United States Response
To Questionnaire Concerning Copyright and Related Rights in the "Cloud" Environment
ALAI 2012 Kyoto

By June M. Besek, Philippa S. Loengard and Idara Udofia[1]

Note: The full text of the provisions of the U.S. Copyright Act referred to in these responses is available at http://www.copyright.gov/title17/. For copies of referenced cases, we suggest you visit either http://www.findlaw.com/casecode/ or http://www.law.cornell.edu/federal/.

Session 1
－Developments of New Platforms

1) How would you define "The Cloud" in your country?

There is no universally recognized definition of "the Cloud." The answers to these survey questions could vary depending on how one defines "the Cloud." For the purposes of these responses, we will work from the definition of "cloud computing" provided by the National Institute of Standards and Technology, a division of the United States Department of Commerce:

> Cloud computing is a model for enabling ubiquitous, 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.

Evelyn Brown, *Two New Publications Provide a Cloud Computing Standards Roadmap and Reference Architecture*, Nat'l Inst. of Standards and Tech. (Sept. 30, 2011) http://www.nist.gov/itl/csd/cloud-091311.cfm.

In simpler terms, it is a way personal devices can access software or other resources available on a network of servers and internet connections.[2] Users can access these resources through an internet connection rather than having to store the information on their individual devices. Thus, we understand "the Cloud" to mean remote storage and associated services offering access, storage, and communication of the remotely stored content.

2) Is exploitation of works, performances, sound recordings and so on generally considered to relate to the Cloud?

---

[1] June M. Besek is the Executive Director of the Kernochan Center for Law, Media and the Arts at Columbia Law School. Philippa Loengard is the Assistant Director of the Kernochan Center. Idara Udofia is a member of the Columbia Law School Class of 2013. The authors thank Jane C. Ginsburg, the Morton L. Janklow Professor of Literary and Artistic Property Law at Columbia Law School, for her review and comments.

[2] BNET S@VVY TECH GLOSSARY, http://www.neahin.org/bnetsavvy/tech-glossary/?first_letter=c (last visited June 28, 2012).

Some types of exploitation do relate to the Cloud, but works/performances are still commonly exploited by other means as well.

As discussed below, the music industry has encountered great benefits and challenges from the existence of the Cloud. Internet storage has provided increased venues for the legitimate dissemination of music, but has also enabled greater illicit sharing of music. Many professionals have used the Cloud to allow their colleagues to collaborate on a project through platforms such as Dropbox[3] to which a user can upload content (images, office documents) and authorize others to access it. The cinematic arts (motion pictures and television) have a strong internet presence despite copyright concerns in applications such as services such as Netflix. ,[4]. The dramatic arts (plays and other theatrical performances) do not have as much presence in the Cloud as other media, which is not surprising as they tend not to exploit their performances on the web. Technology companies have certainly taken advantage of the ability to store information on the cloud. See, for example, the description of Cablevision's service that was the subject of *Cartoon Network LP v. CSC Holdings, Inc.*, discussed in our response to Sessions 2 and 3, question 1(1.2).

3) Are there already commercial platforms established specifically designated for the Cloud or to some extent related to Cloud uses? Can you foresee such new platforms to be established in the near future?

We assume that this question addresses commercial services and software designed for Cloud usage. In the United States, many commercial platforms have been created specifically for Cloud computing, and we are confident that more platforms will be designed in the future. Commercial services and software range from online Cloud computing service providers, such as Amazon Elastic Compute Cloud (Amazon EC2),[5] to online storage providers, like iCloud,[6] and online video-sharing websites such as YouTube.[7] Additional service providers include Dropbox, Vimeo,[8] iTunes Store,[9] Facebook,[10] Netflix, Hulu,[11] ReDigi,[12] and 8tracks.[13] For a more detailed discussion of various service providers see the response to Session 4, question 3.

4) How would you evaluate the Cloud's importance to copyright for the next few years to come?

In the next few years, content producers are increasingly likely to exploit their works on the Cloud. The convenience of virtually unlimited storage and access at a relatively low cost will continue to be attractive for rightholders and end-users alike. In the United States, copyright issues concerning the Cloud are testing the scope of protection under the Copyright

---

[3] *Tour – Simplify Your Life*, DROPBOX, https://www.dropbox.com/tour (last visited July 11, 2012).
[4] Netflix is a service whereby subscribers can download various television programs and films on demand to any device capable of receiving the transmissions. For more information on this service, go to https://signup.netflix.com/MediaCenter.
[5] *Amazon Elastic Compute Cloud (Amazon EC2)*, AMAZON WEB SERVICES, http://aws.amazon.com/ec2/ (last visited June 28, 2012).
[6] *iCloud*, APPLE, http://www.apple.com/icloud/features/ (last visited July 11, 2012).
[7] *Broadcast Yourself*, YOUTUBE, http://www.youtube.com/t/about_youtube (last visited July 11, 2012).
[8] *Explore on Vimeo*, VIMEO, http://vimeo.com/explore (last visited July 11, 2012).
[9] *iTunes*, APPLE, http://www.apple.com/itunes/whats-on/ (last visited July 11, 2012).
[10] *Facebook-Résumé*, FACEBOOK, http://www.facebook.com/facebook/info (last visited July 11, 2012).
[11] *About*, HULU, http://www.hulu.com/about (last visited July 11, 2012).
[12] *Learn More About ReDigi*, REDIGI, https://www.redigi.com/#!/learn (last visited July 13, 2012).
[13] *About*, 8TRACKS, http://8tracks.com/about (last visited July 11, 2012).

Act, and encouraging the development of private-law principles to guide the conduct of copyright owners and technology platforms. For example, as we discuss below, cases involving exploitation of copyrighted works in the Cloud have addressed the definition of a "copy," the significance of volitional control over the making of copies, the scope of the public performance right, and the meaning of "actual knowledge" of an infringement and of "awareness"of facts or circumstances from which infringing activity is apparent.

Sessions 2 and 3

– Can the Internet Treaties of 1996 play an important role in legal issues raised by "Cloud" Business?

1) Is there any case law to be found in your country and/or examples of (good) practices concerning:

1.1) the right of making available to the public with reference to "Cloud" storage, retrieval and dissemination?

There is no right titled "making available" under United States copyright law, but the rights of reproduction, public distribution, public performance and public display enumerated in section 106 of the Copyright Act offer many of the same rights and protections. Cases dealing with the interpretation of these rights in the Cloud context are discussed below in the responses to this questionnaire.

1.2) cloud providers that may be relevant to determine liability for the making available of unauthorized content in the cloud environment?

United States law does reflect the goals set out by WIPO's 1996 internet treaties. The U.S. does not have a 'making available' right, but Cloud providers could theoretically still be held liable for both direct and secondary infringement (including contributory and vicarious liability) in connection with making available infringing content. However, some courts have held that in a highly automated system, the Cloud provider merely responds to the direction of its users and therefore cannot be liable for direct infringement. Some of these cases are discussed below.

In *Cartoon Network LP v. CSC Holdings, Inc.*, the defendant, a cable television service provider called Cablevision, offered its subscribers a service that the plaintiff broadcasters and producers of audiovisual works labeled a kind of "video on demand," and that Cablevision called remote time-shifting.[14] The service enabled end-users to select from among programming that Cablevision distributed in real time (under license from copyright owners), and request that it be stored and subsequently transmitted to the users (without a license from copyright owners).[15] Cablevision maintained on its servers what one might envision as separate "storage boxes" for each user, so that as many copies would be made of any particular program as there were users requesting that the program be recorded.[16] This redundancy serves no apparent engineering objective; rather, the one-copy-per-user scheme seems to have been devised for the sole purpose of avoiding copyright-triggering acts. User copies were created by splitting the broadcast programming data into one stream constituting

[14] 536 F.3d 121 (2d Cir. 2008).
[15] Twentieth Century Fox Film Corp. v. Cablevision Sys. Corp., 478 F. Supp. 2d 607, 612 (S.D.N.Y. 2007) *rev'd in part, vacated in part sub nom. Cartoon Network LP* 536 F.3d 121.
[16] *Id.* at 615.

the real time transmission to subscribers, and a second stream that would be sent to a buffer, where the data representing each portion of the work would reside for some 1.2 seconds, while it was copied and sent to the storage boxes of any subscribers who requested to view the programming at a later time.[17] When a user wished to view the stored program, Cablevision's transmission would originate from that user's personal stored copy.[18] The service thus could be conceived of as a kind of virtual VCR, with the storage occurring on Cablevision's servers instead of at the user's home, and the performance of the work occurring by means of a transmission from Cablevision to the user, instead of occurring wholly at home.[19]

The copyright owners alleged that Cablevision had made unauthorized copies in its "buffer" and on the sectors of its servers reserved for subscribers, and unauthorized public performances of the designated programming.[20] Cablevision claimed that the buffer copies were not "copies" within the scope of the reproduction right, and that the stored copies, albeit "copies," were "made" by the users, not by Cablevision. Cablevision also contended that the transmissions back to the users were not "public performances" because each copy's viewing was limited to its maker. The parties agreed not to litigate whether the end-user conduct was infringing, or whether Cablevision might be secondarily liable for infringing end-user conduct. The district court ruled that the buffer copies were sufficiently "fixed" to be actionable;[21] that Cablevision, not the users, "made" the stored copies,[22] and the transmission of the copied works was "to the public."[23] The Second Circuit reversed on all three grounds.

The Second Circuit rejected the extension of the reproduction right to the buffer copies, on the ground that they did not meet the statutory definition of fixation. The court emphasized what it called the "duration requirement" of the definition:

> [T]he work must be embodied in a medium, i.e., placed in a medium such that it can be perceived, reproduced, etc., from that medium (the "embodiment requirement"), and it must remain thus embodied "for a period of more than transitory duration" (the "duration requirement"). Unless both requirements are met, the work is not "fixed" in the buffer, and, as a result, the buffer data is not a "copy" of the original work whose data is buffered.

536 F.3d at 127.

Although the buffer "embodied" the works, their embodiment was too transitory, the court held. The court distinguished decisions from other circuits for failure explicitly to address the duration requirement.[24] It also criticized a report from the Copyright Office, which had confronted the duration issue, but had reached a different conclusion.[25]

---

[17] *Cartoon Network, LP*,536 F.3d at 125.
[18] *Twentieth Century Fox Film Corp.*, 478 F. Supp. 2d at 615.
[19] *Cartoon Network LP*, 536 F.3d at 125.
[20] *Twentieth Century Fox Film Corp.* 478 F. Supp. 2d at 617.
[21] *Id.* at 622.
[22] *Id.* at 623-24.
[23] *Id*. at 621.
[24] *See, e.g.*, MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993); Stenograph L.L.C. v. Bossard Assocs., Inc., 144 F.3d 96, 101-02 (D.C. Cir. 1998); U.S. COPYRIGHT OFFICE, DMCA SECTION 104 REPORT 107-23 (2001) [hereinafter Copyright Office Section 104 Report], *available at* http://www.copyright.gov/reports/studies/dmca/sec-104-report-vol-1.pdf. Of these authorities, however, only the Copyright Office report specifically addresses reproductions as transient as "buffer copies." The Ninth and D.C.

The significance of the court's ruling on the reproduction right becomes apparent in light of the ruling's impact on the court's interpretation of "public" performance. Because Cablevision's transmissions to each of its subscribers emanated from each subscriber's personal copy (stored, but not "made" by Cablevision), the court ruled that the transmissions were not "to the public" and therefore did not implicate the public performance right.[26] The court distinguished cases finding "public performances" when transmissions were made individually and at different times to multiple members of the public from the same copy. The Cablevision feature that kept the performance from being deemed "public" was the one-to-one correspondence between the transmission recipient and the source copy for the transmission. Not surprisingly, given the decreasing cost of digital storage, *Cablevision* has spawned other business models built on automated copying and individualized transmissions. For example, in *ABC, Inc. v. AEREO, Inc.*,[27] the district court ruled that *Cablevision* compelled a finding that defendant's service, converting live over-the-air broadcasts into unauthorized but individualized Internet streams, did not "publicly" perform the broadcasters' works. Aereo's service allowed a subscriber to connect to a very small antenna, located at Aereo's data center, that receives broadcast television signals, converts and stores them in personalized storage files and then, at the subscriber's request, passes the digital broadcast stream to the subscriber's remote DVR.

In *Disney Enterprises, Inc. v. Hotfile Corp*., several entertainment companies sued an internet company that allowed users to upload and download video files.[28] Users were encouraged to become members in order to enjoy privileges such as faster download times. Hotfile earned money not only from these memberships, but also from affiliate programs. Users who uploaded the most popular (i.e., most downloaded) content were rewarded with various benefits, including cash payments. On Hotfile's motion to dismiss the complaint, a Florida District Court ruled that Hotfile was not subject to direct liability for its services merely because its system allows users to upload and download; the complaint alleged no direct, volitional infringing conduct on the part of Hotfile and its employees. The court dismissed the direct liability claim against Hotfile, but allowed the secondary liability claim to proceed.

