29.2 Fair dealing for the purpose of news reporting does not infringe copyright if the following are mentioned:
(a) the source; and
(b) if given in the source, the name of the
(i) author, in the case of a work,
(ii) performer, in the case of a performer’s performance,
(iii) maker, in the case of a sound recording, or
(iv) broadcaster, in the case of a communication signal.

146 Michael Geist, Has Canada Effectively Shifted from Fair Dealing to Fair use?, (July 13, 2012), online <http://www.michaelgeist.ca/content/view/6589/125/>.
147 Supra note 110.
“It is important to clarify some general considerations about exceptions to copyright infringement. Procedurally, a defendant is required to prove that his or her dealing with a work has been fair; however, the fair dealing exception is perhaps more properly understood as an integral part of the Copyright Act than simply a defense. Any act falling within the fair dealing exception will not be an infringement of copyright. The fair dealing exception, like other exceptions in the Copyright Act, is a user’s right. In order to maintain the proper balance between the rights of a copyright owner and users’ interests, it must not be interpreted restrictively”.  

Some authors have seen in CCH, a "a liberal approach to the enumerated purposes of the dealing" and concluded that the Supreme Court has made fair dealing more flexible, reducing the gap between this provision and U.S fair use.  

Scholars and practitioners were waiting for the Supreme Court case law post CCH to assess whether the alleged liberal approach of fair dealing will be confirmed or rejected.  

**The Supreme Court decisions of July 2012**  

In July 12, 2012, The Supreme Court of Canada released five copyright decisions clarifying the scope of fair dealing under Canadian law. Before analyzing the July

---

148 Ibid. at 48.  
12, 2012 decisions, dubbed the "Copyright Pentalogy", we need to briefly recall the difference between U.S fair use and Canadian fair dealing pre-CCH and pre-Copyright Pentalogy cases. Under U.S fair use the list of qualifying categories or purposes is illustrative rather than exhaustive. Put it differently, U.S statutory provisions distinguish purposes that may qualify as fair use, but accepts that the courts may add new purposes on a case-by-case basis. “The key to fair use lies not in the purposes but rather in the analysis that follows over whether the particular use is fair”.  

As seen earlier in this paper, the flexibility of U.S fair use can be regarded as positive as it opens the door to new innovation that the executive and legislature power might not foresee when drafting the law.

In contrast, Canadian fair use two-stage analysis (pre-CCH and pre-Copyright Pentalogy) has been considered, as exhaustive for it must qualify for one of the enumerated fair dealing purposes.

Copyright Pentagoly decisions have been viewed as shifting fair dealing into a fair use doctrine. In fact, in these decisions, the Supreme Court has confirmed that fair dealing is a user’s right that shall be interpreted in an open and liberal manner. For instance, in the Alberta v Access Copyright case, the court regarded instruction (i.e. teaching) as within the research and private study categories, observing that such activities facilitate students’ research and private study. Moreover, the court reframed private study as personal study that can take place anywhere or with anyone. In the Socan v. Bell case, the Court ruled that Online

---

152 Supra note 110.  
153 Ibid.  
154 Supra note 150.  
155 Ibid.
"previews" of songs were held to constitute "research" for the purposes of "fair dealing", and, as such, are not a compensable activity, in other words that no license is required, and no fee/royalty needs to be paid, for such previews. The decision also emphasizes that there is a "low threshold" for assessing whether a particular activity falls within the ambit of the fair dealing categories (research, private study, criticism, review, news reporting and, once the provisions of the Copyright Modernization Act (Bill C-11) are proclaimed into force, parody, satire and education).  

Some authors have seen in these decisions a “robust and expansive interpretation of "fair dealing"” that might encourage more aggressive assertions of rights to use copyrighted material without obtaining permission from or making payments to rights-owners.  

It seems that Internet intermediaries in Canada may take guidance from these decisions. For instance search engines may, like in the U.S, be entitled to invoke fair dealing to escape liability from providing thumbnails of photos, snippets of videos and other "fragmentary" uses of copyrighted works.

The Copyright Pentagoly cases especially the SOCAN v Bell decision and the Alberta v Access Copyright decisions seem to endorse an expansive interpretation of fair dealing. As will be noted below, this has important implications for a variety of actors especially for Internet intermediaries. According to Michael Geist, the Supreme Court has delivered in the Copyright Pentagoly cases a vision of copyright that emphasizes, user rights, and innovation. Bob Tarantino, considers that “the Pentalogy and The Copyright Modernization Act represent seismic changes in Canadian copyright law” affecting significantly the balance between users, content

---

156 Ibid., at para 27, “In mandating a generous interpretation of the fair dealing purposes, including "research", the Court in CCH created a relatively low threshold for the first step so that the analytical heavy-hitting is done in determining whether the dealing was fair”.

