ALAI Congress Kyoto 2012
October 16 to 18, 2012

Copyright and Related Rights in the "Cloud" Environment

Session 2 . Keynote speech

The WIPO „Internet Treaties"
and Copyright in the „Cloud"

Dr. Mihály J. Ficsor
Member of the Presidency and Hon. President of the Hungarian Copyright Council, former Assistant Director General of WIPO.

VERSION ONE

The question

The overall topic of Session 2:

Can the Internet Treaties of 1996 Play an Important Role in Legal Issues Raised by "Cloud" Business?

The answer

Yes, of course.

THANK YOU FOR YOUR ATTENTION

VERSION TWO – SOMEWHAT MORE IN DETAIL

The „Cloud" and the WIPO Treaties – introductory remarks

From the viewpoint of the application of the provisions of the WIPO „Internet Treaties" (the WCT, the WPPT and the BTAP) and other international, regional and national copyright norms, the most relevant aspects of cloud computing is that **works and other protected materials are included in remote storage capacities** (on servers the location of which may even be unknown) **and they are made available for use either to the customers of the cloud services** (and, at maximum, to persons in his private sphere) **or to the members of the public – normally at any place and at any time chosen by them**.

In view of this, in particular **three rights** provided in the WIPO "Internet Treaties" – **the right of reproduction, the right of distribution and the right of making available** – may be involved.

„Virtual video recorders” – as an older „cloud” generation (1)

US: Cablevision (Cartoon Network v. CSC Holding, Inc): **the mother** (or grandmother) **of all cloud-related copyright cases**.

The court had to decide **three issues**: (i) **whether or not** Cablevision (a „virtual video recorder provider”) made **unauthorized copies in the buffer**; (ii) **whether or not** it made **unauthorized copies on its server**, and (iii) **whether or not it performed an act of unauthorized public performance** when a recorded program was transmitted to the consumer to view it later. While **the District Court gave an affirmative answer to all the three questions, the Second Circuit reversed the ruling on all the three issues.**

Was the Second Circuit right? Under a certain analysis, it was not necessarily.

„Virtual video recorders" – as an older „cloud" generation (2)

<u>„Anti-Cablevision" developments in some other countries – less shadow, more sunshine for copyright owners</u>:

Germany: „**Internet Video Recorder**" ruling of the Federal Court of Justice (BGH). **It depends on the concrete technical aspects** who is to be regarded the maker of a copy, the service or its customer. **The profit-making objective of the service provider** (even if the service is free for the customers, but the provider's objective is to earn advertisement money) may also result in direct liability. **„If… then…" ruling.**

***RTL v. Save.tv – ProSiebenSat v. Save.tv* :** the „virtual video recorder" provider had infringed the broadcasters' rights of reproduction and communication.

„Virtual video recorders" – as an older „cloud" generation (3)

„**Anti-Cablevision" developments in some other countries – less shadow, more sunshine for copyright owners**:

Hungary: The Copyright Council **follows the German way** (official opinion SzJSzT 31/2007).

Australia: The Federal Court in ***NRL, AFL and Telstra v. Optus*:** the „virtual video recorder" had made the copies, or it and the customers had made them together. The act "making" is a basic concept of the Copyright Act and it should be understood in accordance with its ordinary meaning of making something. **Although the customers initiated the automated process, it was Optus which effected the reproduction.** The court also considered it as a relevant fact that the **copies were kept under the control of Optus** and the subscribers' subsequent use took place on that basis.

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (1)

Borderline between direct (primary) and secondary liability.

Applicability of the provisions on the (limitation of) liability of hosting providers (see, e.g. section 512 of the **US Copyright Act** and Articles 14 and 15 of the EU **Electronic Commerce Directive**):

- **no** actual or „constructive" (or „red-flag") **knowledge of infringements**;
- **expeditious, prompt removal** of infringing materials **or blocking access** to them;
- **no financial benefit directly attributable to the infringing activity where the provider has the right and ability to control such activity**;
- **no general monitoring** (such a filtering) **obligation** (*a contrario*: **non-general monitoring obligations may be imposed**).

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (2)

US: key „interoperable" UGC cases: YouTube, Veoh, YouTube, Veoh

UMG Recordings v. Veoh Networks (District Court) : **"By reason of storage at the direction of a user" includes** conduct that arises from **facilitating access to user-stored materials**. The acts of 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**.

UMG Recordings, Inc. v. Shelter Capital Partners LLC. (→ Veoh) (Ninth Circuit): No direct or secondary liability. **General knowledge of infringements is not a knowledge to deny safe harbour. „Right and ability to control"** requires control over **infringing activities that the provider knows about.**

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (3)

US: key „interoperable" UGC cases: YouTube, Veoh, YouTube, Veoh

Viacom v. YouTube (Second Circuit) **:** Relying on the ***Veoh*** ruling → YouTube's **"related videos" function falls within the scope of activities protected** by section 512(c). The algorithm used for the that function "**is closely related to, and follows from, the storage itself**," and is "**narrowly directed tow**ard **providing access to material stored at the direction of users**."

No duty for proactive monitoring. **However** the case **remanded** to the District Court:

- a reasonable juror could find that YouTube **in some circumstances knew of clearly infringing material** that it failed to remove;
- YouTube **may have been willfully blind** to infringements of which it should have known;
- YouTube **may have earned 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.

UGC v. Veoh (Ninth Circuit): Relying on the ***YouTube*** ruling → supplementary brief for **potential taking into account that ruling**.

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (4)

Relevant CJEU rulings on service provider liability: from eBay through Scarlet to Netlog.

L'Oréal and others v. eBay and others (July 2011)

- In order for an internet service [hosting] provider to fall within the scope of Article 14 of Directive 2000/31, **it is essential that the provider be an intermediary provider** within the meaning intended by the legislature in the context of Section 4 of Chapter II of that directive.
- **This is not the case where the service provider**, instead of confining itself to providing that service neutrally by a merely technical and automatic processing of the data provided by its customers, **plays an active role of such a kind as to give it knowledge of, or control over, those data.**
- Since the operator **has provided assistance which entails**, in particular, **optimising the presentation of the offers in question or promoting those offers**, it must be considered not to have taken a neutral position, but to have **played an active role of such a kind as to give it knowledge of, or control over, the data**. It **cannot** then **rely,** in the case of those data, **on the exemption from liability** referred to in Article 14(1) of Directive 2000/31.

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (5)

Relevant CJEU rulings on service provider liability: from eBay through Scarlet to Netlog.

SABAM v. Scarlet (November 2011)

Scarlet qualifying as **access provider** rather than hosting provider.

The issue: **filtering** (as described in the referral)

- **all electronic communications** passing via its services, in particular those involving the use of peer-to-peer software;
- which applies **indiscriminately to all customers**;
- **as a preventive measure**;
- **exclusively at the service provider's expense;** and
- **for an unlimited period**.

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (6)

Relevant CJEU rulings on service provider liability: from eBay through Scarlet to Netlog.

SABAM v. Scarlet (contd.)

- **„serious infringement of the freedom of the ISP concerned to conduct its business** since it would require that ISP **to install a complicated, costly, permanent computer system at its own expense";**

➢The **business** involved was **based,** to a great extent, on (i) **illegal making available of works by a huge number of the customers** of the business, (ii) **increasing by this the number of visitors of its website,** and, (iii) **as a result of this sort of popularity, obtaining income from advertisers**. **What about the business of those whose creations and productions were used illegally, and without which the business could not have had chance to succeed**?