A District Court in California, however, reached a different decision given similar facts in *Perfect 10 v. Megaupload*.[29] The California court refused to dismiss a claim for direct infringement against Megaupload, concluding that Megaupload was not, as defendants claimed, a "mere file storage system." It ruled that the company's actions as alleged in the

---

Circuit decisions involved software loaded into RAM and apparently retained for some minutes. *But see* MDY Indus., LLC v. Blizzard Entm't, Inc., No. CV-06-2555-PHX-DGC, 2008 WL 2757357, at *23 (D. Ariz. July 14, 2008) (reading MAI Sys. categorically to cover any RAM copying, without reference to duration of the copy; it is unclear how long the RAM copy of Blizzard's videogame survived in the temporary memory of customers of MDY's game-enhancing software).

[25] 536 F.3d at 129. For more on this topic, see Jane C. Ginsburg, Recent Developments in US Copyright Law - Part II, Caselaw: Exclusive Rights on the Ebb?, Revue Internationale du Droit d'Auteur (Jan. 2009), *available at* http://ssrn.com/abstract=1305270.

[26] *Cartoon Network, LP*, 536 F.3d at 139.

[27] No. 12 CIV. 1540 AJN, 2012 WL 2848158 (S.D.N.Y. July 11, 2012).

[28] Disney Enterprises, Inc. v. Hotfile Corp., 798 F. Supp. 2d 1303 (S.D. Fla. 2011).

[29] Perfect 10, Inc. v. Megaupload Ltd., No. 11CV0191-IEG BLM, 2011 WL 3203117, at *2 (S.D. Cal. July 27, 2011).

complaint, when taken together, could amount to volitional conduct.[30] These actions included the incentivizing of users to upload infringing content through a rewards system similar to Hotfile's, an affiliate program, and a general awareness that the website was being used for infringement.[31]

In *Warner Brother. Entertainment, Inc., v. WTV Systems, Inc.* defendant provided what it described as a DVD "rental" service called Zediva.[32] Defendants bought numerous DVDs of popular, copyrighted films and installed them in numerous DVD players. When users requested to watch a movie in Defendant's collection, Defendant would play a DVD player containing the requested movie, convert the analog signal into a digital signal and transmit it to the requesting user.[33] Users had up to four consecutive hours to watch the movie, at which time the DVD player with the requested movie could be allocated to another user. If the user didn't finish watching the work she could do so within 14 days; however, when she requested that the movie continue, she might not be allocated the same DVD in the same DVD player. Defendants made money through the charges for streaming the DVDs, which were offered at a lower rate than those of licensed internet video-on-demand services.

The court ruled that the Zediva service directly infringed plaintiffs' copyrighted movies and issued a preliminary injunction.[34] First, the court held that Zediva was responsible for transmitting the works even if it was the customer who made the initial request. Second, the transmissions were made "to the public" as defined in Section 101(2) because the relationship between the audience and Zediva was a commercial, public one regardless of where the movies were viewed. According to the court, "[t]he non-public nature of the place of the performance has no bearing on whether or not those who enjoy the performance constitute 'the public' under the transmit clause [section 101(2)]."[35] The court distinguished the facts from those in *Cartoon Network* because Zediva's customers did not produce their own copy; rather, the same DVDs were used repeatedly to transmit plaintiffs' works. However, it expressed disagreement with *Cartoon Network*'s "volitional conduct requirement" for direct infringement.[36]

Recently, Capitol Records filed a lawsuit against ReDigi.com, an online marketplace of used digital copies of recorded music.[37] The service enables users to store their recordings in online lockers and sell, buy, and stream music in the Cloud.[38] To sell a digital recording in the marketplace, users must download ReDigi's Music Manager software.[39] The software allows users to designate the recordings that they wish to sell from their device.[40] To date, ReDigi allows resale only of recordings that were legally purchased from iTunes Store or Redigi.[41] ReDigi removes eligible recordings from the seller's device and stores the

[30] *Id.* at *4.
[31] *Id.* at *6.
[32] 824 F. Supp. 2d. 1003 (C.D.Cal. 2011).
[33] For a description of the technology behind the transmissions, *see id*. at 1007.
[34] Zediva closed down in October, 2011.
[35] 824 F. Supp. 2d at 1010.
[36] *Id*. at 1011 n.7.
[37] Complaint, Capitol Records, LLC v. ReDigi, Inc., 2012 WL 32056 (S.D.N.Y. Jan. 6, 2012) (No. 12 CIV 0095).
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] REDIGI, *supra* note 12.

recordings in the ReDigi cloud for sale.[42] Buyers are able to view a list of recordings that are for sale, and purchase and download them.[43] In its complaint, Capitol Records alleges that ReDigi is liable for several violations, including direct infringement, contributory and vicarious liability, and inducement of copyright infringement.[44] Among other assertions, the plaintiff claims that ReDigi has and continues to engage in unauthorized reproduction, distribution, and public performances of the plaintiff's copyrighted materials and assists users in making unauthorized copies and sales.[45] In response to some of these allegations, ReDigi has claimed fair use and the first sale doctrine as a defense.[46] Although the first sale has traditionally applied only to hardcopies, ReDigi urges a digital equivalent of the first sale doctrine. ReDigi contends that its system, which removes the digital copy from its prior owner's access, so that only one person "owns" the digital copy at any one time, should enjoy the same exemption from copyright liability as would the used book or record market. At this stage of the process, the plaintiff has requested a preliminary injunction.

Section 512 of the Copyright Act provides some safe harbors for ISPs in certain situations. We will discuss these in greater detail below, in response to Session 5, questions 5.2(2), (3) and (4), and we will discuss the issue of inducement in the answer to Session 5, question 5.2(2).

2) Is there case law on the technological protection measures and Electronic rights management information in the "Cloud" environment?

Technological Protection Measures

We discuss U.S. law concerning the circumvention of technological protection measures (TPMs) in the response to Session 4, question 7, below. Even though much of the case law up to now concerning TPMs has developed outside the context of the Cloud environment, it remains relevant. For example, in *Universal City Studios, Inc. v. Corley*, the Second Circuit Court of Appeals affirmed a judgment against the distributor of a software program known as "DeCSS" designed to circumvent the CSS protection system on commercially distributed DVDs.[47] The court also found that the defendant had violated the anti-circumvention provisions in section 1201 of the Copyright Act by providing links to sites from which the program automatically downloaded. In so doing, the court rejected defendants' argument that fair use provides a defense to section 1201's anti-circumvention provisions.[48]

MDY Industries, LLC v. Blizzard Entertainment, Inc. involved a popular multiplayer online role-playing game, "World of Warcraft," in which players interact in a virtual world as they advance through the game's 70 levels.[49] In effect, the game is located in the Cloud.

[42] *Id.*
[43] *Id.*
[44] Complaint, *Capitol Records v. ReDigi*, 2012 WL 32056.
[45] *Id.*
[46] Defendant's Memorandum of Law in Opposition to Plaintiff's Motion for A Preliminary Injunction, Capital Records, LLC v. ReDigi, Inc., No. 12-cv-0095 (RJS) (AJP) (S.D.N.Y. Jan. 27, 2012), 2012 WL 2281961.
[47] Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).
[48] *See also* 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004) ("While 321's software does use the authorized key to access the DVD, it does not have the authority to use this key, as licensed DVD players do, and it therefore avoids and bypasses CSS.").
[49] 629 F.3d 928 (9th Cir. 2010).

MDY Industries created and distributed a software program, "Glider," that automatically plays the early levels of the game for players, in violation of Blizzard's terms of use. Blizzard's software program "Warden" was designed to protect against the use of such programs, but Glider was designed to circumvent Warden.

MDY sought a declaration from the court that, inter alia, its distribution of Glider did not violate section 1201(a)(2). The court rejected MDY's argument that section 1201 was designed to protect only copyright rights under section 106, and that the "access" protected under section 1201 is not such a copyright right. The court said that section 1201 created a new form of protection, i.e., the right to prevent circumvention of access controls, and section 1201 could be violated by circumvention even if infringement did not ensue.

In support of its decision, the court cited this passage from the legislative history of the DMCA, which indicates that Congress had Cloud services in mind when it enacted the anti-circumvention provisions:

> [A]n increasing number of intellectual property works are being distributed using a "client-server" model, where the work is effectively "borrowed" by the user (e.g., infrequent users of expensive software purchase a certain number of uses, or viewers watch a movie on a pay-per-view basis). To operate in this environment, content providers will need both the technology to make new uses possible and the legal framework to ensure they can protect their work from piracy.

629 F.3d at 947 (quoting H.R. Rep. No. 105-551, pt. 2, at 23 (1998)).

Copyright Management Information

Section 1202 of Title 17 of the United States Code addresses the integrity of copyright management information. Section 1202(a) prohibits a person "knowingly and with the intent to induce, enable, facilitate or conceal infringement," from (1) providing false copyright management information or (2) distributing or importing for distribution false copyright management information. For purposes of section 1202, "copyright management information" includes any of the following conveyed in connection with the work: the title, author, copyright owner, and other identifying information about the work or any of the above, including information set forth on a copyright notice, terms and conditions for use of the work, identifying numbers or symbols referring to such information and, with the exception of public performances by radio and television broadcast stations: the name of and other identifying information about a performer whose performance is fixed in a work other than an audiovisual work, and in the case of an audiovisual work, the name of and other identifying information about a writer, performer, or director who is credited in the audiovisual work.

Section 1202(b) prohibits: (1) intentionally removing or altering copyright management information, (2) distributing or importing for distribution any copyright management information, and (3) distributing or importing for distribution, or publicly performing works, copies of works or phonorecords, knowing that copyright management information has been removed or altered without the authority of the copyright owner or the law, and knowing, or with regard to civil remedies set forth in section 1203, having

"reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement under" Title 17.

Section 1202 has been of limited effect in protecting copyright management information for a number of reasons. First, it protects only that information the rights owner has chosen to attach to the work. There is no requirement, for example, that the name of the author be included.

Second, the double intent requirement sets a standard that is difficult to meet. In order to prove a violation of the statute, one must demonstrate not only that the defendant removed copyright management information or distributed or performed it knowing that copyright management information had been removed, but also that the defendant knew or had reason to know that it would "induce, enable, facilitate or conceal infringement" of copyright.

Third, at least some courts have held that to qualify for protection the copyright management information must be embedded in the copy of the work itself and not just on the webpage or other introductory material.[50]

3) How can we re-examine or re-evaluate the role of the WIPO Treaties with reference to "cloud" developments?

Among the provisions of the WIPO Treaties with particular significance for the protection of copyright and related rights in the Cloud context are the requirements concerning technological protection measures (WIPO Treaty art. 11, WPPT art. 18), copyright management information (WIPO Treaty art. 12, WPPT arts. 19), and the "making available" right (WIPO Treaty art. 8, WPPT arts. 10 and 14). It would be helpful to explore how these rights have been implemented in the national laws of the Member States and whether the formulation of these obligations in the treaties, or the manner in which the treaties have been implemented, appropriately protect rightholders. For example, the formulation of the obligations with respect to copyright management information contains a double knowledge standard which, at least in the United States, has considerably weakened its effect.

Session 4
– New Business Models for effective Protection of Copyright and Related rights in the "Cloud": Role of electronic rights management in new business models

Note: ***In general, services offered on the basis of cloud computing technologies are classified as "Software as a Service"(SaaS), "Platform as a Service" (PaaS) and "Infrastructure as a Service" (IaaS). Under the heading of "New Business Models for effective Protection of Copyright and Related rights in the 'Cloud'", the main focus is on PaaS, whereas both IaaS and SaaS are of minor importance, since they generally do not involve the use of copyrighted works of literature and the arts (issues of copyright in software are not discussed at this congress).***

Note*: *This subsection focuses on successful business models of authors and rightholders who market their copyrighted subject matter in the cloud either themselves or via a service

[50] *See, e.g.*, Kelly v. Arriba Soft Corp., 77 F. Supp. 2d 1116 (C.D. Cal 1999), *aff'd*, 336 F.3d 811 (9th Cir. 2003) (information on photographer's webpage rather than on individual photos). However, the statute does not require embedding the information, only that it be conveyed "in connection with" the copyright protected work.

provider (such as, e.g. Apple's "iTunes in the Cloud"), presumably by employing digital rights management (DRM) and perhaps also technical protection measures (TPM).

1) In your country, what types of cloud services are offered and/or made available by authors and rightholders offering their copyrighted content?

We assume that this question is asking which types of services exist that allow authors or rightholders to post their copyrighted content in the Cloud so that others may access it. There are a variety of services that authors and rightholders can exploit to do this. It is important to note that this response is not exhaustive.

Many of the largest rightholders in the content industry license their content to various platforms. Hulu, for example, is an on-demand video service provider that streams movies, television shows, clips, etc. online. Unlike some other on-demand video service providers, Hulu is owned by top-tier media companies in the content industry.[51] Mainstream television networks and studios license their content to Hulu to make it available to the public. In addition to Hulu, Netflix,[52] Vudu,[53] and YouTube also provide similar on-demand internet video content. Although their business models may differ, these online video service providers, and others like them, provide means through which rightholders can post their copyrighted content in the Cloud. For instance, both media companies and YouTube end-users can directly post their content on YouTube. Music-related services, such as iTunes Store or Pandora Radio,[54] represent Cloud technology that publishers and other rightholders commonly utilize to sell downloads or performances (i.e., streaming) of copyrighted music.