157 Supra note 151.

158 Supra note 80.

159 Supra note 150.

160 Supra note 146.
owners and innovators. As already mentioned, this paper focuses on the balance between owners and innovators while acknowledging that users may be part of the equation.

Having said that, I apprehend that the Supreme Court had to clarify the meaning of fair dealing under Canadian law. In doing so, it had the choice to reiterate its pre-\textit{CCH} case law that is to say a narrow interpretation of fair dealing, which would have protected content owners but would have chilled innovation and affected negatively end users. The Supreme Court had also the possibility to align fair dealing with fair use, and in doing so taking the risk to affect the right of content owners but in the same time promoting innovation and user rights. It appears to me that the Supreme Court found the right balance between the interest of content providers and Internet intermediaries for any copyright rule dealing with new technology has to been flexible, liberal and open-ended. Indeed as already discussed in this essay, the executive and legislature powers might not foresee some innovations when drafting a specific law. They should therefore provide general standards that will be applied and delimited by courts on a case-by-case basis.

Besides, \textit{CCH}\textsuperscript{162} and the Copyright Pentalogy cases\textsuperscript{163} demonstrate that courts in Canada have been able to keep up with the development of new technologies. Even if it is too early to assess the scope of the Copyright Pentalogy decisions, I believe that these decisions will enable Internet intermediaries to invoke the fair dealing defense to escape liability, especially the user generated content for content uploaded on their website and search engines for framing and hyperlinking.

Through the study of U.S and Canadian copyright law pertaining to the liability of Internet intermediaries, we observed that both laws were overall able to cope with the development of new technologies. In fact U.S and Canadian law were able to

\textsuperscript{161} Supra note 151.
\textsuperscript{162} Supra note 110.
\textsuperscript{163} Supra note 150.
address new copyright issues in the cloud while maintaining a balance between content owners and innovators. Although there is no apparent judicial void in either country, new copyright drafts have been proposed in U.S and Canada.

In the following section, we will analyze these laws and assess whether they were indispensable.

SOPA AND BILL C-11: THE SOLUTION TO ADDRESS THE LIABILITY OF INTERNET INTERMEDIARIES WHILE MAINTAINING A BALANCED COPYRIGHT LAW?

In almost the same time, lawmakers in U.S and Canada proposed new copyright laws to supposedly deal with the issues of copyright enforcement in the cloud. We propose in this section to consider whether these laws preserve the balance between rightholders and Internet intermediaries and ultimately whether these are needed.

A. THE IMPACT OF SOPA ON THE LIABILITY OF INTERNET INTERMEDIARIES

As it be will explain further in this section, the Stop Online Piracy Act (“SOPA”) is primarily an intermediary liability bill even if there are many other provisions in the bill. For the purpose of the present essay, solely the provisions related to the liability of Internet intermediaries will be approached.

1. Overview of SOPA

On October 26, 2011, SOPA was introduced in the United States House of Representative along with Bill to the Protect IP Act introduced in the U.S Senate in May 2011. Both bills purport to tackle the issue of piracy in the cloud, especially to expand the ability of U.S. law enforcement to fight online trafficking in copyrighted intellectual property and counterfeit goods. 164

The bill was intended to address the rogue websites that are dedicated to infringing U.S intellectual property rights, especially streaming sites as Megaupload as well as websites that offer online counterfeit good such as pharmaceuticals goods. Although, as discussed in this paper, there is no common agreement in United States that piracy, counterfeiting, and copyright infringement are severe issues.

2. Impact of SOPA AND PIPA on Cloud Intermediaries

The rogue sites targeted by SOPA, whether foreign or domestic, use intermediaries to engage in United State’s transactions. They have registered domain names and use ISP’s to connect to the Internet. They are also accessible via search engines such as Google and Bing and may generate revenue through advertising, requiring the use of online advertisers and advertising brokers such as Google AdSense. Finally, many of them rely on credit card payment systems such as Visa or online payment systems such as PayPal to sell their goods.

