ALAI 2012 Congress
Kyoto, 16-18, October 2012

Copyright and Related Rights in the "Cloud" Environment

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

Dr. Mihály J. Ficsor*

INTRODUCTION

When the first draft of the program of the Kyoto Congress was prepared, there were only two WIPO "Internet Treaties:" the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) adopted in Geneva on December 20, 1996. Both of them entered into force in 2002 and, at the time of the completion of this paper,[1] both of them had 90 Contracting Parties.[2] However, now *de facto* there are three WIPO "Internet Treaties." The third one is the Beijing Treaty on Audiovisual Performances (BTAP) adopted in Bejing on June 26, 2012. The BTAP may be regarded as the third one since it confirms all the principles and maintains all the values of the WCT and the WPPT. Apart from certain details dictated by the different subject matter, its provisions correspond to (and, in several cases, are the verbatim reproductions of) the corresponding provisions of the WPPT.

This paper begins with the obligatory exercise of clarifying the concept of the "Cloud" – and cloud computing – and identifying those characteristics which may be relevant for the interpretation and application of the three "Internet Treaties." The paper then analyzes how the key provisions of the three Treaties may be applied in the cloud environment. Namely, the provisions on the rights concerned, on possible exceptions and limitations, and on the protection of technological measures and rights management information. Although the Treaties do not cover specifically the issues of liability for infringements of copyright and related rights (in particular, not as regards secondary liability), the paper deals with those issues too because they are inseparably interwoven with the questions of what rights and in which way may be applied for the acts performed in the complex structure of cloud-based systems. The paper is closed by summary conclusions.

THE CONCEPT OF THE "CLOUD" AND ITS RELEVANCE FOR COPYRIGHT

One more metaphor to demystify

Metaphors may be useful. They may simplify references to complex phenomena and may also make our style more colorful. However, when it comes to legal regulation, it is not the metaphor which is supposed to be regulated but the phenomenon to which it relates. Although this is obvious, we have seen already in the case of the Internet that certain metaphors could

* Member of the Presidency and Honorary President of the Hungarian Copyright Council, former Assistant Director General of WIPO.
[1] October 10, 2012.
[2] In this number, it is taken into account that Malaysia deposited its instrument of accession to the WCT and the WPPT on September 27, 2012 and that, thus, the Treaties will enter into force for the country on December 27, 2013.

influence people's thoughts in a way that the application of this correct principle – the need for keeping in mind the phenomenon and not being allowed to carry away by the metaphor – turns out to be less easy than expected. The expression "cyberspace" referring to the operation of the Internet was taken so seriously by some "netizen" ideologues and activists that they have gone so far as to claim that it forms a space outside our "traditional" world and, as such, it should be the realm of complete freedom where national laws and international treaties do not have anything to do. The adoption of the first two "Internet Treaties" to offer meaningful international standards for the digital online environment was only possible because, during the intensive preparatory work in various forms and forums,[3] we succeeded to clarify that such a thing as "cyberspace" does not exist the way suggested by some Internet gurus. There is nothing outside our "traditional" world; all the computers from where protected materials are uploaded and into which they are downloaded, all the communication facilities necessary for online communication, all the people who operate the system, all those who gain a lot by contributing to the use protected works[4] and other productions (quite frequently illegally), and all the owners of rights who may lose a lot can be found in one country or in another. Therefore, national laws and international treaties do have a lot to do with this phenomenon.

The same may be true as regards the "Cloud." Although it is obvious that, in reality, nothing takes place in some abstract "cloud" above us – but by means of computers and communication facilities that may be found, and are owned, operated and used by concrete identifiable persons or legal entities, in one country or in another – it is necessary to keep this in mind. If we do not do so, some people might be carried away again by this smart metaphor and may consider that now everything is merged in an amorphous cloudy – or even foggy – phenomenon where one cannot know who does what, where and in which way and, thus, it is impossible to apply copyright and to find out who are liable for infringements.

Definitions of the "Cloud"/"cloud computing"

The NIST definitions. It seems that the most generally accepted definitions and categorizations of the "Cloud" and cloud-based services are those which have been worked out and published by the National Institute of Standards and Technology (NIST), a division of the United States Department of Commerce.[5] (A document freshly published by the European Commission refers to a NIST definition too.[6]) Even those who do not explicitly mention NIST as a source tend to use the concepts and categories identified by it.

---

[3] In addition to the two WIPO Committees of Experts working on what became the WCT and the WPPT, *inter alia*, also two rounds of regional consultations in the three big regions of developing countries – Africa, Asia and Latin America – and "world forums" held at Harvard University, Mexico City, Paris and Naples.