There is also a plethora of user-generated content services, which are services that allow end-users to upload their content to the Cloud. For example, YouTube and Vimeo are well-known websites that allow authors to upload their video content in a way that users worldwide can access it. As for photographic works, Flickr[55] and Google's Picasa[56] are among the more popular image hosting sites. Sometimes referred to as virtual warehouses, these Cloud services allow authors to upload, edit, and distribute copyrighted images in the Cloud. Aside from photographic and audiovisual works, there are also hosting services like SlideShare,[57] which enables users to upload and share presentations with colleagues or other users. Originally intended for slideshow presentations, SlideShare and other platforms have evolved to enable authors to store files formatted in PowerPoint, PDF, Keynote as well as webinar and video formats. In terms of music-related content, 8tracks is an example of a website that enables rightholders to post and distribute their music in the Cloud. Publishing

[51] NBCUniversal, News Corporation, The Walt Disney Company, and Providence Equity Partners (the owner of Newport Television) own Hulu. HULU, *supra* note 11.
[52] For details about the Netflix service see *supra* note 4.
[53] Vudu is a media technology and content delivery company, which among other things, provides an online on-demand video streaming service. VUDU, http://www.vudu.com/ (last visited June 28, 2012).
[54] Pandora Radio is a music streaming service available only in the U.S. The service plays songs similar to the songs that users select. *About Pandora Media*, PANDORA, http://www.pandora.com/about (last visited July 11, 2012).
[55] Flickr is also a video hosting site, however, it is more well-known for photographic works. *Welcome to Flickr – Photo Sharing*, FLICKR, http://www.flickr.com/ (last visited June 28, 2012).
[56] *Welcome to Picasa and Picasa Web Albums!*, PICASA, http://support.google.com/picasa/bin/answer.py?hl=en&answer=157000 (last visited July 11, 2012).
[57] UPLOAD & SHARE POWERPOINT, http://www.slideshare.net/ (last visited June 28, 2012).

platforms like Yahoo!Voice[58] enable authors, among other things, to post their literary works in the Cloud.

There are also general Cloud platforms that facilitate content distribution throughout the Cloud. Unlike Picasa or YouTube, which support a specific type of content (i.e. photographic and audiovisual works, respectively), general platforms support any type of content. Authors and rightholders can use these general services as they see fit to upload their copyrighted works. There are several general platforms offered in the U.S. Take, for example, online back-up services, like Dropbox,[59] Google Drive,[60] or SkyDrive.[61] Among other features, these file hosting services offer Cloud storage, file synchronization, and file-sharing features. These features allow users to share their content within a private group or with the general public and back up files as a safeguard against hard-drive malfunctions. They can also serve as supplemental storage for those who may lack sufficient local hard drive capacity. Social network services, such as Facebook or Google Plus,[62] also facilitate content distribution in the Cloud. Though these sites are best known for their social networking services, they also enable authors and other rightholders to share their content throughout private and public forums.

Of course, most of the services that allow authors to post content they have created also enable users to post, without authorization, copyrighted content owned by others.

2) What kinds of works are being offered in this way (e.g., musical works, literary works, photographic works, audiovisual works, performances etc.)?

As mentioned above, some of the works that rightholders post to the Cloud include sound recordings, musical, literary, photographic, and audiovisual works.[63]

3) What rights do rightholders usually transfer to the providers of cloud services?

Section 106 of the Copyright Act grants exclusive rights to copyright owners.[64] Therefore, the bundle of rights that rightholders can transfer or license to Cloud service providers derives from section 106. To determine which rights rightholders typically grant to service providers, we surveyed the terms of commonly-used Cloud services.

We selected eleven providers: Google Services, Yahoo! Services, Dropbox, Vimeo, YouTube, Amazon Web Services,[65] iTunes Store, Facebook, Netflix, Hulu, and 8tracks. The selection was based on the popularity[66] of the service provider (presumably the agreements of

[58] YAHOO! VOICES, http://voices.yahoo.com/ (last visited June 28, 2012).
[59] DROPBOX, *supra* note 3.
[60] GOOGLE DRIVE, https://drive.google.com/start?utm_medium=ha&utm_source=en-oa-na-us-bk&utm_campaign=en#home (last visited June 28, 2012).
[61] MICROSOFT SKYDRIVE, http://windows.microsoft.com/en-US/skydrive/home (last visited June 28, 2012).
[62] LEARN MORE – GOOGLE PLUS, https://www.google.com/intl/en/+/learnmore/index.html (last visited June 28, 2012).
[63] For a more detailed discussion of the types of works rightholders make available in the Cloud see the response to Session 4, question 1.
[64] 17 U.S.C. § 106.
[65] AMAZON WEB SERVICES, http://aws.amazon.com/ (last visited June 28, 2012).
[66] To help identify popular Cloud services, we used Alexa, a web information company that measures, among other things, web traffic and use. ALEXA, http://www.alexa.com/ (last visited June 6, 2012). Assuming that there

the most popular services reveal which rights are commonly transferred or licensed) and diversity within the surveyed group of providers. Many Cloud service providers use browse-wrap or click-wrap agreements. Assuming that these agreements are binding,[67] rightholders who use these services grant non-exclusive rights in their work.

In general, rightholders typically retain their ownership rights in their copyrighted work and grant providers non-exclusive rights. Eight of the eleven service providers surveyed expressly state in their user-agreements that rightholders retain ownership in their work.[68] Though the licensing agreements between rightholders and Netflix and iTunes Store are not available, the type of rightholders that typically use these platforms to distribute their content—for instance, top tier film studios or record labels like Twentieth Century Fox Film or Sony Music Entertainment—likely retain their ownership rights. A significant portion of the content that Hulu broadcasts is owned by the media companies that own Hulu, and they likely retain ownership of their works.

The survey demonstrated that rightholders grant a license to providers the scope of which depends on the particular service and/or on the rightholder's bargaining power.[69] Some popular providers have a relatively narrow scope of rights that they require users to license. For example, Yahoo! Services, which includes Flickr, Yahoo! Voice, and other Yahoo! Cloud services, stipulates in its terms of service that rightholders grant Yahoo! a non-exclusive right to distribute, reproduce, modify, publicly perform and display rightholders' image-based and

---

is a positive correlation between traffic ranking and rightholders using the Cloud service, with the exception of Dropbox and 8tracks, we selected providers that had a traffic rank less than one-hundred. For example, Google has the number one traffic ranking in the United States. Dropbox ranks at 133, while 8tracks has a traffic rank of 3,219. For purposes of diversity, we included these two providers.

[67] Browse-wrap and click-wrap agreements are licensing agreements that bind end-users who access the site (for browse-wrap agreements) or click that they agree to the license (in the case of click-wrap agreements). For our purposes, the validity of these agreements depends on whether the end-user had reasonable notice of the terms of the license. The courts vary on what constitutes reasonable notice. *See* Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002); Feldman v. Google, Inc., 513 F. Supp. 2d 229 (E.D. Pa., 2007); *cf.*, Cairo, Inc. v. CrossMedia Services, Inc., No. C 04-04825 JW, 2005 WL 756610, at * 5 (N.D. Cal. April 1, 2005) (holding that a user's repeated and automated use of a website may be sufficient to form the basis of imputing knowledge of the website's terms of service thereby putting the user on notice and binding the user to the terms of service agreement).

[68] *See Vimeo API Licensing Agreement*, VIMEO, https://developer.vimeo.com/guidelines/terms (last visited June 4, 2012) ("[N]either party [i.e. Vimeo nor end-user] transfers any right, title, or interest in or to its intellectual property." *Id.* at Section 3.1.); *Terms – Simplify Your Life*, DROPBOX, https://www.dropbox.com/terms (last visited June 4, 2012) ("These Terms do not grant us any rights to your stuff."); *YAHOO! Terms of Service*, YAHOO!, http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (last visited June 4, 2012) ("Yahoo! does not claim ownership of Content you submit or make available for inclusion on the Yahoo! Services." *Id.* at Section 9); *Google Terms of Service*, GOOGLE, https://www.google.com/intl/en_US/policies/terms/ (last visited June 4, 2012) ("You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours."); *Terms of Services*, YOUTUBE, http://www.youtube.com/t/terms (last visited June 5, 2012) ("For clarity, you retain all of your ownership rights in your Content." *Id.* at Section 6.C); *Amazon Web Services Customer Agreement*, AMAZON WEB SERVICES, http://aws.amazon.com/agreement/ (last visited June 5, 2012) ("As between you and us, you or your licensors own all rights, title, and interest in and to Your Content." *Id.* at Section 8); *Facebook Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/legal/terms (last visited June 5, 2012) ("You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings." *Id.* at Section 2); *Terms of Service*, 8TRACKS, http://8tracks.com/terms (last visited June 6, 2012) ("You shall retain all of your ownership rights in your User Submissions." *Id.* at Section 8.2).

[69] Media companies with greater bargaining power use customized licensing agreements. *See* Yafit Lev-Aretz, *Second Level Agreements*, 45 AKRON L. REV. 137, 153-154 (2012).

audiovisual content solely for the purpose for which such content was submitted or made available.[70] Additionally, for Yahoo! Groups, Yahoo! obtains similar rights solely for use in connection with the specific Yahoo! Group to or for which the content was submitted.[71]

Other Cloud service providers demand the right to exploit users' works more fully. Some providers use agreements that grant them the right to exploit users' submissions for uses related to or in connection with the provider without limiting those uses to a particular service.[72] For instance, when rightholders use Google or Yahoo! Cloud services, rightholders non-exclusively license each of the five distinct rights recognized in section 106 (hereinafter "section 106 rights") of the U.S. copyright law.[73] However, the providers' uses are limited as detailed in both Google and Yahoo's terms of service. Without explicitly mentioning section 106 rights, some user agreements grant providers unspecified rights to execute functional ends.[74] Users of Amazon Web Services (which includes Amazon EC2 and S3) grant Amazon the rights that are implicated in carrying out the Cloud service.[75] Rightholders that use 8tracks transfer to the provider a non-exclusive license, "throughout the universe, to use, reproduce, distribute, modify, adapt, prepare derivative works of, publicly display, publicly perform, and otherwise exploit your User Submissions *in connection with the 8tracks Platform and 8tracks' (and its successor's) business*."[76] Despite the language in italics, these agreements and others like it do not significantly limit providers, since most uses providers are likely to make will fall within the scope of the license. Consequently, rightholders license, without meaningful limitations, section 106 rights in their content. Some Cloud service providers acquire even broader rights and omit limits altogether. For example, Facebook users grant Facebook non-exclusive rights in their content regardless of use.[77] For content that

---

[70] *YAHOO! Terms of Service*, YAHOO!, http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html ("With respect to photos, graphics, audio or video you submit or make available for inclusion on publicly accessible areas of the Yahoo! Services other than Yahoo! Groups, *the license to use, distribute, reproduce, modify, adapt, publicly perform and publicly display such Content on the Yahoo! Services solely for the purpose for which such Content was submitted or made available.* This license exists only for as long as you elect to continue to include such Content on the Yahoo! Services and will terminate at the time you remove or Yahoo! removes such Content from the Yahoo! Services." *Id.* at Section 9(b) (emphasis added)).

[71] Section 9(a) in the Terms of Service provides that, "With respect to Content you submit or make available for inclusion on publicly accessible areas of Yahoo! Groups, the *license to use, distribute, reproduce, modify, adapt, publicly perform and publicly display such Content on the Yahoo! Services solely for the purposes of providing and promoting the specific Yahoo! Group to which such Content was submitted or made available.* This license exists only for as long as you elect to continue to include such Content on the Yahoo! Services and will terminate at the time you remove or Yahoo! removes such Content from the Yahoo! Services." *Id.* (emphasis added).

[72] *See Terms of Service*, YOUTUBE, http://www.youtube.com/t/terms (last visited July 11, 2012) ("[Y]ou hereby grant YouTube a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to use, reproduce, distribute, prepare derivative works of, display, and perform the Content *in connection with the Service and YouTube's (and its successors' and affiliates') business*." *Id.* at Section 6 (emphasis added)).

[73] Section 106 of the Copyright Act lists six exclusive rights. However, section 106(6) is not a distinct right but rather a public performance right that specifically concerns sound recordings. Thus, there are five distinct rights.

[74] *See Terms – Simplify Your Life*, DROPBOX, https://www.dropbox.com/terms (last visited June 4, 2012) ("These Terms do not grant us any rights to your stuff or intellectual property except for the limited rights that are needed to run the Services, as explained below.")

[75] *See Amazon Web Services Customer Agreement*, AMAZON WEB SERVICE, http://aws.amazon.com/agreement/ (last visited July 11, 2012) ("You consent to our use of Your Content to provide the Service Offerings to you and any End Users." *Id.* at Section 8).

[76] *Terms of Service*, 8TRACKS, http://8tracks.com/terms (last visited July 11, 2012) (emphasis added).