➢The filtering system proposed was qualified **too complicated and too costly** (without any real analysis or calculation why it should be regarded so). **What about possible filtering systems that would be simpler and less costly or that is not "permanent**"?

➢**Would not it have been justified to consider that the ISP might have to bear the cost of a reasonable filtering system from its income indirectly derived from the infringements taking place through its system**?

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (7)

Relevant CJEU rulings on service provider liability: from eBay through Scarlet to Netlog.

SABAM v. Scarlet (contd.) The outlined filtering system

- **„may also infringe the fundamental rights of that ISP's customers,** namely their right to **protection of their personal data and their freedom to receive or impart information";**

➢ **Insubstantiated, slogan-based sweeping statement** which could hardly stand any serious scrutiny .

➢ **Why would** a filtering system **violate the protection of customers' personal data if it only consisted in the identification of illegal materials and in their removal?** In particular, why would it be so if **an automatic system** were involved and it functioned **only in the relation between the ISPs and their customers** ?

➢ **Did the court see even a modicum of seriousness in the apparent position according to which free unauthorized making available of a freshly released films** to the internet population **is a matter of freedom of receiving and imparting information.**

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (8)

Relevant CJEU rulings on service provider liability: from eBay through Scarlet to Netlog.

SABAM v. Scarlet (contd.) The outlined filtering system

- "could potentially **undermine freedom of information** since that system might not distinguish adequately between unlawful content and lawful content;"

➢**It can be easily proved how huge exaggerations this completely unsubstantiated statement contains** and how much it is badly founded. **It is sufficient to refer to the successful operation of the filtering system applied by YouTube** in accordance with the cross-industry agreement published on **www.ugcprinciples.com**.

➢It is still a major understatement if it is stated that, **in the extremely overwhelming majority of cases, the "matches" found by the filter are unequivocally infringing copies**.

➢The same UGC principles take into account and take care of the **overly exceptional situations** which form only a microscopic tiny fraction of the enormous number of cases.

➢**Is it a reasonably balanced attitude to throw out the baby not just along with the bath water but her alone merely because one of her fingers is still somewhat wet**? Why not to try finding a means to dry that small spot?

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (9)

<u>Relevant CJEU rulings on service provider liability: from eBay through Scarlet to Netlog</u>.

SABAM v. Scarlet (contd.) (If the filtering system were ordered)

- **„the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property,** on the one hand, **and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the othe**r."

➢In the concrete situation with the concrete details, **this may have been true**.

➢However, **it seems quite sure that the CJEU**, in this case, no matter how good intention it may have had, **has fulfilled this requirement even less**; **the preliminary ruling is largely unbalanced to the detriment of copyright owners.**

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (10)

Relevant CJEU rulings on service provider liability: from eBay through Scarlet to Netlog.

SABAM v. Scarlet (contd.) Further unanswered questions:

- What does it mean in Recital (45) of the E-Commerce Directive that **injunctions may consist in orders to require not only the termination but also prevention of infringements? How filtering infringing copies** to prevent their making available to the public **as a means of prevention** rather than *post festam* termination of infringements **should be considered** from this viewpoint? **Are there at present any realistically available effective means to prevent the inclusion of infringing materials** in an online system **other than filtering**? **What would be the meaning and value of this recital if, although orders to prevent online infringements are possible, their only effective application would not be allowed?**
- **What does the prohibition of general obligation to monitor** the information that ISPs transmit or store **mean and what kind of non-general obligations to monitor may be ordered,** in particular **in the light of the clarification in Recital (47)** which reads as follows: **"Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case** and, in particular, does not affect orders by national authorities in accordance with national legislation."? (Emphasis added.)

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (11)

<u>Relevant CJEU rulings on service provider liability: from eBay through Scarlet to Netlog.</u>

SABAM v. Netlog (Februray 2012) (Netlog: a **social networking platform** qualifying as **hosting provider**)

- The court completely **disregarded that, contrary to Scarlet, a hosting provider was involved** to which stricter rules apply under Article 14 of the Electronic Commerce Directive.
- **It repoduced in a copy-and-past verbatim manner the Scarlet findings** on the freedom of conducting business and the alleged conflicts with the protection of personal data and the freedom of information.
- **It did not pay attention to *eBay*, although the application of the principles and criteria laid down in that case would have been justified.**

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (12)

United Kingdom: "authorization" doctrine ready to be applied also for the "Cloud."

No specific ruling concerning cloud-based services. **There have been rulings concerning the liability of Internet service providers for "authorizing" restricted acts which could be relevant in the „Cloud" too.**

➢***Dramatico et alia v BSkyB et alia:*** the court applied the concept of "authorization" relying on factors identified in the previous judgment in *20C Fox v Newzbin*: (i) the **relationship** between the alleged authoriser and the primary infringer, (ii) **whether the equipment/ means supplied constitute the means used to infringe**, (iii) whether it **will be used to infringe**, (iv) the **degree of control** of the alleged authorizer, and (v) **whether he is taking any steps** to prevent infringement.

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (13)

United Kingdom: "authorization" doctrine ready to be applied also for the "Cloud."

➢Judge Arnold's judgment held that ***the operators of the Pirate Bay authorized the infringing activities of its users*** (both by copying or communicating to the public; maybe even through public performance) and that their activities **go beyond merely enabling, or assisting infringement.** The Pirate Bay's system is designed to provide users with the easiest and most comprehensive service possible It is **not merely a passive repository of files** but goes to great length to **facilitate and promote the download of files by its users**: (i) **the means supplied**, i.e. the indexed torrent files, constitute exactly the means necessary to infringe; (ii) **copyright infringement is not only inevitable but is also the main objective** of the service; (iii) the website operator **has the required degree of control**; (iv) the website operator is **not taking any steps** to prevent infringement; moreover **it is expressly encouraging infringement**.

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (14)

Germany: "umbrella solution" in case of dark clouds.

Marions Kochbuch case: (2009) The Federal Court of Justice (BGH) held that **the UGC platform *www.Chefkoch.de* had infringed the right of making available to the public** in photographs uploaded in the system.

- The UGC platform **had adopted the contents represented by the uploaded works as its own; it assumed the responsibility for the content** factually and visibly perceivable by the public.
- Since the provider **had not only granted storage space** to its users **but adopted the contents as its own, it was the one who used works in the form of making them available to the public .**

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (15)

Germany: what is taken down should stay down.

GEMA v. YouTube (Hamburg Regional Court (*G Hamburg*), April 2012)

- YouTube was **not directly liable** for having committed the infringements (in the form of "*Täterhaftung*") **but did have "disturber" liability** ("*Störerhaftung*") by providing its platform and thus contributing to the infringing acts. As a "disturber," YouTube **did not fulfill its duty to stop the infringements by blocking access to the videos without delay after the plaintiff had notified it about them** (in certain cases, YouTube only blocked access to the videos seven months after GEMA's warning).
- When notified of an infringement, YouTube **has the obligation not only to remove or block access to the video without delay but also to take measures to prevent further infringements.** (This duty does not extend to those videos that had already been uploaded to the platform.)
- **No disproportionate duties may be imposed on YouTube**. Nevertheless, **it is a reasonably proportionate obligation to prevent future illegal uploads of the same musical works on the same recording by using filtering software**. YouTube should use the software itself and **could not leave this to its users**.