Yet, SOPA provides United States government and content providers more power to use Internet intermediaries to shut down or restrict websites that deal in counterfeit, pirated, or infringing material. SOPA would also give government officials new powers to target Domain Name System (DNS) registrants and web site owners and to take any appropriate action to close down domains. Under this law, The United States government would be entitled to require ISPs, Search Engines and any other Internet intermediaries to help in stopping access to, blocking, or shutting down infringing accounts. Moreover, SOPA would gives immunity to intermediaries that voluntarily block access or cut off service to rogue websites. Finally, SOPA provides for additional criminal penalties, comprising illegal "public performance by means of digital transmission," and other systems of trafficking in counterfeit materials.

3. Impact of SOPA/PIPA on Internet intermediaries: a Bill that will chill innovation by weakening safe harbors protections

Opponents fiercely opposed the bill, arguing that such bill amount to censorship, that it will disrupt Internet and impose excessive burdens on Internet/cloud intermediaries.

The Electronic Frontier Foundation ("EFF") warned that such bill might have a chilling effect of Internet intermediaries, especially on user Generated Content sites as YouTube and that websites Flickr will likely shut down if the bill becomes law. Policy analysts for New America Foundation say this legislation would enable law enforcement to take down an entire domain due to something posted on a single blog. Additional concerns for Internet intermediaries include the impact on common Internet functions such as hyperlinking from one site to another or accessing data from the cloud. EFF argued the bill would ban linking to sites deemed offending, even in search results.

SOPA seems to supplement the Digital Millennium Copyright Act’s (DMCA) notice and takedown and safe-harbor provisions and to extend them to the Internet intermediaries, in addition to the website hosts of infringing content.

In fact, as here above stated, the DMCA provides a "safe harbor" for websites that host content. Under DMCA provisions, copyright owners detecting that a site was hosting infringing content are required to request the site to remove the infringing material within a specific deadline. SOPA would have circumvented this "safe

harbor" provision by placing the responsibility for detecting and regulating infringement onto the cloud website/provider itself, and by allowing courts to block access to rogue websites”. 169

So far, and following the massive opposition of technology companies, the U.S Congress has halted the debate on SOPA /PIPA. 170

It seems to me that the SOPA episode shows an increasing pressure of rightholders on government to enact laws that would expend the liability of cloud providers. In fact, SOPA/PIPA bills are on example of the attempt to drive the liability of Internet intermediaries to the next level, i.e. to the proactive level. As mentioned Internet intermediaries are required under SOPA to detect and regulate infringing contents whereas they are solely required to take down infringing content following the reception of a notice from rightholders under DMCA rules. SOPA would have eventually allowed an entire site to be shut down or blocked, rather than just the infringing content, and it does not allow for fair use of copyrighted content.

In light of these elements, SOPA would have seriously affected the balance between content owner and innovators, particularly Internet intermediaries. Moreover, It would have chilled innovation, as it would have imposed a heavy liability on Internet intermediaries. After all, U.S congress did not enact SOPA for it may have realized the risk on innovation.

A cost-effectiveness analysis of copyright law pre-SOPA would show that current copyright law is able to address copyright liability issues in the cloud while maintaining a proper balance between content owners and innovators, whereas SOPA would have affected significantly this balance in favor of content owners. In light of the above, SOPA was not necessary and even dangerous.

Now, we propose to consider whether in Canada Bill C-11 was necessary and whether it addressed copyright liability of Internet intermediaries while maintaining a balance between rightholders and innovators.

B. THE EFFECTS OF BILL C-11 ON THE LIABILITY OF INTERNET INTERMEDIARIES

In the 2010 Speech from the Throne, the Government of Canada restated its promise to consolidating laws governing intellectual property and copyright so as to "to encourage new ideas and protect the rights of Canadians whose research, development and artistic creativity contribute to Canada’s prosperity." The bill allegedly follows through on this commitment. 171 On June 29, 2012, the government announced that the Copyright Modernization Act, Bill C-11, had received royal assent and that Canada has now modern copyright regime, which will play a critical role in protecting and creating jobs in Canada’s digital economy. The government contended that he has delivered on its commitment to seek swift passage of modernized copyright legislation in a way that strikes the right balance between the needs of creators and users. 172

In the following section we propose to consider whether Bill C-11 has vindicated a balance between the needs of creators and innovators.

1. Bill C-11 confirmed the safe harbors recognized by case law

Bill C-11 contains five exceptions intended to protect Internet intermediaries from liability: the network services shelter (s. 31.1, Copyright Act), which will apply to both rights of communication and reproduction, and will shield ‘conduits’ that will only provide the means of telecommunication and reproduction, but not participate

172 Ibid.
in its intent; the caching shelter (s. 31.1(3), Copyright Act), which permits lawful industry practices of using technology to cache data to escape liability from infringement; the hosting shelter (s. 31.1(5), Copyright Act), which allows emerging technologies like cloud providers to avoid liability if their purpose is to enable the telecommunication of a work, and provided that there is no awareness or intent to infringe; and finally the information location tool shelter (s. 41.27, Copyright Act), which regards intermediaries not liable if they merely provide access to infringing material, as long as this is done automatically by the technology involved, for the purpose of providing the information, and provided that there is no action/modification of the material by the intermediary.