[4] From now on, unless it otherwise follows from the context, the reference to „works" and „copyright" is to be understood also as a reference to objects of related rights and related rights.

[5] *NIST Definition of Cloud Computing* (Special Publication 800-145); available at http://csrc.nist.gov/publications/PubsSPs.html#800-145.

[6] On September 27, 2012, the document "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – unleashing the potential of cloud computing in Europe" was published (COM(2012) 529 final) accompanied by a Commission Staff Working Document (SWD(2012) 271 final). The latter document quotes the NIST definition (in p. 2) as also quoted in the following paragraph of this paper. The two documents mainly deal with general aspects of cloud computing from the viewpoint of the EU's single internal market, the contractual system (including cross-border licensing), guarantees for secure transactions, standardization, data protection, privacy protection, and even energy and environment aspects. Copyright-related issues (in addition to the questions of the contractual system, which is not covered by this paper, but by other papers to be presented at the Kyoto Congress) are mentioned only in two aspects (in the Commission Staff Working Document): private copying and – very briefly – liability of intermediaries.

The basic statement in the NIST definitions reads as follows:

> 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.

This overall definition hardly reveals all the key aspects of cloud computing that may be relevant for copyright, although it refers to quite an important one: on-demand network access to shared pool of resources for storage and other applications (rather than using the customers' own resources), which is frequently referred to as "virtualization." However, there is a second sentence of the paragraph: "This cloud model promotes availability and is composed of five essential characteristics**,** three service models, and four deployment models." The review of those characteristics and models may offer deeper insight into possible copyright implications of cloud computing and may also be helpful to understand what is meant by the first overall definition quoted above.

The five essential characteristics are as follows: (i) on-demand self-service; (ii) broad network access; (iii) resource pooling; (iv) rapid elasticity and (v) measured service. The latter two characteristics only refer to some convenient elements for the users of cloud services; the first three of them, however, may deserve closer attention from the viewpoint of copyright. They read as follows:

> *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
> *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants [PDAs]).
> *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

The *on-demand self-service* nature of cloud systems seems to be relevant from the viewpoint of the question of who may be regarded to perform acts covered by copyright (and, thus, who may be liable for direct infringements) and who else may have secondary liability.

Broad network access for use by heterogeneous platforms, including some "thin" devices has double copyright relevance. First, it corresponds to, and may satisfy, consumers' demand to get access to anything, anywhere, anytime and, thus, it is both a challenge and an opportunity for copyright owners. Second, the proliferation of "thin" devices is in connection with a "re-centralization" process of the online ecosystem which may have impact on the possibilities of exercising and enforcing copyright.

As a result of re-centralization of computing and online infrastructure – "virtualization" – the internet-abled devices used by consumers are getting similar to mere dumb terminals (as in the old pre-PC times in the 1960s and 1970s when such terminals were dependent on the operation of "smart" mainframe computers). In fact, a kind of interaction takes place between the advent of ever "smarter" "thin" devices (tablets, mobile phones, etc.) and the ever more widespread availability of cloud computing. The "thin" devices are dependent on, or at least they may be truly efficiently used only through, cloud services. At the same time, the attractiveness of cloud services is increased – their potentials may be more fully exploited – by the proliferation of such devices.

Broad network access to cloud services by heterogeneous platforms and devices, for the time being not only by "thin" but also by more autonomous "traditional" devices (PCs, laptops, etc.), allows the establishment of new inventive business models. It also facilitates the application of efficient – and, at the same time, user-friendly – DRM[7] systems. The possibility that consumers (along with a limited number of their family members and their closest – not only "virtual" – friends) may get access to protected works through a determined scope of different devices from different places may reduce, or at least limit to a tolerable level, the (frequently over-hyped) problems of interoperability and transportability of use of legally accessed works.

It should also be seen that the re-centralization trend – in particular when, on certain big platforms, making available of works is closely linked to the use of specific devices – may contribute to the emergence of more or less closed proprietary systems. Where a cloud platform becomes the only relevant – or at least an overly dominant – distribution channel for a certain category of works, competition and anti-monopoly issues may emerge. Such platforms may misuse their monopoly position and may dictate disadvantageous conditions both to owners of rights and to users of their services. Appropriate legislative and judicial protection is needed against such kind of misuse. The discussion of these issues, however, would go beyond the topic of this paper.

Cloud services also raise security and privacy problems since cloud service providers get in the possession of a huge amount of personal and internal data. Such information may be – and, as experience shows, quite often is – misused by cloud operators for commercial purposes. The potential problems arising with this are intensively discussed in both legal literature and in the press. However, they are not covered either by the specific topic of this paper.