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (16)

Netherlands: mixed rulings on the right of making available; providers' passive or active role as a basic criterion.

The response of the Dutch ALAI Group prepared in response to the congress Questionnaire reports on various **court decisions which held or (more frequently) not held that the activities of certain hosting service providers may qualify as acts of making available to the public**, than it sums up certain completely valid **underlining principles** as follows:

In a **more technical approach** it could be argued that Cloud providers are „**merely providing technical facilities."** In contrast, in **more functional approach** criteria, such as „intervention," „the reaching of a 'new public'" and „profit" **determine whether the content is made available to the public**. **The technical approach gives way to difficulties in the Cloud environment** given the fact that in providing „physical facilities" some Cloud providers *de facto* function **as „on demand" radio- and television services and can play an important central role in the exploitation of copyrightable works on the internet** (and are also not only commercially benefitting from the technical service but are also (directly) **benefitting from the exploitation of this content because they also enjoy revenues associated with the consumption of that content (f.e. through advertisements**).

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (17)

Netherlands: only general monitoring obligations are not allowed; specific obligations are.

Stokke v. Marktplaast (Court of Appeal in Leeuwarden) on the issue of monitoring obligations:

- **Article 15 of the E-Commerce Directive does not stand in the way of imposing obligations to monitor for infringements in specific objects of protection** , for instance a monitoring obligation for the specific selection of advertisements that contain the text STOKKE or TRIPP TRAPP (a selection that can be easily made with the use of a filter).
- **Such injunctions have to remain reasonable and proportionate** and are not allowed to become unreasonably expensive or result in obstructions of legitimate trade. (The court has said: „legitimate." Only legitimate!)

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (18)

France: taken down but not staying down; cold shower into the rightholders' neck. For a while, **it seemed that French jurisprudence would go in the same direction as in Germany** (as indicated in the ruling of the Hamburg Regional Court discussed above), see, e.g. the 2011 rulings in *André Rau v. Google and Aufeminin.com*, *Google Inc. v. BAC Films et al*., **Recently, however, with two rulings of the Supreme Court, the so far friendly white clouds have turned dark.**

In *Christian* ***C., Nord Ouest Production v. DailyMotion***, the **French Supreme Cou**rt (*Cour de cassation*) found (in February, 2011) that DailyMotion, as a hosting provider, was **only subject to a notice and take down obligation.**

After that the Supreme Court applied the *Netlog* principles in an automatic way in that DailyMotion case, the **Tribunal de Grand Instance went in the same direction** in its judgment in ***TF et al v. DailyMotion*** in September, 2012 (although the hosting provider was held liable in certain cases since, when it received due notice, had not removed infringing copies promtly enough).

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (19)

France: taken down but not staying down; cold shower into the rightholders' neck.

The the real cold shower came from the **French Supreme Cou**rt which on July 12 , 2012, adopted its ruling in the *André Rau v. Google and Aufeminin.com* and the *Google Inc. v. BAC Films et al* cases. It **reduced the obligation of these UGC-platform-type hosting providers to block access to infringing materials when they receive notice**. **It reversed the judgments of the Courts of Appeal which – rightly enough – had ordered the UGC platforms to prevent the uploading infringing copies of the same works the illegal nature of which had already been identified by previous notices.**

The downward eBay-Scarlet-Netlog-DailyMotion spiral seems to have reached the bottom from the viewpoint of owners of copyright. With due respect to the Supreme Court, **in this case the Court of Appeal was right. The Supreme Court has not even applied all the Netlog criteria. It only identified one more or less concrete reason; namely the unlimited nature of the "notice and stay down" obligation**. **It did not offer any explication why such a specically trageted monitoring obligation might be in conflict with the prohibition of general monitoring obligation** under Article 15(1) of the E-Commerce Directive.

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (20)

Italy: no liability exemption for hosting providers which play active role. In accordance with the EU Electronic Commerce Directive and the Italian Decree 70/2003, **cloud service providers qualify mainly as hosting providers**. However, as the report of the Italian ALAI Group prepared in response to the congress Questionnaire points out, **the courts differentiate between passive and active hosting activities and tend to interpret the exemptions from liability restrictively where the activity is not deemed to be merely passiv**e.

- In the preliminary ruling of ***RTI-Mediaset v. YouTube***, the Tribunal of Rome recognized the liability of YouTube as hosting provider and its **duty to remove**, upon notice of Mediaset, the materials illegally uploaded.
- In the ***RTI v. IOL case***, (adopted in 2011) the court stated that **the service provider did not fully correspond to the criteria of hosting providers** defined in Article 16 of Legislative Decree 70/2003. The court ruled that that **the degree of liability differs in case of "active hosting" as opposed to mere "passive hosting".** Active hosting was evidenced by the **insertion of advertisements to accompany UGC videos and content indexing facilitating users' searches**. Thus, **prohibitory injunction was decreed** as requested by the plaintiff RTI.

Further retrospective discoveries in the „Cloud" – e-mail services, social networks, UGC platforms (21)

Japan: the country of rising sun and cautious hope for owners of rights. The Japanese ALAI Group, in its report to the congress Questionnaire, mentions the "***TV Break case.***" The High Court ruled that **the file-hosting provider was liable for copying of the programs on its server by, and their subsequent transmission to, its customers**. The reasons for this ruling were that (i) the provider **operated and controlled the site**, (ii) **profit derived from the activity was received by the provider**, (iii) at the same time, **it did not take any effective measure to prevent infringing acts** even though there were good reasons to know that infringements took place, and (iv) it **did not react even where it had actual knowledge of infringing videos in its system**. The court held that the operator of the site **performed the infringing acts** (it was **a "sender"** under e-commerce legislation), and therefore, **the limitation of the liability of service providers was not applicable in its favor.**

The report states that there is no statutory provision or **Supreme Court ruling specifically on these issues in respect of cloud services. The Copyright Act of Japan does not have an explicit provision on secondary liability. However,** given the court practice reflected in the above-mentioned High Court judgment, **"there is a possibility" that cloud service providers could be found liable for infringing materials uploaded by their customers.**

„Cloud-native" services – „cyberlockers" (1)

„Cyberlocker" cases in the US: no clear trend

Capitol Records, Inc. v. MP3tunes, LLC*:* The court held 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. The court decided, however, that the company was **ineligible for the section 512(c) safe harbor with respect to infringing songs in its users' digital "lockers" that MP3tunes failed to remove after receiving take-down notices**. Finally, the court also found that MP3tunes.com was **contributorily liable for infringement of rights in such works, because it had reason to know about the infringing activities and provided the site and facilities for the infringing activities.**

Disney Enterprises, Inc. v. Hotfile Corp.: Hotfile **did not behave as a provider which only provides physical facilities** for uploading and downloading. It **also encouraged its users to become members in order to enjoy privileges such as faster download times**. Those who uploaded works which then became the most downloaded were rewarded by certain benefits, **including by payments**. **In spite of such an active role of Hotfile** in the uploading-downloading activity, **the District Court held that it was not subject to direct liability.** Nevertheless it allowed the **secondary liability** claim to proceed.

„Cloud-native" services – „cyberlockers" (2)

„Cyberlocker" cases in the US: no clear trend

Perfect 10 v. Megaupload: another Distric Court ruled in different manner against Kim "Dotcom's" well-known pirate empire in the "Cloud." It found that **Megaupload was not a mere file storage system** and that **its actions – which included incentivizing its users to upload infringing content through a rewards system similar to Hotfile's – taken together with its general awareness that its website was being used for infringements could be regarded as amounting to volitional conduct.** Thus the court held that Megaupload was **directly liable** for the infringement of the relevant acts covered by copyright (which, from the viewpoint of the WIPO "Internet Treaties" meant the right of reproduction and the right of (interactive) making available to the public).