As a preliminary comment, it seems that these five exceptions are not revolutionary considering that Canadian courts have addressed pretty extensively the liability of Internet intermediaries despite the absence of statutory provisions like the DMCA. One may therefore question whether these statutory exceptions were necessary.

We now propose to examine the hosting safe harbor provision in order to consider whether this provision is different from the hosting safe harbor already recognized by courts.

---

173 31.1 (1) “A person who, in providing services related to the operation of the Internet or another digital network, provides any means for the telecommunication or the reproduction of a work or other subject-matter through the Internet or that other network does not, solely by reason of providing those means, infringe copyright in that work or other subject-matter”.

174 31.1 (3) "Subject to subsection (4), a person referred to in subsection (1) who caches the work or other subject-matter, or does any similar act in relation to it, to make the telecommunication more efficient does not, by virtue of that act alone, infringe copyright in the work or other subject-matter”.

175 31.1 (5) “Subject to subsection (6), a person who, for the purpose of allowing the telecommunication of a work or other subject-matter through the Internet or another digital network, provides digital memory in which another person stores the work or other subject-matter does not, by virtue of that act alone, infringe copyright in the work or other subject-matter”.

176 41.27 (1) “In any proceedings for infringement of copyright, the owner of the copyright in a work or other subject-matter is not entitled to any remedy other than an injunction against a provider of an information location tool that is found to have infringed copyright by making a reproduction of the work or other subject-matter or by communicating that reproduction to the public by telecommunication”.

60
The Hosting safe harbor (s.31.1 (5))

"Subject to subsection (6), a person who, for the purpose of allowing the telecommunication of a work or other subject-matter through the Internet or another digital network, provides digital memory in which another person stores the work or other subject-matter does not, by virtue of that act alone, infringe copyright in the work or other subject-matter".

This shelter allows hosting providers to escape liability if their purpose is to allow the communication of a work and if they are not aware or they do no intend to infringe third party IP rights.

Is this a new provision? We observed earlier in this paper that the Supreme Court acknowledged in SOCAN 177 a principle of immunity for host providers and reassessed the presumption of lawful authorization discussed in CCH, concluding that “knowledge that someone might be using neutral technology to violate copyright is not necessarily sufficient to constitute authorization, which requires a demonstration that the defendant did give approval to, sanction, permit, favor, encourage, the infringing conduct”. 178

Sections 31.1.5 and 31.1.6 provide the same immunity for host providers provided that they are neutral, that is, they do not participate to the illicit act per se. The statutory hosting safe harbor provisioned under Sections 31.1.5 and 31.1.6 is thus similar to the judicial hosting safe harbor provided in SOCAN.

As already discussed, section 31.1.5 encompasses hosting services, including cloud services. The issue is that it’s unclear whether the transmission of the stored

---

177 Supra note 116.
178 Supra note 110.
data/content is subject to a similar shield. The question raised by ISP’s 179 is that, as drafted, Bill C-11 allows cloud providers to host remote storage of personal time-shifted and format-shifted copies, but it is vague as regards the retrieval of those copies.

During the parliamentary discussions, a motion to amend this provision was rejected by the “Conservatives” who contended that nothing in the bill prevented a business-to-business arrangement between broadcasters and cloud providers. Given the fact that the provision remains unchanged, it will solely cover the hosting but not the transmission of the hosted data/programs. Cloud providers offering a network-based digital video recorder (DVR) stored at the provider’s central location rather than at the consumer’s private home, (Network Based Personal Video Recording (PVR’s)), shall therefore get the prior approval of broadcasters before transmitting hosted programs acquired legally by end-users. If no agreement is reached between cloud storage providers and broadcasters, the risk is left with companies who introduce cloud-based services in Canada.

Ultimately, with respect to the liability of hosting/cloud providers, the lawmaker confirmed the immunity granted by the judicial authority but rejected any clarification concerning the conditions of such immunity, contending that the bill did not prevent a business-to-business arrangement. We can appreciate that the lawmaker preferred to set general standards but did not want to stipulate detailed rules that may affect innovation. However, we can question whether this statutory immunity was necessary for identical safe harbor was recognized by case law.