[77] *See Terms of Service*, FACEBOOK, http://www.facebook.com/legal/terms (last visited July 11, 2012) ("For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings*: you grant us a non-exclusive,*

is neither graphic/audiovisual nor affiliated with Yahoo! Groups, Yahoo! acquires a bundle of non-exclusive rights that Yahoo! can use to any end. [78]

Some cloud service providers allow users to submit comments or feedback. Many service providers state in their Terms of Service that the copyrights in any such feedback are the property of the service provider.[79]

4) What uses of copyrighted material are the users of such cloud services permitted?

End-users are permitted to use copyrighted material as described in the particular service's user agreement.[80] Users are allowed to exploit copyrighted content as is necessary to use the service, provided that the use is in accordance with the terms of service.

The types of specific uses permitted vary and depend on the Cloud service provider. For example, YouTube end-users are allowed to use, reproduce, distribute, display, and perform copyrighted content on YouTube to the extent permitted by the functionality of YouTube.[81] According to the current Apache License, developers who create applications for

---

transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it." *Id.* at Section 2.1 (emphasis added)).

[78] *Yahoo! Terms of Service*, YAHOO!, http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (last visited July 11, 2012) ("With respect to Content other than photos, graphics, audio or video you submit or make available for inclusion on publicly accessible areas of the Yahoo! Services other than Yahoo! Groups, *the perpetual, irrevocable and fully sublicensable license to use, distribute, reproduce, modify, adapt, publish, translate, publicly perform and publicly display such Content* (in whole or in part) and to incorporate such Content into other works in any format or medium now known or later developed." *Id.* at Section 9(c) (emphasis added)).

[79] We identified three providers (Yahoo!, Amazon Web Services, and Apple) whose terms of service state that the provider acquires ownership rights in user-feedback. *See id.* ("[Y]our Contributions automatically become the property of Yahoo! without any obligation of Yahoo! to you." *Id.* at Section 10(e)); *Amazon Web Services Customer Agreement*, AMAZON WEB SERVICES, http://aws.amazon.com/agreement/ (last visited June 5, 2012) ("If you provide any Suggestions to us or our affiliates, we will own all right, title, and interest in and to the Suggestions, even if you have designated the Suggestions as confidential. We and our affiliates will be entitled to use the Suggestions without restriction. You hereby irrevocably assign to us all right, title, and interest in and to the Suggestions and agree to provide us any assistance we may require to document, perfect, and maintain our rights in the Suggestions." *Id.* at Section 8.6). *See also Apple's Unsolicited Idea Submission Policy*, APPLE, http://www.apple.com/legal/policies/ideas.html (last visited June 5, 2012) ("You agree that: (*1) your submissions and their contents will automatically become the property of Apple, without any compensation to you*; (2) Apple may use or redistribute the submissions and their contents for any purpose and in any way; (3) there is no obligation for Apple to review the submission; and (4) there is no obligation to keep any submissions confidential." (emphasis added)).

[80] Customized licensing agreements between service providers and entertainment companies also grant end-users rights in the media companies' copyrighted content. See *infra* Session 5, question 5.2(6) for more details on customized licensing agreements. Presumably, these customized licensing agreements grant end-users permission for general uses. Since these agreements are not publicly available, we can not comment on the specific rights, if any, that these agreements grant to end-users.

[81] *See* YOUTUBE, *supra* note 72 ("You also hereby grant each user of the Service a non-exclusive license to access your Content through the Service, and to use, reproduce, distribute, display and perform such Content as permitted through the functionality of the Service and under these Terms of Service. The above licenses granted by you in video Content you submit to the Service terminate within a commercially reasonable time after you remove or delete your videos from the Service." *Id.* at Section 6(C)).

Amazon are allowed, among other things, to use, reproduce, and make derivatives of user submissions.[82]

5) Can you give any figures regarding both royalty rates and total revenue authors and rightholders receive when their works are being offered in the cloud?

This information is not publicly available.

6) What kind of TPM and DRM is used by these services?

We assume that this question addresses the types of technical protection measures (TPMs) and digital rights management (DRM) technology that U.S. Cloud service providers utilize domestically. Cloud service providers use DRM schemes on their own and in conjunction with other networks and user devices that interact with the Cloud. Thus, service providers use an array of DRM technology. In many cases, the details concerning the technical measures that are used in DRM schemes are not publicly available. In this response we identify some of the TPMs that Cloud service providers utilize, but the list is not exhaustive.

Service providers use multiple TPMs. Many service providers use a login system. The login systems are password-protected and provide access to databases, websites, pages, folders, and/or specific content. For instance, private Clouds, like iCloud, require a password to access stored content.[83] Providers also use encryption to deter or block downloading.[84] Compatibility requirements are useful for limiting the devices and networks that can access and exploit content. For instance, iPod users must use certain devices to download content to their iPod.[85] Until recently, Apple used DRM to limit audio-playback to authorized devices for iTunes music.[86] To regulate where the content may be used, some service providers rely on tracking technology that locates user devices.[87] Through tracking technology, service providers can limit use to authorized geographic regions. Service providers also utilize limited-use DRM which controls the length of time a user can access and use content.[88] On-demand video streaming websites frequently offer free trials for a limited time after which the

---

[82] *AWS Customer Agreement*, AMAZON WEB SERVICES, http://aws.amazon.com/agreement/ (last visited June 7, 2012) ("Your Submissions will be governed by the terms of the Apache Software License, unless you specify one of our other supported licenses at the time you submit Your Submission." *Id.* at Section 8.2). *See also Apache License Version.2.0*, THE APACHE SOFTWARE FOUNDATION, http://www.apache.org/licenses/LICENSE-2.0 (last visited June 7, 2012) ("Subject to the terms and conditions of this License, each Contributor [i.e. copyright owner] hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.").

[83] *See iCloud Security and Privacy Overview*, ICLOUD, http://support.apple.com/kb/HT4865 (last visited June 29, 2012).

[84] *See, e.g., id.* (listing features that are secured through encryption); *Security - Dropbox for Teams*, DROPBOX, https://www.dropbox.com/teams/security (last visited June 29, 2012) (explaining services that are secured by encryptions).

[85] *Play Music and More on iPod*, APPLE, http://www.apple.com/ipod/ (last visited June 29, 2012) (listing the iPod compatible devices).

[86] *Press Info*, APPLE, http://www.apple.com/pr/library/2007/04/02Apple-Unveils-Higher-Quality-DRM-Free-Music-on-the-iTunes-Store.html (last visited June 29, 2012).

[87] *See* Lionel S. Sobel, *DRM as an Enabler of Business Models: ISPs as Digital Retailers*, 18 BERKELEY TECH. L. J. 667, 681 (2003) (explaining how ISPs can track users who are accessing digital content).

[88] JANNA QUITNEY ANDERSON ET AL., UBIQUITY, MOBILITY, SECURITY: THE FUTURE OF THE INTERNET III 166-67 (2009).

service is unavailable.[89] End-users are often prompted to purchase a product, upgrade a service, or comply with the provider's requirements to regain access. For example, iTunes Store allows movie-renters up to 30 days after their purchase to download their rented movie.[90] Once they download the movie, they have 24 hours to view it.[91] Cloud service providers also use technology to verify authenticity and acquire information about end-users or potential copyright infringers. For example, through digital watermarking, technicians can embed information into media content, which allows sites to track usage and convey ownership information, contact details, and usage rights.[92]

7) Under the legislation of your country, to what extent are TPM protected against their unauthorized circumvention?

The requirements concerning technological protection measures were implemented in U.S. law through the WIPO Copyright Performances and Phonograms Treaties Implementation Act of 1998, Title I of the DMCA, which added chapter 12 to Title 17 of the United States Code.[93]

Section 1201(a) prohibits the circumvention of a "technological protection measure that effectively controls access to a work" protected under Title 17.[94] Examples of such technological protection measures ("TPMs"), referred to as "access controls," include passwords and encryption. Thus, section 1201(a)(1) prohibits the act of hacking a password or decrypting an encrypted work.

In addition, section 1201(a)(2) prohibits manufacturing, importing, offering to the public, providing or otherwise trafficking (hereafter, "trafficking") in any "technology, product, service, device, component or part thereof" (hereafter, "device/service") that circumvents access controls (e.g., DeCSS for DVDs), if the device/service: (1) "is primarily designed or produced for the purpose of circumventing" access controls; (2) "has only limited commercially significant purpose or use other than to circumvent" access controls; or (3) is knowingly marketed for use in circumventing access controls.[95]

Similarly, section 1201(b) prohibits trafficking in any device/service that circumvents TPMs that effectively protect a right of a copyright holder under Title 17 in a work or a portion thereof (an example of this type of TPM would be a "copy control" technology – one that prevents the user from making a copy of the work displayed).[96]

Sections 1201 (d)-(j) provide a number of exemptions, excusing conduct that would otherwise violate the prohibition on circumventing access controls contained in section 1201(a), under specific and detailed conditions. These exemptions include those for:

---

[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Communication of Ownership and Copyrights*, DIGITAL WATERMARKING ALLIANCE, http://www.digitalwatermarkingalliance.org/app_comm.asp (last visited June 28, 2012).
[93] Pub. L. No. 105-304, 112 Stat. 2860, 2863 (1998).
[94] 17 U.S.C. § 1201(a).
[95] § 1201(a)(2).
[96] § 1201(b).

• Nonprofit libraries, archives and educational institutions to allow them to determine whether or not they would like to acquire a work;
• Law enforcement, intelligence, and other government activities;
• Reverse engineering of computer programs for the sole purpose of identifying and analyzing elements of the program necessary to achieve interoperability with other programs:
• Encryption research;
• Protection of minors by preventing their access to materials on the internet;
• Circumvention with the sole effect of identifying and disabling the capability of a TPM to collect personally identifying information; and
• Security testing.

The law also provides for a triennial administrative proceeding, pursuant to which the Librarian of Congress may institute additional exemptions. The additional exemptions currently in force are described at http://www.copyright.gov/1201/2010/.
Each administrative proceeding is *de novo*; the Copyright Office is currently in its fifth administrative rulemaking proceeding to determine which exemptions will be in force for the next three year period. Information on this proceeding is available at http://www.copyright.gov/1201/.

8) Is unauthorized circumvention of TPM a practical problem for those offering their content in the cloud?

Yes; unauthorized circumvention of TPMs is a practical problem for rightholders, since circumvention may allow their works to be accessed and exploited without their authorization and to their detriment.

5 Copyright-avoiding business models

Note: *This subsection focuses on business models of persons other than authors and rightholders, who build upon someone else's copyrighted material and who – successfully or not – try not to be subject to copyright liability. Examples are services that make use of the private copying exception (such as, e.g., personalized internet video-recorders) or which strive to benefit from an exception to legal liability as an Internet Service Provider (such as, e.g., under the EU e-Commerce Directive). In addition, strategies of authors who market their copyrighted works outside of copyright (such as, e.g., under an open content or Creative Commons (CC) licence) can also be regarded as "copyright-avoiding" business models (although technically, they are based on copyright).*

5.1 – Private copying in the Cloud

1) In your country, are there services – and if so, what kind of services are there - that offer its users to store private copies in the cloud?
Examples are storage services with limited access (such as Google's "Picasa"), platforms with general public access (such as, e.g., Flickr) and mixed-forms (such as, e.g. Facebook) but also so-called internet-video recorders and possible other forms of private storage services.

Yes; end-users are able to privately store their content in the Cloud. Some of the services that provide private storage include iCloud, SkyDrive, Google Drive, and Dropbox. Some of the video streaming websites that have private storage services include YouTube and Vimeo. If users set their privacy settings to private, they can privately store their content on services like Flickr, Facebook, or Picasa. Additionally, Cloud computing service providers such as Amazon EC2 or IBM's Blue Cloud[97] have configured private space for end-users to store their content.

Some "digital storage lockers" are truly private, allowing access only to the users who uploaded the content. However, some content that has been placed in "private" storage lockers is readily available to the general public. While other services, such as Dropbox and Google Docs,[98] allow access to only a limited number of persons. Some providers generate unique links (or "hotlinks") for uploaded content. Subsequently, third parties, even those unaffiliated with the uploader or the Cloud service, can follow these links (which are often publicized widely) and retrieve the uploaded content.[99]

2) In legal terms, to what extent do the operators of such services benefit from its user's private copying exception? Are there any other exceptions under copyright law? (note that general exceptions of legal liability are discussed under 5.2)

There is no private copy exception in U.S. copyright law. End-users and service providers may, in appropriate circumstances, use the statutory fair use defense against primary infringement, as discussed below. Secondary liability of service providers is premised on some form of primary liability. Accordingly, Cloud service providers will not be liable for infringement based on their users' activities when those activities qualify for the fair use defense or when those activities do not amount to a primary infringement (such as where the performance involved is a private, not public, performance). [100] In addition, even if the end-user copying would not be considered a fair use, the Cloud service provider may qualify for limitations on liability as an internet service provider under section 512.