„Cloud-native" services – „cyberlockers" (3)

Unpleasant adventures of RapidShare and others in Germany.

GEMA v. RapidShare. The suit was launched still in 2009 and, in 2010, the ***Regional Court*** of Hamburg *(LG Hamburg)* **found basically in favor of GEMA**. **The ruling of the the Higher Regional Court** in Hamburg (*OLG Hamburg*), in March 2012, **approved the LG's decision.**

RapidShare must implement effective measures to prevent uploading illicit copies. Although RapidShare **was ready to take down infringing materials when it had been notified about them, it did not take any measure against the uploading of copies equally infringing the same works** by the same or a different user of its service. **The court has obligated RapidShare to implement** additional measures – in practice, **a filtering system** to prevent copyright infringements from occurring repeatedly in this way. That is, the cloud service provider **had to guarantee that if copies infringing copyright in a given work is taken down then such copies also stay down** (notice to take down and to stay down).

„Cloud-native" services – „cyberlockers" (4)

Unpleasant adventures of RapidShare and others in Germany.

In ***Atari v. RapidShare***,„ **the locker provider, first, seemed to be the winner.** The **Regional Court** (*LG*) of Düsseldorf, similarly to the way it happened in the GEMA v. RapidShare case**, found against it**. **However, the Higher Regional Court** in Düsseldorf (*OLG*) **reversed the ruling** in favor of RapidShare. The OLG did not find it justified to obligate RapidShare, in addition to take down illegal copies when duly notified, also to prevent, through a filtering system, repeated uploading of illegal copies of the same works.

The **Federal Court of Justice** (*BGH*) seems to have seen the factual situation more realistically and deduced from it more adequate findings. The BGH, in its judgment **reversed the ruling of the Düsseldorf OLG. Although** it stated that, in principle, **file hosting services are to be recognized as an appropriate business model, they should duly cooperate with copyright owners not only by removing illegal copies from their system but also by preventing their inclusion** (that is, if illegal copies of a work are taken down, they should stay down and not uploaded again). **If RapidShare does not apply a reasonable filtering system for this purpose, it will be liable for the infringements.**

„Cloud-native" services – „cyberlockers" (5)

Unpleasant adventures of RapidShare and others in Germany.

Until June 2011, ***Kino.to*** was the biggest German-speaking Internet UGC site. The users of the service uploaded the works to their personal „lockers" and received a link to them. Everybody having access to the internet was able to also access those links and hence either stream or download the movies.

The Regional Court (*LG*) of Leipzig held that **Kino.to had communicated works to the public in the sense of Article 106 of the German Copyright Law, which means making available to the public** in accordance with Articles 15II(2) and 19a of the Copyright Law. The court found that the relevant action of exploitation was to place the works on the internet and that of **no importance was whether or not the work was accessed, if accessed how frequently and by what kind of technological means**.

The court **sentenced the main operator of the pirate cloud service to four-and-a-half-year imprisonment** for the infringements of copyright. Other operators of the service also received well-deserved prison sentences.

Exceptions and limitations (in particular for private copying) (1)

General applicability of exceptions and limitations.

It goes without saying that **the provisions of the international treaties on exceptions and limitations** – both the specific ones (controlled by the three-step test) and the three-step test – **do apply also for the cloud-based systems.** However, the application of possible exceptions or limitations for private copying raises some particular issues in the cloud environment.

Private copying – is the copying in the „Cloud" truly private?

In certain cases, as discusssed above, **it may be questioned whether the copy in the "Cloud" is made by private persons or by the cloud service**. **In the latter case, obviously one could not speak about private copying.**

There are national laws under which the **private reproduction exception does not apply where a commercial service makes a copy for subsequent private use**. Even **where** there is no such provision, **the exception is not applicable in case of direct or indirect economic advantage** – as for example in the case of Article 5(2)(b) of the Information Society (Copyright) Directive . **Any profit-making nature of cloud services may exclude the application of the exception.**

Exceptions and limitations (in particular for private copying) (2)

Why the French law is right and applicable on private copying in spite of *Padawan*.

The report prepared by the French ALAI Group in response to the congress Questionnaire states that **the status of "private copying" is not sufficiently clear** under the European *acquis communautaire* and the French legislation. **Under the French jurisprudence**, in order that a copy may qualify as a result of private reproduction, **the copier and the user of the copy should be the same person.** The report **deduces from this that, since in the "Cloud," a third person makes available the means of reproduction, that person qualifies as the copier and the exclusive right applies**. Unless the user makes the copy**, we cannot speak about a private copy**.

However, the French Report **refers to „another analysis,"** according to which **neither the French Intellectual Property Code nor the *acquis communautaire* imposes the condition that the copier and the user of the copy should be the same. According to the report, the *Padawan* decision of the CJEU supports such an analysis** at the EU level since it seems that **it has reconciled the existence of a „copying service" with the private copying exception.**

Exceptions and limitations (in particular for private copying) (3)

<u>Why the French law is right and applicable on private copying in spite of *Padawan*.</u>

The French Intellectual Property Code does not allow any interpretation that would support „another analysis." The copier and the user must be the same person. The Code only provides for an exception in respect of copies **„reserved strictly for the private use of the copier and not intended for collective use**." (Article L. 122-5(2): *„strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective"*). Thus, **if it is found that the service provider is the maker of the copy, the exception does not apply.**

Just because the *Padawan* decision refers in certain points to copying services, it does not mean that the French law would be in conflict with the *acquis communautaire*. There is **no legal analysis in the decision** in this respect, which is quite understandable since **the CJEU simply was not supposed to provide a preliminary ruling on this question. None of the points in the referral by the national court addressed this issue. There is no "*res iudicata*;" it is up to national laws** to regulate these questions on the basis of a due interpretation of Article 5(2)(b) of the Information Society (Copyright) Directive. .

Exceptions and limitations (in particular for private copying) (4)

<u>Why the French law is right and applicable on private copying in spite of *Padawan*.</u>

The relevant recital – **Recital (38) – of the Directive:**

„Member States should be allowed to provide for an exception or limitation to the **reproduction** right for certain types of reproduction of audio, visual and audiovisual material **for private us**e, accompanied by fair compensation. This may include the introduction or continuation of remuneration schemes to compensate for the prejudice to rightholders. Although differences between those remuneration schemes affect the functioning of the internal market, those differences, with respect to analogue **private reproduction**, should not have a significant impact on the development of the information society. **Digital private copying** is likely to be more widespread and have a greater economic impact. Due account should therefore be taken of the differences between digital and analogue private copying and a distinction should be made in certain respects between them." (Emphasis added.)

It is true that the recital also uses the expression "*for private use*" (it is also a condition; the copy must not be used outside the private sphere), **but it consistently speaks about "*private reproduction*" and "*private copying*" as a result of which a copy is made**. **Where someone makes copies for others for direct or indirect profit-making purposes in a service intended to be used by the members of the public, it is definitely not "private copying"** but, at maximum, copying for the purpose of subsequent private use.

Exceptions and limitations (in particular for private copying) (5)

Why the French law is right and applicable on private copying in spite of *Padawan*.