The Supreme Court may have clarified the regime of transmission of hosted programs to end-users. Indeed in ESA/C v SOCAN,180 the Supreme Court ruled:

179 Michael Geist, Does Bill C-11 Create Barriers to Network PVRs and Cloud Services in Canada?, (March 21, 2012), online: <http://www.michaelgeist.ca/content/view/6385/125/>.
180 Supra note 150.
"The principle of technological neutrality requires that, absent evidence of Parliamentary intent to the contrary, we interpret the Copyright Act in a way that avoids imposing an additional layer of protections and fees based solely on the method of delivery of the work to the end user. To do otherwise would effectively impose a gratuitous cost for the use of more efficient, Internet-based technologies". 181

(...)

In our view, the Board improperly concluded that the Internet delivery of copies of video games containing musical works amounts to "communicating" the works to the public. This view is evidenced by the legislative history of the Copyright Act, which demonstrates that the right to "communicate" is historically connected to the right to perform a work and not the right to reproduce permanent copies of the work.

In light of the principle of technological neutrality and the definition of the term "communicating" a work to the public, the Supreme Court drew a distinction between online transmissions, which are "reproduction"-like (e.g., downloads) and online transmissions, which are "performance/communication"-like (e.g., streaming), and concluded that transmissions so categorized are only entitled to get compensated for one tariff. 182 Following this decision, it seems that cloud providers offering DVR do not need to get the prior approval of broadcasters before transmitting hosted programs acquired legally by end-users and that they are entitled to provide such transmission at not additional costs.

At the end of the day, bill C-11 solely confirmed the immunity granted by the judicial authority without describing the conditions of such immunity. The Supreme Court had to clarify these conditions in ESA/C v SOCAN.

181 Ibid. at 9.
182 Ibid at 28; supra note 151.
2. The redundancy of the user generated content provision?

Bill C-11 encompasses a new exception that would explicitly allow individuals to create new user generated content. According to the government this provision will “permit the use of legitimately acquired material in user-generated content created for non commercial purposes. It has been contended that, “this applies only to creations that do not affect the market for the original material, and that examples could include making a home video of your friends and family dancing to a popular song and posting it online, or creating a ‘mash-up’ of video clips”. ¹⁸³

Though this provision seems to be pretty original for end-users, from an Internet intermediary perspective, one may question whether such provision applies only to user or also to user generated content providers such as Youtube? Actually section 29.21 (1) expressly allows the user generating the content to authorize an intermediary to disseminate it:

“Its not an infringement of copyright for an individual to use an existing work or other subject matter or copy one, which has been published or otherwise made available to the public, in the creation of a new work or _other subject-matter in which copyright subsists _and for the individual — or, with the individual’s authorization, a member of their household _— to use the new work or other subject-matter _or to authorize an intermediary to disseminate it (...).”

Internet intermediaries embraced this provision. For instance, Google contended that Bill C-11’s protections for non-commercial, user-generated content will be important to creative communities in Canada. Google also advocated that it

supported, in general, the Internet intermediary safe harbor provisions in Bill C-11 contending that one of the critical issues the government has identified in this bill is ensuring that copyright law doesn’t hinder the development of cloud computing in Canada.\footnote{Parliament of Canada, (March 1st, 2012), online: Open Parliament <http://openparliament.ca/committees/bill-c-11-41-1/41-1-6/jacob-glick-1/only/>.}

The UGC provision seems to clarify the liability of user generated content providers. Yet, some have questioned whether the UGC provision could have made more sense as an express element of the Act’s “fair dealing” exception?\footnote{Margot Paterson, The Copyright Modernization Act and UGC, (June 2012), online: Fraser Milner Casgrain LLP <http://www.fmc-law.com/upload/en/publications/2012/0612_The_Copyright_Modernization_Act_and_UGC.pdf>.} Indeed Bill C-11 already expanded fair dealing to include education, satire and parody as acceptable purposes. Besides, as seen in this paper, the Supreme Court interpreted pretty extensively the definition of fair dealing in the Copyright Pentalogy decisions.\footnote{Supra note 150.} Some practitioners (M. Paterson) feel that UGC has a lot in common with satire and parody, as a new use of existing content. Moreover, it has been argued that there are already established tests or standards to judge whether dealing is fair or not, potentially giving more certainty in determining which UGC is and is not “fair”.

At the end of the day, the user generated content provision might be redundant with the fair dealing doctrine.

3. **The enablement right do not target Internet intermediaries**

Section 27 (2.3) of Bill C-11 would create an “Enablement Right” clause.