Fair use is an affirmative defense against copyright infringement. It is found in section 107 of the Copyright Act, which reads:

> 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

[97] *IBM Cloud Computing: Overview*, IBM, http://www.ibm.com/cloud-computing/us/en/?csr=agus_ibmcloud_2012331&cm=k&cr=google&ct=USBRB301&S_TACT=USBRB301&ck=ibm_the_cloud&cmp=USBRB&mkwid=s4aKQz66c_11089732696_432qb116465 (last visited June 29, 2012).
[98] *Google Docs*, GOOGLE, http://www.google.com/google-d-s/documents/index.html (last visited July 12, 2012).
[99] Carrie Bodner, *Master Copies, Unique Copies and Volitional Conduct: Cartoon Network's Implications for the Liability of Digital Storage Lockers*, 35 COLUM. J. L. & ARTS (forthcoming 2012).
[100] Online Cloud service providers also benefit from the 512 safe harbor protections under section 512. Service providers that qualify for the 512 safe harbor are exempt from primary and secondary liability. For more details on the 512 safe harbor see the response to Session 2 and 3, question 1(1.2). For more on the difference between a private and public performance, see our discussion of *Cartoon Networks LP v. CSC Holdings Inc.* in Sessions 2 and 3, question 1(1.2).

> 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.

17 U.S.C. § 107.

Courts have weighed and applied these factors differently over the years.[101]

5.2 – Copyright-avoiding models on the basis of – presumed – exceptions to copyright liability or limited interpretations of the "making available" right

1) To what extent do the operators of cloud services benefit from a narrow interpretation of the making available (or communication to the public, or public performance) right?

As discussed above, the United States does not have a "making available" right denominated as such, but the rights of reproduction, distribution, public performance and public display provide many of the same protections. However, some courts have construed these rights narrowly in certain respects that benefit service providers. First, some courts have concluded that where a provider has set up a highly automated system, there is no volitional conduct by the service provider in copying or performing copyrighted works at the direction of users, and therefore service providers cannot be directly liable for infringement. This is discussed further in our answer to Session 2 and 3, question 1(1.2).

Another way in which some courts have interpreted rights to the benefit of Cloud service providers is in their narrow view of what it means to publicly perform or publicly display copyrighted content.[102] The court in *Cartoon Network LP v. CSC Holdings, Inc.* (discussed above in response to Sessions 2 and 3, question 1(1.1)), held that programming copied and stored at a customer's request by Cablevision's automated system could be

[101] *Compare* Castle Rock Entm't, Inc. v. Carol Pub. Group, Inc., 150 F.3d 132, 145 (2d Cir. 1998) (emphasizing the purpose factor by implying that the amount and substantiality factor was not satisfied because the purpose is illegitimate), *and* Warner Bros. Entm't Inc. v. RDR Books, 575 F. Supp. 2d 513, 548 (S.D.N.Y. 2008) (underscoring the purpose factor by making an "amount and substantiality" analysis according to the following guideline: "Depending on the purpose, using a substantial portion of a work, or even the whole thing, may be permissible."), *with* Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 566 (1985) ("[The] last factor [i.e. the effect on the market value] is undoubtedly the single most important element of fair use.").

[102] U.S. copyright law provides an exclusive public performance and public display right. 17 U.S.C. §§ 106(4)-(6). Thus, private performances and displays do not implicate the performance and display rights under U.S. copyright law.

transmitted to the customer at the time of her choosing without infringing the public performance right. The court looked at the potential audience of each individual transmission and determined that "because the RS-DVR system, as designed, only makes transmissions to one subscriber using a copy made by that subscriber, we believe that the universe of people capable of receiving an RS-DVR transmission is the single subscriber whose self-made copy is used to create that transmission."[103] Accordingly, the court held the transmissions were not infringing because they were not communicated "to the public."[104]

In *In re Cellco*, the court ruled that cell phone ringtones were not a public performance because they were not directly accessible to the public during the download process and, as the Second Circuit had discussed in the *Cartoon Networks* case "only one subscriber is capable of receiving this transmission or performance, the transmission is not made to the public and is not covered by the Transmission Clause." [105] As discussed above in response to Session 2 and 3, question 1(1.2), the court in *Warner Brothers Entertainment, Inc., v. WTV Systems, Inc.,* took a broader view of the meaning of public performance. [106]

There has also been controversy over the scope of the public distribution right. Content providers have alleged that users who upload sound recordings to the internet thereby violate the copyright owner's public distribution rights. Some courts have ruled that no violation of the distribution right occurs unless another user actually downloads the song in question. For example, in *Arista Records, Inc. v. MP3Board, Inc.*, the District Court in New York concluded that merely making copyrighted recordings available without authorization through links posted by users to defendant's website did not sufficiently establish unlawful distribution or dissemination.[107] In *London-Sire Records, Inc. v. Doe 1*, a Massachusetts District Court held that "merely exposing music files to the internet is not copyright infringement [but] evidence supports an inference that the defendants participated in the peer-to-peer network precisely to share copyrighted files."[108]

2) According to the law in your country, what is the legal status (primary or secondary liability - contributory infringement or vicarious liability; aiding and abetting, other liability such as an inducer, "Störer") of the provider of cloud services with regard to copyright infringing content uploaded by its users?

[103] *Cartoon Network*, 536 F.3d at 137.

[104] The definition of public performance is found in section 101. At issue here was the "transmit clause" of section 101 which says that "to perform or display a work "publicly" means…to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) [any place open to the public or at any place where a substantial number of persons outside of a normal circle of family and its social acquaintances is gathered] or to the public, by means of any device or process…" Recall that in the *Cartoon Network* case only direct liability, and not secondary liability, was at issue.

[105] In re Cellco P'ship, 663 F. Supp. 2d 363, 371-74 (S.D.N.Y. 2009).
For more details on the "Transmission Clause" also known as the "transmit clause", *see supra* note 104.

[106] 824 F. Supp. 2d 1003.

[107] Arista Records, Inc. v. Mp3Board, Inc., No. 00 CIV. 4660, 2002 WL 1997918 at *3, 4 (S.D.N.Y. Aug. 29, 2002).

[108] London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d 153, 176 (D. Mass. 2008). *See also* Hotaling v. Church of Jesus Christ of Latter-Day Saints, 118 F.3d 199 (4th Cir. 1997) (In order to show distribution of a copyrighted work, a party must show that an unlawful copy was actually disseminated to the public.); Arista Records LLC v. Lime Group LLC, 715 F. Supp. 2d 481, 507 (S.D.N.Y. 2010) (discussing that making content available is insufficient to establish actual infringing activity).

Unless they comply with the requirements of the section 512 safe harbors, discussed below in question 3, Cloud service providers can be held primarily or secondarily liable and can be guilty of contributory infringement or vicarious liability in connection with infringing material uploaded by its users. Secondary liability embraces vicarious liability and contributory liability (including liability for inducement). If a service provider fails to meet the requirements of the section 512 safe harbor, it is not automatically deemed liable for such infringement; a court will evaluate the merits of a rightholder's claim according to the case law.

As the Supreme Court explained in *MGM Studios, Inc. v. Grokster, Ltd*.:

> When a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability on a theory of contributory or vicarious infringement. One infringes contributorily by intentionally inducing or encouraging direct infringement and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it.

545 U.S. 913, 929-30 (2005) (quoting In re Aimster Copyright Litig., 334 F.3d 643 (C.A. 7 2003)).

One can also be contributorily liable by furnishing the means for infringement with knowledge that it will be used to infringe. But the Supreme Court in *Sony Corp. of America v. Universal City Studios* held almost three decades ago that where the "means" is a staple article of commerce, the distributor will be contributorily liable only if that article has no substantial noninfringing use.[109] In *Sony*, the home video recorders distributed by Sony were found to have substantial noninfringing uses, yet Sony was not liable. However, in *Grokster*, a case decided 21 years after *Sony Corp.* involving peer to peer file-sharing, the Supreme Court ruled that *Sony* "did not displace other theories of secondary liability" and even if a defendant's product or service has a substantial noninfringing use, that defendant may still be liable if it took active steps to encourage direct infringement by its users.[110] The Court held that there was specific evidence that Grokster intended to cause copyright violations through its software, including (1) documents that demonstrated that Grokster was attempting to satisfy a "known source of demand for copyright infringement," i.e., former Napster users; (2) Grokster's failure to develop filtering tools or other means to limit infringing activity; and (3) Grokster's business model, which was based on advertising revenue that increased with high volume use, which the record shows was infringing.[111]

In *Columbia Pictures Industries, Inc. v. Fung,* an infringement suit brought by several large rightholders against the owner of a peer-to-peer network, a California district court

[109] 465 U.S. 113 (1984).
[110] 545 U.S. at 934.
[111] *Id.* at 939-40. The Court was clear, however, that neither of the latter two factors would, without evidence of intent, support a finding of inducement liability. *Id.* at 939 n.12 & 940.

explored the relationship between inducement liability and the section 512 safe harbors.[112] The court stated that "inducement liability and the Digital Millennium Copyright Act safe harbors are inherently contradictory. Inducement liability is based on active bad faith conduct aimed at promoting infringement; the statutory safe harbors are based on passive good faith conduct aimed at operating a legitimate internet business."[113] Thus, if a website is inducing users to infringe, the website should not be able to escape liability through 512's safe harbor provisions.[114]

The reward programs established by many of the service providers discussed throughout this survey, especially those that focus on popular music, seem prime examples of contributory infringement or "inducement."

3) In your country, do cloud service providers benefit from an exception to liability (such as, e.g., under the EU e-Commerce Directive), and if so, to what extent (e.g., total exemption from liability or exemption only from duty to pay damages)? Please cite to and briefly describe statutory provisions and relevant case law.

Section 512 of the Copyright Act provides "safe harbors," or limitations on liability, for internet service providers (ISPs) under certain conditions. Without the section, ISPs could be liable more often for infringing content on their sites or transmitted through their service.

There are four types of service provider activities protected under section 512: (a) transitory digital network communications, (b) system caching, (c) storing information posted by users on their system or network; and (d) providing information location tools that may direct users to infringing material.[115] If a service provider qualifies for a safe harbor it is exempt from monetary damages and its activities can be enjoined only in very limited circumstances.

Each of the safe harbors described above has certain requirements. For example, section 512(c) provides:

> INFORMATION RESIDING ON SYSTEMS OR NETWORKS AT DIRECTION OF USERS.—
>
> (1) IN GENERAL. — A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider -

[112] No. CV 06-5578 SVW(JCx), 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009).
[113] *Id.* at *18.
[114] For an argument that inducing infringement should not categorically remove a service provider from the safe harbor provisions, see R. Anthony Reese, *The Relationship Between the ISP Safe Harbors and Liability for Inducement*, 2011 STAN. TECH. L. REV. 8 (2011).
[115] Note that "service provider" is defined differently for § 512(a) and for the balance of § 512. *See* § 512(k).

> (A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
>
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
>
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
>
> (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

The required notification is discussed below.

As noted above, section 512(c) protects online service providers for hosting content residing on systems or networks.[116] Provided that the other requirements under the section are met, online service providers are exempt from liability arising from "infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider."[117] A conservative interpretation of the key language of the statute is that section 512(c) exclusively applies to online storing. However, some courts have concluded that section 512(c) "is clearly meant to cover more than mere electronic storage lockers."[118] For instance, in *UMG Recordings, Inc. v. Veoh Networks, Inc.*, the Central California District Court interpreted "by reason of storage at the direction of a user" to include conduct that arose from facilitating access to user-stored material.[119] The court there held that that the reproduction of works through the creation of differently-formatted or condensed videos, the public performance of works when users stream stored content, and the distribution of works when users access stored videos through downloading all fall within the scope of protected activities.[120]

In *Viacom v. YouTube,* Viacom argued the "related videos" function that identifies and provides thumbnails of clips of videos that are similar to the videos that users selected is not an activity that is exempt under section 512(c). Relying on the *UMG Recordings v. Veoh Networks* case, the Second Circuit disagreed and ruled that YouTube's related videos function falls within the scope of activities protected by section 512(c) because, the algorithm used for the related video feature "is closely related to, and follows from, the storage itself," and is

---

[116] 17 U.S.C. § 512(c).
[117] *Id.*
[118] UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081, 1088-89 (C.D. Cal. 2008). This case is discussed further in our answer to question 4 below.
[119] *Id.*
[120] *Id.* at 1087-88, 1092.

"narrowly directed toward providing access to material stored at the direction of users."[121] Some courts have also broadly construed the statute to include activities that were not directly "at the direction of a user".

In *Io Group, Inc., v. Veoh Networks, Inc.*, the court held that the activities that stemmed from Veoh's automated software qualified for section 512(c) protections.[122] Veoh's software automatically processed user-submitted content and reconstructed the content in a user-friendly way. In its analysis, the court stated that, "[i]nasmuch as this is a means of facilitating user access to material on its website" the automated software functions are included.[123]

There are additional requirements for the service provider to take advantage of the section 512 safe harbors. For example, the provider must designate an agent to receive notifications of claimed infringement.[124] Also, it must adopt, implement, and notify subscribers or users of a policy that provides for the termination of the accounts of repeat infringers and must ensure that the service's operations do not impede other sites' standard technical protection measures.

Section 512 has other provisions as well. It limits the liability of public or nonprofit institutions of higher education that serve as ISPs in situations where faculty members or graduate students employed by the institution post infringing material, provided the institution has been generally compliant with United States copyright law.[125] Section 512 also provides for penalties on those who falsely file claims of infringement[126] and excepts from liability those who, in complying with a notice of infringement, become subject to claims from users or subscribers, provided they notify the user or subscriber of the removal and reinstate the work within 10 days if the material is deemed not to be infringing.[127] It also provides guidelines for users or subscribers who believe their postings were taken down in error to demand that their postings be reinstated.[128] Section 512(j) lists instances when a court may grant an injunction to an ISP in cases of alleged infringement.