Article 5(2)(b) of the Directive reads as follows:

„Member States may provide for exceptions or limitations to the reproduction right provided for in Article 2 in the following cases:

(b) in respect of reproductions on any medium made **by a natural person** for private use and **for ends that are neither directly nor indirectly commercial,** on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject matter concerned; (Emphasis added.)

This provision makes it even clearer that private copying exception does not apply when the copy is made in for private use but by a service (which certainly does not clarify as a natural person) for direct or indirect commercial purposes. **Practically all copying services (except for those offered by public institutions) are for at least indirect commercial purposes**. Article 5(2)(b) only allows that a person other than the potential user (usually a member of the family or a close acquaintance) make the copy who is a natural person.

The French law is in accordance with the Directive. The *Padawan* decision would be in conflict with it if the court truly intended to hold that not only private copying by a natural person without any commercial end is private copying but also copying by services not qualifying as natural persons and seeking direct or indirect commercial advantage.

Exceptions and limitations (in particular for private copying) (6)

Does a right to remuneration (or "fair compensation") apply?

The copy which may be found in the "Cloud," in the majority of cases, is **(i) either a copy made and made available by the cloud service** usually under TPM control for streaming or downloading, **(ii) or a back-up-type second copy of a lawfully obtained copy** uploaded by the user of the service, **(iii) or the same where an unlawful copy is involved**.

Doubts may emerge about the applicability of a private copying payment in all the three cases: In the case mentioned under **(i)**, the cloud copy is clearly **not a private copy**. In the case referred to under **(ii)**, an exception may be applied but **not as a private copying exception; rather as a back-up exception concerning a lawful copy**. As regards the third case under **(iii)**, **any exception for copying from illegal sources would be in conflict with the three-step test,** and **the copies** made in this manner **are subject to the obligation of the cloud provider to "take it down"** rather than pay a compensation for the infringements. (In this respect, in the "Cloud," **the issue of illegal copying emerges in a way different from the use of recording equipment and material in domestic environment where the "taking down" of infringing copies is not a re**ality.)

The **European Commission Staff Working Document recently published on „cloud"-related issues is also skeptical about the applicability of the private copying levy system** in the "cloud" environment. The relevant title is telling: "**Cloud computing services challenges to the private copying levies regime**.".

Exhaustion of rights (1)

Exhaustion where it may truly apply.

The **WIPO "Internet Treaties" leaves it to Contracting Parties whether they provide for exhaustion of the right of distribution, and if they do in which way** (in particular, whether they provide for international exhaustion or territorial exhaustion). Howevere, agreed statements limit the concept of copies to tangible copyies.

ReDigi: fully-fledged online music store in the guise of a "resale" forum.

Capitol Records v. ReDigi.com (online marketplace of "used digital copies of recorded music") The service **allows users to store their recordings in online lockers and *sell, buy, and stream* music in the Cloud.** The software allows users to designate the recordings legally purchased from iTunes Store or ReDigi that they wish to sell from their device. In such a case, ReDigi removes eligible recordings from the seller's device and stores the recordings in the ReDigi cloud for sale. Buyers are able to view a list of recordings that are for sale, and purchase and download them.

Exhaustion of rights (2)

ReDigi: fully-fledged online music store in the guise of a "resale" forum.

In its complaint, **Capitol Records claims** that **ReDigi is liable for several violations, including direct infringement, contributory and vicarious liability, and inducement of copyright infringement.** ReDigi continues to engage in **unauthorized reproduction, distribution, and public performances** of the plaintiff's works and assists users in making unauthorized copies and sales.

ReDigi has claimed fair use and the first sale doctrine as a defense. Although the first sale has traditionally applied only to tangible copies, **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.**

Exhaustion of rights (3)

ReDigi: fully-fledged online music store in the guise of a "resale" forum.

ReDigi's claims may hardly stand a serious scrutiny. Exhaustion only applies to the right of distribution. **The right of making available to the public is not exhausted.**

The exhaustion of the right of distribution (with the underlining right of reproduction) is also hardly applicable in this case. Exhaustion **only applies where the same lawfully obtained copy is subsequently sold** or the property right in it is otherwise transferred. In the ReDigi model **nothing like this happens. *In principle,* the customer's copy is removed but it is not that copy which is transferred to the ReDigi system, but a new copy is made** there, **and where that copy is "sold," still another is made. Thus, not the right of distribution, but the right of reproduction is concerned for which no exhaustion of the right applies.**

In the preceding paragraph, the words "in principle," is stressed. It is submitted that **what may happen in principle does not necessarily happen in practice** (since there is no obstacle to maintain the copy on an external storage device).

Exhaustion of rights (4)

The CJEU tries to extend the doctrine of exhaustion of rights to where it is not applicable.

In ***UsedSoft v. Oracle***, the subject matter of the dispute was Oracle's programs covered by an end-user license agreement (EULA). The EULA contained a term forbidding the licensee to transfer the computer program to a third party. **UsedSoft,** a company based in Germany, is **"reselling,"** through its online system, **programs covered by the licenses** (practically in the same way as in the US ReDigi is „reselling" used copies).

The **CJEU** in its UsedSoft v. Oracle ruling **held that the exhaustion of the right of distribution is also applicable for digitally distributed computer programs** (CJEU case C-128/11). By doing so, **the CJEU erred for several reasons and adopted new law in conflict with the existing EU norms** (which has gone much beyond of its competence).

Exhaustion of rights (5)

The CJEU tries to extend the doctrine of exhaustion of rights to where it is not applicable.

The court was right when it was of the view that – in the case of downloading works (including computer programs) – **it is possible to apply the right of distribution as one of the way of implementing the right of making available to the public**. **However, the Information Society (Copyright) Dir**ective, in the case of literary and artistic works (including computer programs), **has implemented the right of making available to the public,** in its Article 3(1), the same way as provided in Article 8 of the WCT; that is, **in the framework of a broad right of communication to the public**

Legally qualifying certain acts of making available to the public as "distribution" does not change the fact that what takes place in the case of interactive online transmissions is **not transfer of property in a copy, but making a *new copy* in the computer in which a work** (including a computer program) **is downloaded**.

Although it is possible to speak about "distribution," it is a very special distribution: *distribution though reproduction through (interactive) transmission* and, as such, **it is a form of making available to the public**. The right of distribution may be exhausted by the first sale of copies, but **neither the right of reproduction is exhausted when a copy is made** (its applicability is intact in respect of any new act reproduction), **nor the right of communication to the public** (it is also intact regarding any further communication).

Exhaustion of rights (6)

The CJEU tries to extend the doctrine of exhaustion of rights to where it is not applicable.

The CJEU has **quoted Recital (29) and Article 3(3)** of the Information Society (Copyright) Directive and **but it has adopted a ruling which is in a head-on crash with these provisions**:

Recital (29): „**The question of exhaustion does not arise in the case of services and on-line services in particular. This also applies with regard to a material copy of a work or other subject-matter made by a user of such a service with the consent of the rightholder**. Therefore, the same applies to rental and lending of the original and copies of works or other subject-matter which are services by nature. **Unlike CD-ROM or CD-I, where the intellectual property is incorporated in a material medium, namely an item of goods, every on-line service is in fact an act which should be subject to authorisation where the copyright or related right so provides.**

Article 3(3): The rights referred to in paragraphs 1 (**the right of reproduction**) **and** 2 (**the right of communication to the public, including makinag available to the public**) **shall not be exhausted by any act of communication to the public or making available to the pub**lic as set out in this Article. (Emphasis added.)