This clause states:

“It’s an infringement of copyright for a person to provide, by means of the Internet or another digital network, a service
that the person knows or should have known is designed primarily to enable acts of copyright infringement if an actual infringement of copyright occurs by means of the Internet or another digital network as a result of the use of that service.”

Section 27 (2.4) explains the factors that will be taken into account so as determine whether a person/service enabled a copyright infringement:

“(2.4) In determining whether a person has infringed copyright under subsection (2.3), the court may consider:

(a) Whether the person expressly or implicitly marketed or promoted the service as one that could be used to enable acts of copyright infringement
(b) whether the person had knowledge that the service was used to enable a significant number of acts of copyright infringement;
(c) whether the service has significant uses other than to enable acts of copyright infringement
(d) the person’s ability, as part of providing the service, to limit acts of copyright infringement, and any action taken by the person to do so
(e) any benefits the person received as a result of enabling the acts of copyright infringement; and
(f) the economic viability of the provision of the service if it were not used to enable acts of copyright infringement”.

This bill will, according to the government, gives copyright owners the tools to pursue those who willfully and knowingly enable copyright infringement online,
such as operators of websites that facilitate illegal file sharing.\textsuperscript{187}

Section 27 (2.3) focuses on sites that are “designed primarily” for the purposes of enabling, and consequently, intent and knowledge are central factors in finding an illegal website an enabler. It seems that it will allow copyright owners to sue illegal peer-to-peer file sharing sites.\textsuperscript{188}

Some authors were concerned that this provision might be used to target Internet intermediaries such as Youtube.\textsuperscript{189} In an Osgoode Professional Development’s seminar, titled “Understanding Bill C-11: The Copyright Modernization Act.”,\textsuperscript{190} it has been argued that there should not be any concern that these provisions would also target legal Internet intermediaries, for that C-11 created five “safe harbors” for Internet intermediaries. It has been contended that all together, these exceptions were deemed to be the safety net protecting and legal or “good” ISPs versus the illegal or the “bad” enablers. I believe that it was not the intention of the lawmaker to target Internet intermediaries for it would not make sense to target these and provide in the same time safe harbors. Besides section 27 (2.4) provide detailed factors that should be taken into account so as to determine whether a provider enabled copyright infringement. These detailed factors should help courts distinguish between bad providers such as and good Internet providers such as Youtube, Google, Facebook, Icloud and Bell.

As noted, the government contended that this provision would give copyright owners the tools to pursue those who willfully and knowingly enable copyright infringement online, such as operators of websites that facilitate illegal file sharing. Michael Geist rightfully observed that “just as there are questions whether SOPA is even needed in the U.S” for the current is effective in dealing with online piracy, “the

\textsuperscript{187} Ibid.
\textsuperscript{189} Michael Geist, The Behind---the---Scenes Campaign to Bring SOPA to Canada, (January 23, 2012), online: Michael Geist,< http://www.michaelgeist.ca/content/view/6257/125/>.  
\textsuperscript{190} Infra note 195.
same is true with the enabler provision in Bill C-11, given that the music industry is already suing IsoHunt,\textsuperscript{191} the Canadian based torrent search site, using current law”\textsuperscript{192}

In light of the above, it seems that the enablement right provision might be redundant with current case law dealing with P2P copyright infringement. As noticed by Michael Geist, we can legitimately question whether the enabler provision in bill C-11 was ever needed.

4. The “notice and notice” regime v. the “notice and take down” regime

In \textit{SOCAN},\textsuperscript{193} we observed that the Supreme Court established safe harbor immunities for Internet intermediaries. We also remarked that the conditions of such immunity were not explained, the Supreme Court referring to the notice and take down procedure provisioned under European law but ruling that courts do not have the authority to implement such procedure. In Bill C-11, the lawmaker did not follow the suggestion made by justice Binnie in \textit{SOCAN}.\textsuperscript{194} Instead it enacted a notice and notice regime.

In this section, we propose to evaluate whether a notice and notice regime existed pre-bill C-11. We will also compare the notice and notice regime with the notice and take down regime applied in the U.S. This comparison will enable us to assess whether the notice and notice regime can replace the notice and take down regime.

\textbf{a. Overview of the “Notice and Notice” Regime}

Under the statutory notice and notice regime an ISP receives a notice from a rightholder that a subscriber might be infringing copyright, which it then forwards

\textsuperscript{191} See Label complaint against Isohunt filed before the Supreme Court of British Columbia in May 12, 2010, \url{http://www.scribd.com/doc/83175814/isohunt-scbc}

\textsuperscript{192} \textit{Supra} note 189.