4) Also according to the law in your country, what duty of care is owed by cloud service providers to monitor and eventually remove copyright infringing content?

Cloud service providers do not have an affirmative duty to monitor their sites for infringement. Section 512(m) states that safe harbor protection cannot hinge on "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of this subsection."[129] However, under sections 512(c)(1)(A) and 512(d)(1), providers do have a duty to respond to "red flags" that make infringement apparent to the reasonable person. For instance, if a website permits users to post links to sites with the names

[121] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 40 (2d Cir. 2012) (quoting *UMG Recordings, Inc.*, 620 F. Supp. 2d at 1092.).
[122] Io Group, Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008).
[123] *Id.*
[124] § 512(c)(2).
[125] § 512(e).
[126] § 512(f).
[127] §§ 512(g)(1)-(2).
[128] § 512(g)(3).
[129] § 512 (m).

'pirate' or 'bootleg', some courts have held that the service provider is no longer protected by 512's safe harbor provisions.[130] Red flags, however, must be obvious to the reasonable person, and require no further investigation by the host service provider.[131]

Whether, in the event of repeat notices concerning the same content, there is a duty to monitor, and other responsibilities of service providers under section 512, have been explored in a number of cases. For example, in *Viacom Intern., Inc. v. YouTube, Inc.*[132] (further discussed in question 7 of this Session) the entertainment conglomerate Viacom sued YouTube,[133] a video-sharing site now owned by Google, claiming that the website was directly and secondarily liable for copyright infringement of the large number of Viacom-owned materials that were posted on the site without authorization by users between 2005 and 2008.[134] YouTube allows users to upload and view video clips free of charge. In order to upload a video clip a user must register with the site, but no registration is required to view a clip. In registering, users must pledge that they will not upload infringing material. YouTube makes a copy of each video as it is uploading. Once a video is uploaded, YouTube makes further copies as it converts the video to a format compatible with a multitude of platforms.

Viacom alleged that YouTube's activities violated the company's exclusive rights of public performance, public display and reproduction in the works. Specifically, Viacom alleged that YouTube was not eligible for the safe harbor protections of section 512(c) because it ignored "red flags" that made the infringing activity apparent. Viacom argued that awareness of facts and circumstances from which infringing activity is apparent does not require specific knowledge of each individual incidence of infringement. The District Court had earlier held – and the Court of Appeals affirmed – that the knowledge of such infringing activities had to be specific and the clips identifiable. The Second Circuit ruled:

> [t]he actual knowledge provision turns on whether the provider actually or "subjectively" knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement objectively obvious to a reasonable person.

Viacom, 676 F.3d at 31.

As a consequence, Viacom was unsuccessful in its claim that YouTube had a duty to proactively identify and eliminate certain clips that Viacom repeatedly warned were

---

[130] *See, e.g., Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 643-44 (S.D.N.Y. 2011). *But see* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007) (The court rejected the plaintiff's argument that the defendant was aware of apparent infringing activity because the defendant provided services to "illegal.net" and "stolencelebritypics.com". The court explained that these terms are not necessarily an admission of illegal conduct, but rather the terms may be used to increase appeal.) For a discussion of the "red flags" discussion in *Viacom Intern., Inc. v. YouTube, Inc.*, see response to Sessions 5, question 5.2(4).

[131] *See* UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1108 (C.D. Cal. 2009) *aff'd sub nom.* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011); *Viacom*, 676 F.3d at 31-32.

[132] 676 F.3d 19.

[133] YOUTUBE, *supra* note 7.

[134] During the time period that is the subject of the suit, YouTube had not implemented a general filtering mechanism. It has since done so.

unlawfully posted.[135] However, the court held that a reasonable juror could find that YouTube in some circumstances knew of clearly infringing material that it failed to remove, and remanded to the district court on this issue.

Plaintiffs also alleged that the District Court erred in failing to rule in their favor despite evidence that YouTube was "willfully blind" to the infringing activity.[136] This common-law doctrine attributes actual knowledge to the person or entity who consciously avoids confirming the existence of blatant infringements. While the Court of Appeals held that the statute rejects an affirmative duty to monitor one's site, it noted that the District Court should have considered whether or not YouTube was willfully blind to infringements of which it should have known, and directed the district court to consider this issue on remand.[137]

The Second Circuit Court of Appeals also addressed Viacom's argument that YouTube did not qualify for protection under section 512(c) because it earned a financial benefit from infringing activities that it had the right or ability to control and that, through its uploading and storage processes, had significant control over the materials posted on its site. Both issues were remanded to the District Court for further consideration.

In *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, the Ninth Circuit Court of Appeals addressed service providers' monitoring and takedown reponsibilities.[138] Veoh is an online video service similar in many respects to YouTube, although Veoh allows users to download as well as stream video clips. Veoh has on its system user-uploaded videos as well as partner content provided by major media companies. In order to upload content to Veoh's system, users must register. For every upload, a message appears stating that users should not upload videos that infringe copyright. Once a video is uploaded, the content is automatically made available to users, including non-registered users..

Veoh complies with section 512(c)'s obligations concerning takedown of infringing content for which it receives a notification. In 2006 Veoh adopted a rudimentary filter system and upgraded to an Audible Magic system the following year. Veoh claimed it attempts to filter out content that copyright holders have not authorized to appear on Veoh's system. Moreover, when content is taken down pursuant to a notification, Veoh uses filtering technology to automatically disable access to identical videos and block subsequently submitted duplicates.[139] Veoh also terminates the accounts of repeat infringers.

UMG alleged that Veoh was liable for direct and secondary infringement, and for inducing copyright infringement. UMG contended that after Veoh was notified of specific infringing material, Veoh should have sought out actual knowledge of other infringing videos and removed the content. UMG also alleged that Veoh was aware of the widespread

---

[135] For a criticism of the court's decision on this issue, see Peter S. Menell, *Judicial Regulation of Digital Copyright Windfalls: Making Interpretive and Policy Sense of Viacom v. YouTube and UMG Recordings v. Shelter Capital Partners*, THE MEDIA INSTITUTE (May 3, 2012), http://www.mediainstitute.org/IPI/2012/050212.php.

[136] *Viacom*, 676 F.3d at 35.

[137] The Second Circuit did say, however, that willful blindness was not the same as a duty to monitor, and so this passage may limit the websites' duties, but it does not fully abrogate the willful blindness doctrine. *Id*.

[138] 667 F.3d 1022.

[139] *Id.* at 1028.

infringement occurring on its system and thus Veoh should have identified and taken down copyright-infringing material, and that its efforts at filtering were "too little, too late."

The court rejected UMG's broad conception of "knowledge" under section 512 (c)(1)(A), concluding that merely hosting copyrightable content with general knowledge that its service could be used to post infringing material did not constitute knowledge sufficient to take Veoh out of the section 512(c) safe harbor. According to the court, the DMCA places the burden of identifying infringing material on the rightholders.[140] The court also rejected UMG's argument that Veoh had the right and ability to control infringing activity, explaining that "'right and ability to control' under § 512(c) requires control over infringing activity that the provider knows about."[141]

The District Court for the Southern District of New York also looked at a service provider's duties in *Capitol Records, Inc. v. MP3tunes, LLC*.[142] In this case, plaintiffs EMI and fourteen other record companies sued Michael Robertson, creator of MP3Tunes, a website that sold music in the mp3 format but also had a component that allowed users to store music in personal online lockers on the Cloud. Songs uploaded to a locker could be played by the user through any internet-abled device. MP3tunes.com had a sister website, Sideload.com which allowed users to search the internet for free songs. If the Sideload.com user had an MP3tunes.com account, Sideload.com would ask the user if he wished to have the song downloaded to his MP3tunes.com locker. The songs Sideload.com found would also be added to Sideload.com's index of searchable songs.

MP3tunes.com claimed it was neither directly nor secondarily liable. The plaintiffs claimed MP3tunes.com was ineligible for the section 512 safe harbors because it did not satisfactorily implement a repeat-infringer policy, did not respond to take down notices quickly enough, ignored signs of widespread infringement and profited from the infringing activity. The court ruled that the ISP responsibly implemented its repeat-infringer policy, terminating accounts where necessary, tracking users' identities and responding promptly to takedown notices. The court also decided that MP3tunes.com was not liable for direct infringement because it was its users who chose what songs to upload, and merely enabling a party to download infringing material is not an infringing act.[143] The court ruled, however, that the company was ineligible for the section 512 (c) safe harbor with respect to infringing songs in users' digital lockers that MP3tunes failed to remove after receiving takedown notices. The court ultimately found MP3tunes.com contributorily liable for infringement of this material, because it had reason to know about the infringing activities and provided the site and facilities for the infringing activities.

5) What evidence must a rightholder present in order to have infringing content removed?

In order to have infringing content removed, a rightholder must provide a notification of claimed infringement in writing to the designated agent of a service provider. The notification must include "substantially the following":

---

[140] *Id.* at 1038.
[141] *Id*. at 1043.
[142] 821 F. Supp. 2d 627.
[143] The court wrote that if it were, "the DMCA's purpose – innovation and growth of internet services – would be undermined." *Id.* at 645.

> (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
> (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
> (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
> (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
> (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
> (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

17 U.S.C. § 512 (c)(3).

A notification that does not comply substantially with these requirements may not be considered in determining whether a service provider has actual or red flag knowledge of infringement. After the service provider has removed the allegedly infringing material pursuant to a compliant notification, the party who posted it can file a counter-notification on the service provider. The service provider must then put the material back up within ten business days unless the rightholder files an action for infringement of the material in dispute.[144]

6) In your country, are there any contracts that have been concluded between cloud service providers and rightholders concerning the use of copyrighted material by the users of the cloud services?

Yes; Cloud service providers generally use terms of service agreements to bind rightholders to conditions concerning the use of their work by third parties.[145] When the rightholders are media companies, which have greater bargaining power than general users, Cloud service providers use customized licensing agreements.[146] Through these agreements with service providers, media companies grant non-exclusive rights in their work to Cloud users. For example, the agreement between YouTube and WMG allowed end-users to

[144] § 512(g).
[145] For a discussion of the types of rights rightholders transfer to third-parties see response to Session 4, question 4.
[146] *See* Yafit Lev-Aretz, *supra* note 69, at 153-154.

incorporate music from WMG's music catalog into videos that users create and upload to YouTube.[147]

7) In your country, what copyright-avoiding cloud services are operating successfully, and what services that sought to be avoiding copyright have been banned and eventually shut down?

We assume that a successful copyright-avoiding Cloud service is a Cloud service that has not been forced to change its business practices due to copyright infringement liability. Some service providers, such as MP3tunes, YouTube, or Cablevision, have so far survived challenges and continue to operate. Some Cloud service providers operate successfully because they do not violate copyright law while others are protected by the section 512 safe harbors. One example of a non-infringing service provider is Dropbox, an online storage locker that allows users to store and make available content. Online service providers like MP3tunes and YouTube, on the other hand, can take advantage of the section 512 safe harbors discussed above. If they comply with the requirements, service providers will not be liable for activities enumerated in section 512, although individual users may be.[148] For example, the court in *Capitol Records v. MP3tunes*[149] held that the section 512 safe harbor protected some but not all of MP3tunes' activities. It did not protect MP3Tunes in instances where the company received notices of copyright infringed material that was posted and took no action.

The *Viacom v. YouTube* case also deals with the scope of the section 512 safe harbor protections.[150] As discussed above, the case has been remanded to the district court, which has not yet issued a final judgment. Should it find that YouTube had awareness of or willfully blinded itself to specific infringements, YouTube will not qualify for safe harbor protection with respect to those infringements. However, YouTube has significantly changed its service since the period complained of in the *Viacom* suit (for example, it has added filtering), so it is very unlikely that the *Viacom* suit, however it is finally decided, will cause YouTube to shut down.

Megaupload[151] and *Warner Brothers Entertainment v. WTV System*[152] (the case mentioned earlier involving the Zediva system) are two of the more recent cases of unsuccessful copyright-avoiding services. The Zediva case is discussed above in our response to Session 2 and 3, question 1(1.2). Megaupload.com was a commercial online service that reproduced and distributed copies of popular copyrighted content without authorization. Users were able to upload, stream, and download content that was stored on remote servers and in remote cyber lockers. Allegedly engaged in criminal copyright infringement worldwide, the Megaupload.com website was seized and the U.S. Department of Justice commenced a

[147] *Id.* at 156.
[148] 17 U.S.C. § 512. For a discussion of §512 see the response to Session 5, question 5.2(3).
[149] Discussed in the response to Session 5, question 5.2(4).
[150] For a discussion of the facts of this case, see the discussion in Session 5, question 5.2(4).
[151] Megaupload is not a U.S. based company. However, we include the service provider because the U.S. Department of Justice has commenced a criminal case against the owners of the company.
[152] *Warner Bros. Entm't, Inc.*, 824 F. Supp. 2d 1003. For more details about this case see the response to Session 2 and 3, question 1(1.2).

criminal suit against Megaupload Ltd. and its owners.[153] Megaupload has been charged with several counts related to criminal copyright infringement.[154] The suit is in the pre-trial phase.