Exhaustion of rights (7)

<u>The CJEU tries to extend the doctrine of exhaustion of rights to where it is not applicable.</u>

When a „used" program is uploaded to UsedSoft, **a new copy is made which is covered by the exclusive right of reproduction.**

The act of making available a copy on the UsedSoft site for downloading by somebody else **is covered by the exclusive right of making available.**

Neither of these rights may be „exhausted" under the international treaties and the „*acquis communautaire*."

The CJEU ruled that they are exhausted if they are characterized as „distribution."

The CJEU ruling, since it is in clear conflict with the EU law (and the EU „constitutional" rules), may hardly be regarded as valid.

Exhaustion of rights (8)

The CJEU tries to extend the doctrine of exhaustion of rights to where it is not applicable.

The CJEU tries to defend its ruling on the basis that the Computer Program Directive (adopted in 1991; consolidated in 2009) **is *lex specialis*** in relation to the Information Society (Copyright) Directive.

However, this argument cannot stand scrutiny. **The WCT and the Information Society (Copyright) Directive apply for computer programs as *lex generalis*. The provisions of the Computer Programs Directive may only apply where they truly contain specific norms. However, there is no specific rule in that Directive which might relate to Recital (29) and Article 3(3) of the Information Society (Copyright) Directive and what might serve as a basis to interpret „distribution" in a different way.**

Summary on rights, exceptions, limitations and exhaustion (1)

1. As regards the right of reproduction, the fundamental question is who is to be regarded as the maker of the copy; the customer of a cloud service, the cloud service or both of them together. The dominating trend in legislative norms and case law is that, if the copying in the storage space reserved for the customer is made through a completely automatic system, it may be regarded as private copying and covered by an exception.

2. From the very beginning, however, it has been a disputed question of whether, in a case mentioned in the preceding point, it is truly the customer who may be regarded the maker, or the only maker, of the copy. This is so since the copying system is in the possession and under the control of the cloud provider and the copy normally stays in its infrastructure. There are countries under whose laws the private copying exception does not apply in those cases where a third person makes a copy for a would-be private user – in particular if it is not a natural person and if it does so for direct or indirect commercial advantage. In such countries, there may be appropriate reasons to consider that such copying is not covered by the exception and, thus, the exclusive right applies.

3. Where cloud providers make copies on their servers, their acts are obviously covered by the exclusive right of reproduction. This seems to be the case also where, as a matter of simplification, rationalization or some other reason, they replace the copies made at the initiation of the customers by a single copy or some copies other than the "customer-made" ones which then the customers may use.

Summary on rights, exceptions, limitations and exhaustion (2)

4. Where, from a website in the "Cloud," works are made available to the public in an interactive manner, obviously the right of making available to the public applies in accordance with Article 8 of the WCT, Articles 10 and 14 of the WPPT and Article 10 of the BTAP. The online provider must obtain license from the owners of rights.

5. The legal situation is less clear and more complex where the customers of cloud services retrieve the works or other materials stored on the cloud providers' servers either in the form of streaming or downloading – in principle from any place and from any moment. Even where the customers retrieve works from the storage spaces reserved for them, due to the potentially great number of acts of accessing the same works in an interactive way, the result may be regarded as similar to or the same as "normal" making available to the public from a website. From the viewpoint of the exploitation of the works concerned, there is no substantial difference between such a situation and a possible one where the customers may get access a copy or copies made by the cloud provider. It goes without saying that if the customers may get access to a copy clearly made by the cloud provider for interactive use, the right of making available to the public applies.

Summary on rights, exceptions, limitations and exhaustion (3)

6. Court practice tends to recognize that cloud providers qualify as hosting providers and the relevant provisions on the liability of such providers apply to them. However, in those cases where cloud providers go beyond the passive role of hosting contents uploaded by their customers, they may become more easily liable in the form of secondary liability and even in the form of direct liability. Direct liability may occur in particular where cloud providers fulfill some kind of editing functions in respect of infringing materials and/or actively promote certain infringing contents or activities.

7. It is recognized as a basic obligation of cloud providers – as also of any other hosting providers – that they should act promptly to remove or block access to infringing copies when they receive notice or get red-flag knowledge about them. General monitoring obligations normally cannot be prescribed under current legislative norms. In contrast, it is justified to obligate cloud providers to apply reasonable targeted monitoring (filtering) systems to block access to uploading infringing copies of works that have already been identified as such, in particular in a notice-and-take down procedure. Those courts seem to act correctly which, in such a case, apply the principle that what has been duly taken down should stay down.

Summary on rights, exceptions, limitations and exhaustion (4)

8. **Exceptions and limitations, in general, may be applied in the same way in the cloud environment as in the "traditional" environment** – always **under the control of the three-step test.** However, **the conditions of the applicability of certain exceptions may change**. For example, as discussed above, **special considerations may prevail as regards private copying exceptions. The basis for the application of private copying levies may shrink or fade away.**

9. **The principle of exhaustion of rights is not applicable in case of online services when an intangible copy is downloaded.** Such acts **may be characterized as acts of distribution** and the right of making available may be applied through a right characterized as right of distribution (in the form of distribution through reproduction through transmission). **However, the acts do not cease to be covered by the characteristics of the acts and right of making available to the public in the case of which no exhaustion applies. Where a "used" copy of the work is uploaded** to a cloud website, **to offer it to be downloaded from there, two rights are involved and neither of them is covered by the exhaustion principle: the right of reproduction and the right of making available to the public**. The possibility that the original downloader may delete his or her own copy (although the copy may be very easily saved on an external device) does not change this legal situation.

The role of digital rights management, in particular technological protection, in cloud services (1)

<u>Renaissance of DRM in the "Cloud:" Mulholland Drive seen in UltraViolet light</u>.

There is sufficient experience how the provisions of the WIPO "Internet Treaties" on technological protection measures (Article 11 of the WCT, Article 18 of the WPPT and Article 15 of the BTAP) **and on rights management information** (Article 12 of the WCT, Article 19 of the WPPT and Article 16 of the BTAP) **may – and should – be interpreted and applied adequately in national laws.**

Technological protection measures (**TMPs**) and digital rights management information (**RMI**) are frequently applied as **combined in digital rights management (DRM)** systems. **As regards the second element of DRM systems, (RMI)** – also due to the quite detailed treaty provisions – **no substantial interpretation problems have emerged. In contrast, as regards TPMs, due partly to the more general language of the provisions of the Treaties and partly to a kind of ideology-based resistance against it by "copyright minimalist" circles, heated debates have taken place.**

By now, however, **adequate international standards have been established also for the interpretation and application of the TPM provisions. They are equally applicable in the „cloud" environment .**

The role of digital rights management, in particular technological protection, in cloud services (2)

<u>Renaissance of DRM in the "Cloud:" Mulholland Drive seen in UltraViolet light</u>.

One of the basic standards and principles is that **the three-step test must control not only the application of exceptions and limitations as such but also the impact of intervention mechanisms employed to guarantee the enjoyment of certain exceptions and limitations where TPMs are used.**

This principle was **stated in a particularly clear manner in the ruling of the French Supreme Court (*Cour de cassation*) in the *Mulholland Drive* case** (in February 2006). The court clarified that **TPM protection cannot be removed for the sake of mere better convenience** of users where as a result conflicts would emerge with the normal exploitation of works for which the use of TPMs are necessary.