\textsuperscript{193} \textit{Supra} note 116.

\textsuperscript{194} \textit{Ibid}.
to the subscriber. The identity of the subscriber may then be released following a court order, but the ISP will not be penalized for operating as a neutral intermediary. ISP’s will be required to forward a notice of infringement received from right holders to the customer. 195 This regime essentially translates into law a voluntary deal made a decade ago between the biggest Canadian ISP’s – Bell, Shaw, Rogers, etc. – and the music industry so as to perform such a function – for free. The fact that ISP's have played such a role on behalf of copyright claimants is hidden in plain sight in their “Terms of Service agreements”. 196

One can question whether a statutory notice and notice regime was necessary when such regime was applied de facto by major ISP’s. The eventual reason behind this statutory recognition would be to compel all ISP’s to apply the notice and notice regime and not solely ISP’s that entered a voluntary agreement with the content industry. The appropriateness of this statutory provision will be discussed later in this section.

b. Is the Notice and Notice Regime comparable to the notice and take down regime?

The notice and notice regime has been maintained in Canada for charter of rights reasons 197. Some concerns have been raised that a notice and take down regime could create incentive for internet intermediaries to remove rapidly alleged infringing content without serious evidence of actual copyright infringement which could have a potential chilling effect on free expression. 198


198 Michael Geist, Canada’s, Notice and notice, (16 February 2007), online: <p2pnet.net>.
Besides, the issue with the notice and take down regime lies in the fact that it would be ineffective in preventing P2P file sharing for that notice and take down applies solely to content posted online. It is not an efficient tool against files shared on P2P for the files shared are not located online but on the hard drive of individuals involved in file sharing. It has also to be mentioned that the Canadian lawmaker did not want to import in Canada the graduate response experienced in France and the United Kingdom for charter rights reasons as this approach would eventually involve consumers being disconnected from the Internet.

The contended issue with the notice and take down regime is the potential chilling effect on freedom of speech. It has been claimed that, in order to avoid any risk of litigation, Internet intermediaries in the U.S tend to remove or block access to notified infringing content, without taking the time to invest in further details the veracity of the notification. Internet intermediaries are thus pressed to a kind of voluntary censorship although they do not have the authority of a court or knowledge of the legal defenses that can be raised against such notification, e.g. fair use, claim over public domain material and notices in unclear form.

These criticisms do not seem to be justified at least with respect to the U.S DMCA for it has built various safeguards to discourage arbitrary notice and take down. In fact, any takedown notice must be notified to the content provider, who then has the chance to protest that the material should not be removed, in such case it shall be ‘put back’ by the Internet intermediary. If the original “notifier” then continues to dispute the legality of the material, and the content provider to confirm it, the dispute must be redirected to the courts. While dispute is in progress, the Internet


intermediary is shielded so as to keep the content posted, free from liability, even if at the end of the day a court rules that the content was illicit. This system of notices and counter-notices principally builds on a common understanding between copyright holders and Internet intermediaries, and symbolizes a serious attempt to provide a balanced solution between rightholders and innovators. 202

The DMCA also provided firm rules that the person requesting a take down must appropriately identify himself or herself as the rights-holder with locus to call take down and indicates details allowing illicit content to be clearly located. Both rules seem to deter false complaints and help the receiver of the notice to comply. Besides there are severe penalties for any person making a false allegation as to infringement (s 512 (f)), which have, been enforced by the U.S courts. 203

In light of the above, it seems that the criticisms against the U.S notice and take down regime are not grounded for this regime seems to have an evident deterrent function with respect to eventual abuses. 204

In addition, the notice and notice regime may not be relevant to address infringing contents hosted by Internet intermediaries. For instance, when contents (video, music) are uploaded online on Youtube, it may be difficult for Youtube to identify precisely the user who posted/uploaded the infringing video. Assuming that Youtube can identify the user, and forward him/her a notification of infringement, this will not prevent other users to access and view the infringing video uploaded on Youtube Website.

Some authors have therefore suggested to associate the ‘notice and notice’ regime with the ‘notice and take down notice’ to deal with P2P issues:

‘Notice and notice’ and ‘notice and takedown’ are complementary methods of dealing with online file sharing. They have often been portrayed as mutually exclusive processes. They

202 Supra note 37, at 13.
204 Supra note 37, pp.13.
are not. Notice and notice may be somewhat useful in dealing with P2P file sharing; notice and takedown is necessary to deal with files that are hosted by the ISP. 205

Perceiving the pertinence of such association, Hong Kong has proposed a merged model, which in general entails forwarding notices from the copyright holder to the alleged infringer and taking down the infringing material. 206

At the end of the day Canada lawmaker had the opportunity to implement an hybrid system taking full advantage of both regimes. Instead it preferred to make binding private agreements signed between content providers and ISP’s by implementing a statutory notice and notice regime.