8) In your country, are there any legislative changes under discussion as regards the liability of service providers who provide for cloud services? In particular, do you think that liability of service providers will be reduced or, rather, increased?

Neither rightholders nor service providers are entirely happy with the current notice-and-takedown regime of section 512, but there are currently no legislative proposals to amend it.

In 2011, bills were introduced in the U.S. Congress to enhance the ability of law enforcement officials and rightholders to hold accountable foreign websites engaged in facilitating piracy and counterfeiting of U.S. intellectual property (sometimes referred to as "rogue websites"). S. 968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property (PROTECT IP Act or PIPA) was introduced in the Senate on May 12, 2011; five months later H.R. 3261, the Stop Online Piracy Act (SOPA) was introduced in the House of Representatives. In broad brush, PIPA would have allowed the Attorney General to bring an action against a foreign website (or the owner or operator thereof) dedicated to infringing activities. The Attorney General could seek an injunction against the site, and also apply to the court for an order to require U.S.-based domain-name servers and search engines to prevent access to the site from the U.S., and U.S. based advertisers and financial transaction providers to stop providing services to the site. Rightholders could also sue such a site, whether domestic or foreign, or the owners or operators thereof. Rightholders could also seek a court order requiring financial transaction providers and internet advertising services to stop activities with respect to rogue websites. These sites would not be taken down, and individuals in other countries could continue to access them.

SOPA is similar to PIPA but different in some respects. It would permit rightholders to bring an action against a rogue website and obtain a court order to require financial transaction providers and internet advertisers to stop serving that site, but only if the rightholder first filed a notification on the provider or advertiser and the notification were ignored or a counter-notification were filed. Among other things, SOPA would also have created criminal penalties for online streaming of copyrighted material.[155]

Due to broad opposition (ostensibly based on concerns about the integrity of the internet and internet "censorship," among other things), many legislators have distanced themselves from the bills and it is apparent that the bills in their current form will not move forward. It is unclear whether new legislation will be introduced.

9) Do you see any progress regarding filtering technology?

[153] United States v. Kim Dotcom, No. 1:12CR3, 2012 WL 517537 (E.D.Va.).
[154] *Id.*
[155] SOPA, PIPA and a third related bill, S. 2029 (the Online Protection and Enforcement of Digital Trade Act) are available at http://www.thomas.gov. For a detailed summary of these bills, see BRIAN T. YEH, CONG. RESEARCH SERV., R7-5700, ONLINE COPYRIGHT INFRINGEMENT AND COUNTERFEITING LEGISLATION IN THE 117TH CONGRESS (2012), *available at* http://www.kelleydrye.com/email/PIPASOPAandtheOPENAct.pdf.

Filtering technology is constantly evolving in the U.S. Filtering technology has been defined as "automated content identification technologies" that are used to monitor service providers' systems for potential copyright infringements."[156] Filters use fingerprinting, metadata, watermarks, and other forms of technology to monitor audio, video, and image-based content.[157] Audible Magic[158] and Vobile DNA[159] are examples of some of the more common copyright filters. Currently, most of the major user-generated content websites use some form of filtering.[160]

Several media companies and service providers have joined together to advocate increasing the role of filtering technology in copyright enforcement and produced a document setting out the terms of their agreement.[161] These "Principles for User Generated Content Services" mandate that all user-generated content sites employ filtering technology and allow rightholders to determine how matches that the filters find should be treated.[162] The Principles also ask service providers to communicate the importance of copyright to users, to track repeat infringers and to identify and remove links to sites that are clearly used primarily for infringement. In return, the signers of the document agree to work with service providers to ensure that fair use of copyrighted materials is accommodated and pledge that if a service provider adheres to the Principles, the content providers will not assert infringement claims in the event that infringing content is posted by users.[163]

In response, several American research institutions and interest groups drafted the Fair Use Principles of User Generated Video Content, which are guidelines designed to facilitate copyright enforcement and at the same time protect fair use.[164]

The groups have expressed concerns that use of filtering technology may overreach and screen out lawfully posted material, thus depriving end-users of their privileges under the

---

[156] This definition is excerpted from the Fair Use Principles for User Generated Content, https://www.aclunc.org/issues/technology/blog/asset_upload_file939_6218.pdf, further described below. It is, however, a fairly accurate, unbiased description of the filtering process.

[157] *See, e.g.*, *Applications*, VOBILE, http://www.vobileinc.com/applications.html (last visited July 11, 2012).

[158] AUDIBLE MAGIC, http://audiblemagic.com/ (last visited July 5, 2012).

[159] *Technology*, VOBILE, http://www.vobileinc.com/technology.html (last visited July 11, 2012).

[160] Sonia K. Katyal & Jason M. Schultz, *The Unending Search for the Optimal Infringement Filter*, 112 COLUM. L. REV. SIDEBAR 83, 93 (2012). *See also* Sonia K. Katyal, *Filtering, Piracy, Surveillance, and Disobedience*, 32 COLUM. J.L. & ARTS 401, 401-403.

[161] Companies including CBS Corporation, Sony Pictures, Disney, Viacom, Microsoft, NBCUniversal and Veoh developed and adopted the Principles for User Generated Content Services. These guidelines can be found at http://www.ugcprinciples.com/ (last visited July 11, 2012). *See also* William C. Harrelson, *PART II: Filtering the Internet to Prevent Copyright Infringement: ISP Safe Harbors and Secondary Liability in the U.S. and France*, 35 NEW MATTER, no. 2, 2010 at 7.

[162] Principles for User Generated Content Services, http://www.ugcprinciples.com/. *See also*, Alan N. Braverman & Terri Southwick, *The User-Generated Content Principles: The Motivation, Process, Results and Lessons Learned*, 32 COLUM. J. L. & ARTS 471 (2009).

[163] *Id*.

[164] The organizations that endorse the Fair Use Principles for User Generated Video Content include the following: Electronic Frontier Foundation (a digital rights advocacy group); the Center for Social Media from American University's School of Communications; the Program on Information Justice and Intellectual Property from American University's Washington College of Law; Public Knowledge (a public interest group dedicated to open internet and public access); the Berkman Center for Internet and Society at Harvard Law School; and the American Civil Liberties Union (ACLU) of Northern California. The document can be found at https://www.eff.org/files/UGC_Fair_Use_Best_Practices_0.pdf (last visited July 18, 2012).

fair use doctrine.[165] In a report to the Federal Communications Commission, Public Knowledge, an interest group dedicated to public access and an open internet, identified several concerns connected to filtering technology.[166] It argued that technology that fails to account for nuanced uses and is designed to automatically block unauthorized content that matches copyrighted material can be over-inclusive and harmful to lawful and protected forms of speech.[167] These interest groups recommend that content should not be automatically blocked unless the content was flagged for video and audio matches and a substantial portion of the flagged content is comprised of a single copyrighted work.[168] Additionally, the report emphasizes that end-users should have an opportunity to dispute automated filters and respond to DMCA notices and takedowns.[169] In the same vein, the report stresses that instead of cancelling an account, which may block lawful content, automated blocks should remove only content that is specifically flagged.[170] YouTube is an example of a service provider with a policy that takes into account some of these guidelines. For example, when YouTube's Content ID tool automatically removes users' content, YouTube users can submit a complaint and have the content reposted.[171]

In light of the developments in filtering technology and the discourse concerning a balance between private and public interests, we foresee service providers using filter technology and graduated responses. Graduated response programs vary. In general, a graduated response is an approach whereby users are given two or more warnings of infringing or potentially infringing content before service providers take action, which may include blocking content or terminating services.[172]

In July 2011, a number of major content providers and their trade organizations entered into a Memorandum of Understanding with some of the largest ISPs to create the Center for Copyright Information (CCI).[173] One of the CCI's main goals is to set up a system through which content owners can notify participating ISPs of possible instances of infringement by a specific computer (identified through its Internet Protocol address). The ISP will then alert the user responsible for the potentially illegal activity, explain why the action is illegal and provide advice on how to legally obtain audiovisual content and avoid receiving further alerts. These alerts will carry no legal consequences, but repeat offenders will have to acknowledge receipt of the warnings and, eventually, contact the ISP to discuss the matter.

5.3 – "Copyright-avoiding" business models operated by authors for the "Cloud"

[165] For more details on fair use, see Session 5, question 5.1(2).
[166] MEHAN JAYASURIYA ET AL., FORCING THE NET THROUGH A SIEVE: WHY COPYRIGHT FILTERING IS NOT A VIABLE SOLUTION FOR U.S. ISPS (2009), *available at* http://www.publicknowledge.org/pdf/pk-filtering-whitepaper-200907.pdf.
[167] *Id.* at 1, 47-49.
[168] *Id.*
[169] *Id.*
[170] *Id.*
[171] A *Guide to YouTube Removals*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/intellectual-property/guide-to-youtube-removals (last visited June 18, 2012).
[172] Peter K. Yu, *The Graduated Response*, 62 FLA. L. REV. 1373, 1374 (2010).
[173] This Memorandum is available at http://www.copyrightinformation.org/sites/default/files/Momorandum%20of%20Understanding.pdf.

1) In your country, is there a noticeable use of "copyright-avoiding" business models, such as Creative Commons (CC) or comparable open content licenses by rightholders with respect to cloud-based exploitations of works?

There is a noticeable use of Creative Commons (CC) and other open source licenses for a range of works. Software is commonly licensed under an open source model; CC licenses are frequently used by academics to encourage dissemination of their journal articles. They are also used by creators and performers seeking to break into a field and "become known." Several online services have added CC search capabilities which make it easier for users to exploit copyright-avoiding business models. For example, Google has added features to its search engine that allow users to identify images under various creative commons licenses.[174] Flickr also added a similar feature to its search engine.[175] At the moment, there are over forty-thousand photos that are posted on Flickr's CC page.[176] Vimeo provides similar features for audiovisual works.[177] Currently, over one million videos are posted on Vimeo's creative commons page.[178] ccMixter is a remixing site that provides music licensed by Creative Commons.[179] Currently, there are over three-hundred pages of songs that are free for commercial use that are posted on the ccMixter website.[180]

It is increasingly common for academics and researchers to deposit their articles in digital repositories that permit free public access to scholarly articles and other materials. (They do not thereby wholly avoid copyright, e.g., they retain derivative work rights and the right to publish in other formats.) One highly respected open access site is PubMed Central (PMC), a freely accessible digital archive of biomedical and life sciences research journal literature managed by the U.S. National Library of Medicine in the National Institutes of Health (NIH). PMC is committed to preserving the journal literature "in a form that ensures unrestricted access to it over the longer term."[181]

A 2008 U.S. law requires that the final, peer-reviewed manuscripts of articles that result from research funded by the National Institutes of Health be sent to PubMed Central.[182] Some private foundations that fund scientific research also require that the resulting articles be published on PubMed Central.[183] Journal publishers deposit articles in PubMed Central pursuant to voluntary agreements. Some publishers deposit their content in PMC immediately after publication. Others, however, wait for a year or more after publication in order to avoid adversely affecting their own market.

---

[174] *See Find Creative Commons Images with Image Search*, OFFICIAL GOOGLE BLOG, http://googleblog.blogspot.com/2009/07/find-creative-commons-images-with-image.html (last visited July 13, 2012).
[175] *See Creative Common*, FLICKR, http://www.flickr.com/groups/creativecommons/ (last visited July 13, 2012).
[176] *Id.*
[177] *See Creative Commons on Vimeo*, VIMEO, http://vimeo.com/creativecommons (last visited July 13, 2012).
[178] *See id.*
[179] *Yea, But Is It Legal ?*, CCMIXTER, http://ccmixter.org/about (last visited July 13, 2012).
[180] *See Music Free for Commercial Use*, CCMIXTER, http://dig.ccmixter.org/free_music?offset=0 (last visited July 13, 2012).
[181] *See PMC Overview*, PMC, http://www.pubmedcentral.nih.gov/about/intro.html (last accessed June 20, 2012).
[182] Consolidated Appropriations Act, PL 110-161, Div. G, Title II, Section 218 (2008).
[183] *See, e.g., Authors' FAQs*, WELLCOME TRUST, http://www.wellcome.ac.uk/About-us/Policy/Spotlight-issues/Open-access/Guides-and-FAQ/WTD018855.htm (last accessed June 20, 2012); Howard Hughes Medical Institute Research Policies, http://www.hhmi.org/about/research/sc320.pdf (last accessed June 20, 2012).

Many institutions of higher education already have or are developing institutional "open access" repositories in which faculty and students are encouraged, or required, to deposit their scholarly articles or dissertations. For example, Harvard University has created a digital repository for faculty works and instituted a policy that requires faculty members to deposit their journal articles in that repository and to allow the university to make them freely available online, unless they receive a waiver.[184] The university provides guidance to faculty on how to negotiate changes to typical publishing contracts to reserve the appropriate rights.

2) If so, in what areas (music, literature, audiovisual works, scientific works etc.) are such licenses most often used?

See response to question 5.3 (1), directly above.

3) Are there any figures available as to how the authors of such works generate income from such cloud-based exploitations, and how much?