This has also been confirmed in the agreed statement adopted by the Beijing Diplomatic conference in June 2012 on the relationship between Article 15 of the BTAP (on TPMs) and its Article 13 (on the three-step test). The agreed statement has made it clear that not only the exceptions and limitations must be in accordance with the three-step test for the applicability of which certain measures are used, but the use of those measures should also be controlled by, and remain in accordance with, the three-step test.

The role of digital rights management, in particular technological protection, in cloud services (3)

Renaissance of DRM in the "Cloud:" Mulholland Drive seen in UltraViolet light.

T**he application of cloud technology may also solve the "problems" of alleged inconveniences** about which the plaintiff *Que choisir* was complaining in the Mulholland Drive case . It may be done **by using DRM protection in a flexible and user-friendly manner** – in accordance with the basic element of the concept of cloud-based systems, namely that they **make it possible using works included in the "Cloud" anytime, anywhere and on a great variety (but a determined number) of devices** .

The recently launched UltraViolet (UV) DRM-controlled cloud system is a good example:

- It allows users of digital home entertainment content to **stream and download** purchased content to **multiple platforms and devices**.
- Clients receive an account, **six accounts allowed per house**hold.
- The account provides **access to a „locker**" where licenses for purchased content are stored. The account holder **may register up to 12 devices for streaming and/or downloading** for transfer onto physical media (e.g. DVDs, SD cards, flash memory). Downloaded filles **can be played on any UltraViolet player registered to the household account,** but it will not play on devices which are not compatible with UltraViolet. Files can also be streamed over the Internet. Up to three streams can be simultaneously transmitted.
- A **common file format** has been designed to play in all UltraViolet players and work with all approved DRM systems.

The role of digital rights management, in particular technological protection, in cloud services (4)

Combination of software and hardware/firmware TPMs for cloud services: fight against illegal "modchips"

Legal cloud services, in general, use DRM systems, and within them TPMs, frequently in a combination of software and hardware (or firmware) measures (the latter TPMs **built in devices for use of works**). Hardware/firmware TPMs beyond any doubt whatsoever **correspond to the concept of TPMs** under the relevant provisions of the WIPO "Internet Treaties." **They provide efficient guarantees for adequate protection and exercise of rights, since their circumvention tends to be more difficult .**

Atempts at circumventing hardware/firmware protection built in devices to guarantee lawful use of protected works **may take place in other cases too, and** in the case of the device-specific legal cloud services they **seem to be proliferating**. However, **at present, the most typical field** where such protection is under attacks is the **use of games in video consoles**. The attacks take the form of manufacturing, distributing and using **"modchips" to circumvent firmware protection built in video consoles.** There are **attempts at trying to "legalize" this form of commercial-scale unauthorized circumvention** of hardware/firmware TPMs. Although **at the moment these mainly concern video consoles, it is clear that, in case they succeed, the other promising cloud-distribution-cum-TPM-controlled-device systems might fall as victims** too. Therefore, it is justified to review the current battles around "modchips."

The role of digital rights management, in particular technological protection, in cloud services (5)

US: attempt at (mis)using administrative rulemaking to try to remove firmware protection and open the way for game piracy.

As it is known, section **1201 of the Copyright Act mandates the Librarian of Congress to designate** – as a result of three-annual rulemaking proceeding – **certain classes of works to be exempted from the prohibition against circumvention of access-control TPMs** when such circumvention is done to engage in "non-infringing uses of works in the designated classes."

In the current rulemaking proceeding, the Electronic Frontier Foundation (EFF) has proposed the designation of the following „class" of works to be exempted from access-control protection: "**computer programs that enable lawfully acquired software applications, where circumvention is undertaken for the purpose of enabling interoperability of such applications with computer programs on the gaming con**sole." As it turns out from the minutes of the hearing on this proposal, such interoperability **would be needed basically for the purpose of using Linux software and "homebrew" games** (created by independent programmers) **on the consoles protected by firmware TPMs.**

The role of digital rights management, in particular technological protection, in cloud services (6)

US: attempt at (mis)using administrative rulemaking to try to remove firmware protection and open the way for game piracy

In the debate at the hearing, it has become quite clear that **the "problems" the EFF aims to eliminate are a matter of relative inconvenience**. There are **several other possible ways to use Linux and "homebrew" games**, even if it may be that, in certain cases, the obstacle-free use of the currently firmware-protected consoles might be more convenient. At the same time, **it is obvious that, as soon as TPM protection is removed from the consoles, they become efficient tools for game piracy** (the more so, since **the same steps are needed** to include Linux and "homebrew" games as to include pirated copies).

The principle adopted by the French Supreme Court in the *Mulholland Case* may be of some guidance also in this case. **Mere convenience is not a sufficient reason to apply exceptions to the prohibition of circumvention of TPMs** that are indispensable – as in the case of console firmware – for normal exploitation of works.

The role of digital rights management, in particular technological protection, in cloud services (7)

US: attempt at (mis)using administrative rulemaking to try to remove firmware protection and open the way for game piracy

It is also seems to be **doubtful whether there are truly any non-infringing use that is supposed to be achieved through removing TPM protection of video games**. However, **even if there were such a use,** from the viewpoint of the international norms, it is also a condition that **any exception to the prohibition of circumvention of TPMs should not cause a conflict with the "three-step test."**

Since video consoles are important means of distributing and otherwise making available works with indispensable DRM control, **the removal of such a key guarantee for lawful use would conflict with a normal exploitation of the works concerned**. Therefore, the adoption of the proposed exemption **might create conflicts with the international copyright treaties to which the US is party not only in respect of the obligations concerning TPMs but also of the three-step test.**

The role of digital rights management, in particular technological protection, in cloud services (8)

Europe: mixed rulings with healthy trends. The provisions of Article 6 of the the Information Society (Copyright) Directive **do not leave any doubt whatsoever that the Member States must provide adequate protection and effective remedies against the circumvention of firmware-based TPMs,** including preparatory acts such as manufacturing and distributing of such kinds of unauthorized circumvention devices as the modchips. There are now **ever more EU countries where the courts,** possibly after some detours in the not necessarily right direction**, have interpreted and applied Article 6 of the Information Society (Copyright) Directive adequately.**

For example, in the **United Kingdom**, where in the ***Gilham v. the Queen*** case, the defendant was condemned for criminal offence because it had distributed modchips in 2009. Then in ***Nintendo Co Ltd and Nintendo of Europe GmbH v Playables Ltd and Wai Dat Chan***, the High Court granted **summary judgment against and importer of R4 modchips** in July 2010 for copyright infringement and unauthorized circumvention of the TPM in question. **The defendant tried to argue that the circumvention device had also a lawful use** in the form of playing "homebrew games." However, **the court was not impressed by this**. It stated that "[**t]he mere fact that the device can be used for a non-infringing purpose is not a defence,** provided one of the conditions in section 296ZD(1)(b) [of the amended Copyright, Designs and Patents Act of 1988 on the prohibitions of circumvention of TPMs] is satisfied."

The role of digital rights management, in particular technological protection, in cloud services (9)

Europe: mixed rulings with healthy trends.