Let us proceed now to the three service models determined in the NIST definition:

> *Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.[8] The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not

[7] The reference to DRM (digital rights management) usually means a combination of technological protection measures (TPMs) and rights management information (RMI). However, sometimes, what is meant may be just a TPM or a RMI system.

[8] (Original note in the text quoted) A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

This categorization may be of some help for judging the issues of possible direct or secondary liability of cloud service providers since it is about the question of who operates and may control and which aspects of the system.

Practically the same applies as regards the four "deployment models" mentioned in the NIST definition:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

It seems to be evident that, due to availability to the general public, public clouds deserve specific attention from the viewpoint of copyright. This does not mean, however, that the other three models are irrelevant. This is true also as regards "private clouds" since, although those services may only be available to one organization, within that organization, this may mean availability to various business units, and this may go much beyond the copyright concept of "private" use (which normally only means use within a circle of a family and a narrow scope of close friends).

Definitions in the reports prepared by national ALAI Groups in response to the congress Questionnaire. The reports prepared by the national ALAI Groups[9] try to define the "Cloud" and "cloud computing" by concentrating on those aspects that may be relevant for copyright, although some of them mainly state that there is no specific definition in the country concerned[10] or just refer to the NIST definitions.[11]

There is only one national report which quotes an official definition; namely, the *Mexican* report. It applies for the use of cloud computing in public institutions: "Cloud computing: a model of providing digital services that permits to public institutions to accede to a catalogue of standardized digital services, which may be: infrastructure as services; platform as services and software as services." [12] As it can be seen, this definition does not contain truly substantive elements; it rather only refers to the three service models described in the NIST definitions.

The reports, in general, stress the aspect of remote storage. The *Belgian* report states that "in general manner, it may be said that cloud computing consists in transfer to, and maintain on, distant servers data traditionally located on local servers or the user's client device."[13] The *Swiss* report contains, in a verbatim manner, the same definition.[14] The *French* report refers to this in a broader context by mentioning as a main characteristic that cloud computing essentially means „providing services through distant information technology capacities."[15] The *Hungarian* report also refers, as the key characteristic of the "Cloud," to the following aspect: „the users' digital contents, including their personal data as well as copies of protected works and objects of related rights, are not stored in PCs, laptops or other personal devices, but on servers operated by others."[16] The *Israeli* report offers the simplest definition: "Remote storage of digital files."[17] The definition in the *Italian* report is more detailed but essentially it also stresses the aspect of remote computing: "It is normally assumed that the Cloud provider

[9] All the reports to which reference is made in this paper may be found at the congress website: www.alai.jp/ALAI2012/program/national-report-e/html.

[10] Colombian Report at www.alai.jp/ALAI/program/national_report/Colombia.pdf, p. 1.; Finnish Report, prepared by Jorma Waldén, at www.alai.jp/ALAI/program/national_report/Finland.pdf, p. 1.

[11] Greece Report, prepared by Dionysia Kallinikou and Pierrina Koriatopoulou, at www.alai.jp/ALAI/program/national_report/Greece.pdf, p. 1; Japanese Report at www.alai.jp/ALAI/program/national_report/Japan.pdf, p. 1;

[12] Mexican Report, prepared by Ricardo E. Larrea Soltero and Luis Schmidt Ruiz del Moral, at www.alai.jp/ALAI/program/national_report/Mexico.pdf, p. 1. (*Computo en la Nube: al modelo de prestación de servicios digitales que permite a las instituciones públicas acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios*.) Source: *El Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, publicado en el Diario Oficial de la Federación* of September 6, 2011, Second Article, point V.

[13] Belgian Report, prepared by Axel Beleen, at www.alai.jp/ALAI/program/national_report/Belgium.pdf, p. 1. (*De manière générale, on peut dire que l'informatique en nuage consiste à déporter sur des serveurs distants des données traditionnellement localisées sur des serveurs locaux ou sur le poste client de l'utilisateur*.)

[14] Swiss Report, prepared by Vincent Salvadé, at at www.alai.jp/ALAI/program/national_report/Switzreland.pdf, p. 1. (*De manière générale, on peut dire que l'informatique en nuage consiste à déporter sur des serveurs distants des données traditionnellement localisées sur des serveurs locaux ou sur le poste client de l'utilisateur.*)

[15] French Report, prepared by Jean Martin in collaboration with Audrey Lefèvre, Franck Macrez, Thierry Maillard, Mélanie Clément and Pierre Sirinelli, at www.alai.jp/ALAI/program/national_report/France.pdf, p.1. (*On considère, selon l'approche classique des professionnels, qu'il s'agit de prestations de services de gestion de capacités informatiques distantes.*)

[16] Hungarian Report, prepared by Mihály J. Ficsor with the assistance of Pál Tomori, Gábor Faludi, Anikó Gyenge, Péter Mezei, András Szinger, Péter Munkácsi and Péter Tarr, at www.alai.jp/ALAI/program/national_report/Hungary.pdf, p. 1.