We are not aware of any reliable figures. To the extent that a right holder opts to use "copyright avoiding" business models, presumably he or she is relying on remuneration that can be obtained outside the copyright system, e.g., in the case of academic authors, on government or private grants, or on the financial benefits that ultimately come with a tenured position. In the case of authors or performers, it is possible that they derive revenue from sales of concert tickets, related merchandise, or through voluntary contributions. Crowdfunding, advertising, "freemium," and commons-based distribution are among several business models that authors or performers have used to generate income. Crowdfunding is a collective financing scheme where individuals contribute to a work for a stake (e.g. credits) in the project.[185] Authors can also receive earnings from advertisements posted on their websites or in their content. For instance, some YouTube members receive payments that are based on a share of advertising revenue generated when the public views the member's video.[186] Freemium is a business model where the basic service or product is provided for free, but a premium is charged for advanced features, functions, or goods.[187] Lastly, commons-based distribution is a strategy where authors share their revenues with the group of contributors who financed the creative work.[188]

---

[184] *See* Patricia Cohen, *At Harvard, a Proposal to Publish Free on the Web*, N.Y. TIMES, Feb. 12, 2008; Robert Mitchell, *Harvard to Collect, Disseminate Scholarly Articles for Faculty*, HARV. GAZETTE ONLINE (Feb. 14, 2008) http://news.harvard.edu/gazette/story/2008/02/harvard-to-collect-disseminate-scholarly-articles-for-faculty/.

[185] For instance, see http://www.kickstarter.com/discover for some examples of crowdfunding. Currently, "Space Command" is a film project that initially pledged to raise $25,000 and it has raised over $190,000. Third-parties that make financial contributions receive various rewards such as copies of the film or behind-the-scenes video content. *Space Command by Mark Zicree*, KICKSTARTER, http://www.kickstarter.com/projects/58936338/space-command?ref=home_spotlight (last visited July 12, 2012). "These Days: A Novel" is an example of a book that is financed through crowdfunding. The author of the book pledged to raise $10,000 and has raised over $11,000. Depending on the size of the donation, contributors to this book can receive copies of the book or acknowledgements. *These Days: A Novel by Jack Cheng*, KICKSTARTER, http://www.kickstarter.com/projects/jackcheng/these-days-a-novel?ref=home_location (last visited July 12, 2012).

[186] *YouTube Partner Earnings Information*, YOUTUBE, http://support.google.com/youtube/bin/answer.py?hl=en&answer=72902 (last visited July 5, 2012).

[187] David Bollier, *Sustainable Models for Creativity in the Digital Age*, DAVID BOLLIER (Feb. 28, 2011, 1:30PM), http://bollier.org/sustainable-models-creativity-digital-age (last visited July 5, 2012).

[188] *Id.*

4) Also in your country, what legal obstacles are authors faced with when making use of open content and CC-licenses?
Examples might be the unenforceability of such licences; the refusal to award damages for unauthorized commercial use of works that have been made available only for non-commercial use; collecting societies refusing to represent authors who want to market some of their works under a CC-licence; the exclusion of CC-authors from receiving remuneration under a private copying regime etc.

In *Jacobsen v. Katzer*, the Court of Appeals for the Federal Circuit addressed the question whether a copyright holder who broadly licensed his work for free public use under an "open source" license could bring an action for copyright infringement against a user who incorporated plaintiff's work in a software package without complying with the terms of the open source license (e.g., concerning attribution, use of copyright notice, description of changes to the source code, etc.).[189] The court held that the conditions in the open source license govern the use of the software unless the parties enter into an alternative arrangement. The court ruled that Jacobsen could bring an infringement claim against defendant who violated the terms of the license.

The United States' largest copyright clearance agency for text-based works, Copyright Clearance Center (CCC), represents authors who have previously licensed their work through Creative Commons (CC), provided the authors can represent that they still hold the rights they wish to license through CCC.

An author who has granted a Creative Commons license for a musical work – as long as the grant is not for all uses – may still join the performing rights organizations (PROs) BMI (Broadcast Music International) and ASCAP (the American Society of Composers, Authors and Publishers) and grant these organizations the right to license their musical works, including works subject to a CC license. This is because their members grant ASCAP and BMI only a non-exclusive right to license the public performance of their works, and ASCAP and BMI members always retain the right to directly license any of their works. The member must, however, inform the organization that there is another direct license in the work and provide the terms of that license. An ASCAP or BMI member that has directly licensed his or her works for a specific use will not be paid by the organization for performances covered by the scope of that direct license. In practice, it is difficult for a PRO member who has granted a CC license for a work to comply with this notice of direct license provision, because the CC license attaches to a work forever, regardless of where or in what medium it is performed.

Another practical problem for U.S. performing rights organizations (collectively, U.S. PROs) that arises from the grant of a CC license is that, although the CC license allows the author to limit her license to non commercial uses (the "NC" icon), the U.S. Copyright Act does not define commercial versus non-commercial public performances. For example, the U.S. PROs grant licenses to non-commercial public radio and television broadcasters and license non-for-profit entities that publicly perform music. Thus, under U.S. Copyright law, as written and applied, there is no framework for determining what is a non-commercial public performance of a musical work.

[189] 535 F.3d 1373 (Fed. Cir. 2008).

Last and importantly, the blanket licenses granted by ASCAP and BMI to music users permit the use of any and all songs in their varied and broad repertories of musical works—they do not grant licenses for the use of one specific work. Therefore, a music user who may be performing a work pursuant to a CC license would likely still require a performing rights organization license for the performance of musical works not subject to the CC license.

The United States does not have a private copying regime except with respect to digital audio recording devices and media, which are narrowly defined.[190]

Session 6
－Future Model of One-Stop-On-Line Licensing in the Cloud Environment

1) Does your country have specific private international law rules for copyright in particular and for intellectual property in general or are there general rules of private international law that apply in these circumstances? In particular do your country's rules of judicial competence (personal jurisdiction) make it possible to sue a foreign intermediary who makes it possible for infringements to occur or to impact in the forum? Which law applies in such instances? Would the law applicable to the primary infringement apply? Would the law of the intermediary's residence or place of business apply?

The rules that generally apply in actions brought in federal court apply to copyright.

Personal Jurisdiction

For questions of personal jurisdiction, federal district courts follow the rules of the state in which they sit. Most states have "long arm" statutes that give the state personal jurisdiction over someone who, although outside the state, causes injury within the state. For example, New York's long arm statute provides, inter alia, that a New York court may exercise personal jurisdiction "over any non-domiciliary . . . who, in person or through an agent,"

> [C]ommits a tortuous act within the state causing injury to a person or property within the state, except as to a cause of action for defamation of character arising from the act, if he (i) regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered, in the state, or (ii) expects or should reasonably expect the act to have consequences in the state and derives substantial revenue from interstate or international commerce….

N.Y. C.P.L.R. 302.

A recent case from the New York Court of Appeals (the highest court of the state) considered where the injury from online copyright infringement takes place, i.e., whether acts

[190] *See* 17 U.S.C. §§ 1001 (4)-(5).

of infringement cause injury to a person or property within the state. *Penguin Group (USA) Inc. v. American Buddha* involved a New York publisher's copyright infringement suit against an online library based in Oregon and Arizona that allegedly made free copies of the publisher's books available online.[191] The court held that, for purposes of the New York statute cited above, a New York-based copyright holder sustains an injury in New York when its copyrighted works are uploaded to the Internet outside of the state. The court explained that the "unique threat" posed by uploading a copyrighted work to the internet justified this result. According to the court, it was appropriate to consider New York the site of the injury in a case involving online copyright infringement dispersed throughout the country and possibly throughout the world.[192]

The court explained that its decision "does not open a Pandora's box allowing any nondomiciliary accused of digital copyright infringement to be haled into a New York court when the plaintiff is a New York copyright owner of a printed literary work."[193] It pointed out that there are other requirements of section 302 that would act as safeguards, and that as a constitutional matter an out-of-state defendant had to have "minimum contacts" with the forum state.

Recently, in *Mavrix Photo, Inc. v. Brand Technologies, Inc.*, the Ninth Circuit Court of Appeals held that an out-of-state defendant in a copyright infringement suit was subject to jurisdiction in California.[194] Mavrix, a Florida corporation, is a celebrity photo agency that sued Brand, an Ohio corporation, for loading Mavrix's photos to its website without authorization. The court held that Brand's activities met the requirements of due process. It concluded that Brand's acts were intentional; it was expressly aimed at California because Brand's website continuously sought to exploit the California market through sales and advertising for its own profit; and Brand caused foreseeable economic harm in California.

Application of U.S. Law

Some U.S. courts have held that U.S. law will apply to an act of infringement that takes place, at least in part, in the United States.[195] Other courts have held that at least one infringement must have taken place entirely in the United States for U.S. law to apply.[196] However, the courts are in agreement that where infringements take place entirely outside of the United States, U.S. copyright law will not apply.

In *Shropshire v. Canning*, the Canadian defendant uploaded a copyrighted video from Canada to YouTube's servers, located in California, for public performance within the United States.[197] The court held that U.S. law applied since the activity was not "wholly extraterritorial," and it was irrelevant that defendant didn't know that YouTube's servers were in the United States. But in *Elsevier Ltd. v. Chitika, Inc.*, the court concluded that if copies of plaintiffs' copyrighted books were uploaded in India and downloaded from defendants' server by plaintiffs' investigator within the United States, then plaintiffs' complaint failed to allege

[191] 946 N.E. 2d 159 (N.Y. Ct. App. 2011).
[192] *Id*. at 163-64.
[193] *Id*. at 165.
[194] 647 F.3d 1218 (9th Cir. 2011), *cert. denied*, 132 S. Ct. 1101 (2012).
[195] *E.g.*, Subafilms Ltd. v. MGM-Pathe Communications Co., 24 F.3d 1088 (9th Cir. 1994).
[196] *E.g.*, L.A. News Serv. v. Reuters Television Int'l Ltd., 149 F.3d 987 (9th Cir. 1998).
[197] 809 F. Supp. 2d 1139 (N.D. Cal. Aug. 22, 2011).

an infringing act that took place entirely within the United States.[198] However, the court declined to dismiss the claim because factual questions remained as to the locus of defendants' infringement – e.g., where the initial copying took place, where the servers are located, etc.

In *Tire Engineering and Distribution LLC v. Shandong Linglong Rubber Co.*, the Fourth Circuit Court of Appeals joined the Second and Ninth Circuits in adopting the "predicate-act" doctrine.[199] The court held that "[o]nce a plaintiff demonstrates a domestic violation of the Copyright Act, then, it may collect damages from foreign violations that are directly linked to the U.S. infringement."[200] In that case, the initial copyright violation – defendants' reproduction of plaintiffs' blueprints for mining-vehicle tires – took place in the United States. Accordingly, the court affirmed the district court's award of damages based on defendants' extraterritorial exploitation of their infringement.

Even when no infringing act occurs in the United States., it still may be possible for the case to be heard in a U.S. court, in which case the U.S. court will apply foreign copyright law.

2) Does your national collective rights management organisation grant multi-territorial licences and are there cloud-specific licence models when it comes to collective licensing? If so, does this include rules on cross-border contracts (including jurisdiction and choice of law aspects)?

The United States does not have a single national collective rights management organization. Multiple private organizations license works, each dedicated to a separate industry. For example, BMI and ASCAP are performing rights organizations (PROs) that collect royalties owed to songwriters for the public performance of their songs. The Copyright Clearance Center licenses academic and reference books. There are also organizations that represent various visual artists in licensing their works. Some of these organizations grant multi-territorial licenses.

The PROs generally limit their licensing activities to the U.S. and its territories, and rely on foreign PROs to monitor and collect royalties due in their respective markets. However, for reasons of efficiency, ASCAP has granted a license for a live concert in the U.S., with an addendum, permitting the concert to be streamed live and streamed from an archive, in over 50 countries, for a limited time period. Moreover, and again for reasons of efficiency, ASCAP has granted to certain European societies the right to license certain uses of ASCAP's repertory on a pan-European basis as well as for the Middle East and North Africa. ASCAP has also granted to certain societies in the Asia Pacific region the right to license certain uses of music for that region. Such agreements between ASCAP and other foreign PROs take place within the framework of the rules applicable to CISAC societies, ranging from the binding rules of professional conduct for music collecting societies to the commitment to use the CIS tools, or common information standards for collecting and exchanging data and royalties.

[198] 826 F. Supp. 2d 398 (D. Mass. 2011).
[199] 682 F.3d 292 (4th Cir. 2012). *See, e.g.*, Update Art, Inc. v. Modiin Publ., Ltd., 843 F.2d 67, 73 (2d Cir. 1988); *L.A. News Serv.*, 149 F.3d at 990-92.
[200] *Tire Eng'g & Distribution*, 682 F.3d at 11.

With respect to licensing for the Cloud, ASCAP and BMI license all manner of streaming services, from Netflix to Pandora and Spotify;[201] all of these services operate from servers where the works are stored and streamed at the demand of subscribers.

New York, New York

July 2012

[201] *App Store*, SPOTIFY, http://itunes.apple.com/us/app/spotify/id324684580?mt=8 (last visited July 6, 2012).