In **Spain,** in 2009, in the case initiated by ***Nintendo*** against ***Movilquick***, the Court of Salamanca, in a weird ruling, found that Movilquick's modchip **was served for circumventing the TPM** applied by Nintendo in its video console for the protection of the games produced by it. It also recognized that **this opened the gate for the use of pirated games**. However, **it still dismissed Nintendo's claim** by referring to the possibility that, when the TPM is circumvented, the console may be used not only for illegal purposes but also for certain legal purposes.

Another Spanish court, however, seems to have recognized that it is bound to apply the clear legal provisions on the protection of TPMs rather than to disregard them. In 2010, **the Criminal Court of Palma de Mallorca**, **found guilty the importers and sellers of R4 card modchips for circumvention of firmware TPM applied in Nintendo video console**. One of the defendants was condemned to **imprisonment; heavy fines** were applied; and the payment of **substantial damages** was ordered.

The role of digital rights management, in particular technological protection, in cloud services (10)

Europe: mixed rulings with healthy trends.

In **France**, **similar developments** have taken place. **In 2009, a criminal court in Paris adopted more or less the same kind of strange judgment** – and for similar flawed reasons – **as the Salamanca court** in Spain in a procedure initiated by ***Nintendo*** against ***Divineo SARL***, a distributor of illegal R4 cards to circumvent the TPM protection of Nintendo consoles. **It did not condemn the perpetrators.**

However, two years later, at the appeal of Nintendo, the **Court of Appeals in Paris** (in September 2011) **issued guilty verdict with suspended imprisonment, high criminal fines and a big amount of damages** to be paid to Nintendo.

The role of digital rights management, in particular technological protection, in cloud services (11)

<u>Europe: mixed rulings with healthy trends (but?)</u>.

In **<u>Italy</u>, since the verdict of the Supreme Court (Corte di Cassazione) adopted in 2007** – **and another one in 2011** – in criminal cases, **it has been a stable position in jurisprudence that the circumvention of TPM protection of video consoles is prohibited and the distribution of modchips is a crime**.

However, on July 26, 2012, **the Tribunale di Milano requested from the CJEU a preliminary ruling in the *Nintendo Co., Ltd and Others v PC Box Srl and 9Net Srl.***

The role of digital rights management, in particular technological protection, in cloud services (12)

<u>Europe: mixed rulings with healthy trends (but?)</u>.

The Milan court's questions to the CJEU:

1. **Must Article 6 of Directive 2001/29/EC be interpreted, including in the light of recital 48** in the preamble thereto, **as meaning that the protection of technological protection measures attaching to copyright-protected works** or other subject matter **may also extend to a system**, produced and marketed by the same undertaking**, in which a device is installed in the hardware** which is capable of recognising on a separate housing mechanism containing the protected works (videogames produced by the same undertaking as well as by third parties, proprietors of the protected works) a recognition code, in the absence of which the works in question cannot be visualised or used in conjunction with that system, the equipment in question thus incorporating a system which is **not interoperable with complementary equipment or products** other than those of the undertaking which produces the system itself?

2. **Should it be necessary to consider whether or not the use of a product or component whose purpose is to circumvent a technological protection measure predominates** over other commercially important purposes or uses, **may Article 6 of Directive 2001/29/EC be interpreted, including in the light of recital 48 in the preamble thereto, as meaning that the national court must adopt criteria in assessing that question which give prominence to the particular intended use** attributed by the right holder to the product in which the protected content is inserted or, in the alternative or in addition**, criteria of a quantitative nature** relating to the extent of the uses under comparison, **or criteria of a qualitative nature**, that is, relating to the nature and importance of the uses themselves?

The role of digital rights management, in particular technological protection, in cloud services (13)

<u>Europe: mixed rulings with healthy trends (but?)</u>.

It is **difficult to decipher** the meaning of these complicated questions, but the first question **seems to boil down to asking whether or not hardware/firmware TPMs are TPMs**. To this question, in the light of quite clear norms in the international treaties and in the *acquis communautaire*, **the answer may not be difficult**. However, **the second question is quite foggy. May it seek to clarify whether it is allowed under Article 6(4) to circumvent such a TPM if the device in which it is included might be used not only for illegal activities but also for certain legal activities**?

The role of digital rights management, in particular technological protection, in cloud services (14)

<u>Europe: mixed rulings with healthy trends (but?)</u>.

Recital (48) which the referral seem to regard as decisive

(48) Such legal protection should be provided in respect of technological measures that effectively restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases without, however, preventing the normal operation of electronic equipment and its technological development. Such legal protection implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6. **Such legal protection should respect proportionality and should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection**. In particular, this protection should not hinder research into cryptography.

The role of digital rights management, in particular technological protection, in cloud services (15)

<u>Europe: mixed rulings with healthy trends (but?)</u>.

In the last but one sentence on which the Milan court seems to concentrate in a somewhat isolated way, there are two principles. The first one is proportionality. This is a very important and valid principle. However, **in the given context, it should be applied not only from the viewpoint of whether or not in the name of proportionality it is justified to disregard the need for the protection of TPMs, but also in a way that whether or not it would be proportionate to remove the key element of the ecosystem of game industry and to deprive it of an indispensable means of protection against piracy** (and in this way to persuade it, along with its authors, that it is not worthwhile investing creative and financial efforts into the production of new attractive video games).

The second principle is that devices or activities which have a commercially significant purpose or use other than to circumvent TPMs should not be prohibited. The calculation of **the significance of this principle from the viewpoint of the question of whether or not the manufacture and distribution of modchips may be considered legal** is quite easy. **Zero. A modchip is a circumvention device**. **The sentence is about those devices** (for example, PCs and laptops were in mind) **which are used predominantly for other purposes**. If the question were whether or not a video console might be prohibited as a circumvention device this principle might apply. But **modchips have nothing to do with this.**

Summary on DRM (TPMs + RMI) protection

1. The obligations under Articles 11 and 12 of the WCT, Articles 18 and 19 of the WPPT and Articles 15 and 16 of the BTAP to provide adequate legal protection and effective legal remedies against unauthorized circumvention of technological measures (TPMs) and unauthorized alteration or removal of electronic rights management information (RMI) are fully applicable in the cloud environment. Cloud computing makes the use of TPMs possible in an extremely flexible, consumer-friendly and still efficient manner. This is not only a proof to rebut certain unfounded criticisms against TPM protection but also a reason for which truly adequate measures be applied for such TPM-supported (or by using another expression, DRM-supported) "cloud" business models.

Summary on DRM (TPMs + RMI) protection

2. Cloud business models guaranteeing adequate and effective but still flexible and well-balanced exercise and protection of copyright frequently use hardware/firmware TPMs in the devices through which protected works may be used in a duly controlled way as guarantees of normal exploitation of works. Hardware/firmware-based TPMs are protectable TPMs without any doubt whatsoever. The reason for which it is justified to refer to them specifically is that recently attempts have been made to remove this indispensable element from the cloud-based ecosystem of normal exploitation of works. The attempts take the form of trying legalize devices produced for unauthorized circumvention of such TPMs in general citing mere convenience justifications. At present, the attacks are directed mainly against firmware-based TPMs used in video consoles where mainly (but far from only) the game industry is concerned. The concrete objective is legalizing the use of "modchips" to circumvent firmware protection which would open the floodgates for game piracy and endanger sustainable creation and production of high-quality video games. Allowing unauthorized circumvention of firmware-based technological measures would be in conflict not only with the obligation to grant adequate protection for TPMs but also with the three-step test.

THANK YOU FOR YOUR ATTENTION

www.copyrightseesaw.net

ceeeca@t-online.hu