As comprehended in this section, Bill C-11 endorsed judicial safe harbors recognized by courts. Although most of the provisions discussed here above might not have been necessary, arguably they still clarify copyright law without being too detailed. This may increase legal certainty.

If we briefly compare SOPA and Bill C-11 we can note that SOPA would have increased significantly the liability of Internet intermediaries. It would have weakened safe harbors protections and ipso facto chilled innovation. On the other hand, Bill C-11 upheld and clarified current case law without imposing new strong liability on Internet intermediaries. Contrary to SOPA, Bill C-11 seems to have maintained the balance between content owners and Internet intermediaries.

CONCLUSION

Today, they are more questions than answers about how intellectual property protection shall evolve to adapt to Internet and cloud services. This ambiguity exists because it is only the very beginning of this technological shift. It is very difficult to predict how cloud computing will be used to foresee the legal implications of these uses. The essential question then is whether the lawmaker should provide detailed legal regulation *ex ante* or should instead enact general principles that will be detailed by courts. The development of new technologies is so fast that it is almost impossible for the lawmaker to enact statutory rules keeping up with such rapid growth.

As seen in this paper, current copyright laws (in relation with the liability of Internet the liability) either in the U.S or in Canada deal efficiently with copyright issues in the cloud while maintaining a proper balance between content owners and Internet intermediaries. Their strength is in what is perceived as a weakness, that is general copyright standards that were not initially intended to deal with copyright infringement in the cloud. In order to cope with the development of new technologies, these standards have been detailed by courts on a case-by-case basis.

We have also seen that SOPA is dangerous as it would have implemented rules that may have affected seriously the balance between rightholders and Internet intermediaries and ultimately chilled innovation whereas bill C-11 upheld and sometimes clarified current case law and maintained the balance between content owners and Internet intermediaries. It seems to me that the ultimate solution would be to maintain current copyright laws in U.S and Canada and to let the courts address new copyright liabilities issues in the cloud on a case-by-case basis. The lawmaker may intervene so as to enact new statutory law only to upheld and clarify previous case law as Bill C-11 did.
Finally, one has to mention that here is a new trend in the cloud, that is, the signature of private agreements between the content industry and Internet intermediaries. One may question whether this could be the future of cloud regulation, i.e. a market where an auto-regulation can take place without the intervention of the legislature or the courts? Should the lawmaker or the courts act to regulate these private agreements *ex ante* or *ex post*? As seen in this essay, Bill C-11 upheld private agreements signed between content providers and ISP’s by implementing a statutory notice and notice regime. This is out of the scope of the present study but it might be an interesting topic to be considered by scholars.

*  *

*
BIBLIOGRAPHY

Books


Journal Articles


Statutes


Copyright Act, (R.S.C., 1985, c. C-42), ss. 27, 29

Copyright Modernization Act, Bill C-11, ss 31.1, 41.27,

Canadian Cases

Alberta (Education) v. Canadian Copyright Licensing Agency (Access Copyright), (2012) SCC 37.


U.S Cases


A.V. v. iParadigms, LLC, 562 F.3d 630 (4th Cir. Apr. 16, 2009).

Capitol Records, Inc. v. MP3tunes, LLC, 07 Civ. 9931.
Cartoon Network, LP v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008).

Gershwin Publishing Corp. v. Columbia Artists Management, Inc. 443 F.2d1159, 1161 (2d Cir. 1971).


MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993).


Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th. Cir. 2007).


**Electronic Sources**


Michael Geist, *Canada’s, Notice and notice*, (16 February 2007), online: <p2pnet.net>.

Michael Geist, *All the News That’s Fit To Post and Link: Federal Court Clears Up Legal Risks*, (July 03, 2012), online: <http://www.michaelgeist.ca/content/view/6573/135/>.

Michael Geist, *Has Canada Effectively Shifted from Fair Dealing to Fair use?*, (July 13, 2012), online <http://www.michaelgeist.ca/content/view/6589/125/>.
Michael Geist, *Does Bill C-11 Create Barriers to Network PVRs and Cloud Services in Canada?*, (March 21, 2012), online: <http://www.michaelgeist.ca/content/view/6385/125/>.


80