[17] Israeli Report, prepared by Tony Greenman, at www.alai.jp/ALAI/program/national_report/Israel.pdf, p. 1.

supplies his customers with technology, software and/or storage space that are accessible through an Internet browser. The remote exploitation of resources and the dematerialization of tools available to the users are therefore the main features characterizing the Cloud."[18] The *Norwegian* report emphasizes the remote storage aspect too: "the cloud is generally understood as an external data storage unit or database used to provide a wide spectre of services where data storage capacity is offered to end users."[19] The *Polish* report states practically the same when it mentions the "style" of cloud-based services "as a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies."[20] The *US* report, having quoted the basic NIST definition and another one in legal literature, concludes as follows: "we understand 'the Cloud' to mean remote storage and associated services offering access, storage, and communication of the remotely stored content."[21]

The *Croatian* report rather emphasizes the resource-sharing aspect of cloud computing: "'Cloud' computing or simply the 'Cloud' can be defined as Internet-based computing that facilitates sharing of resources, software and information."[22]

The remote storage is also in the focus of the somewhat more detailed definition in the *Spanish* report:

> From a legal point of view we could define "The Cloud" as a group of services of the *Information Society* that allow storage of data that the user-subscriber can access to from any device connected to the Internet in any given time and from any given place. The information is stored permanently on Internet servers and it is sent to temporary client caches, including laptops, entertainment centres, etc. (in terms of exploitation of the works, it would be a kind of "making available" or a service that can combine storage and public communication of the works).[23]

The *German* report contains a more detailed definition too:

> Cloud Computing describes data processing on several, interconnected servers which are accessed over a network and from which the usage of software and hardware is offered. The services offered in the Cloud cannot necessarily be located geographically, since their individual components may be distributed on all servers of the Cloud. The Cloud Services are at least partially performed at a location distant from the user. The essential characteristic which differentiates Cloud Services from conventional web sites and conventional methods of outsourcing is the employment of several interconnected servers: web sites can also be stored on only one single server; IT outsourcing can involve only one big mainframe computer.[24]

The *Dutch* report, having quoted the basic NIST definition, states:

---

[18] Italian Report at www.alai.jp/ALAI/program/national_report/Italy.pdf, p. 1.
[19] Norwegian Report at www.alai.jp/ALAI/program/national_report/Norway.pdf, p. 1.
[20] Polish Report, prepared by Filip Lukaszewicz under the direction of Teresa Grzeszak, at www.alai.jp/ALAI/program/national_report/Poland.pdf, p. 1.
[21] US Report, prepared by June M. Besek, Philippa S. Loengard and Idara Udofia , at www.alai.jp/ALAI/program/national_report/UnitedStates.pdf, p. 1.
[22] Croatian Report, prepared by Romana Matanovac Vučković, Ivana Kunda, Iva Kuštrak and Marko Jurić, Tihomir Katulić at www.alai.jp/ALAI/program/national_report/Croatia.pdf, p. 1.
[23] Spanish report, prepared by Ramón Casas, Franz Ruz, Eva Soria and Nerea Sanjuan, at www.alai.jp/ALAI/program/national_report/Spain.pdf, p. 1.
[24] German Report, prepared by Anna Gietke, at www.alai.jp/ALAI/program/national_report/Germany.pdf, p. 1.

> In a more everyday use 'The Cloud' is defined as accessing software or other content that is stored remotely on a network of computers (often by third parties) through the internet by personal devices that function as terminals. The two main advantages for consumers are that they do not need to store (a lot of) content on their own devices and that the information is available to them at any time or place (even if they are not in the vicinity of their own computer).[25]

The report adds the following remark in a footnote: "Downloading and subsequently storing software or content on the user's computer is not included in this definition. One of the essential characteristics of the Cloud is that the content remains stored in the Cloud and it is only *used* on the terminal." This comment refers to the way cloud-based systems function and to their "virtualization" aspect.

In the *Swedish* report, the definitional elements are combined with references to typical forms of cloud-based services:

> "The Cloud" is normally understood to embrace different forms for worldwide accessibility via the Internet. Hence, it may offer access to IT resources via the Internet – such as storage, Gmail, Facebook and Google Apps – standardized communication from one person to the masses, database answering to questions, self-service, scaling resources and distributed/visualized infrastructure. Cloud computing services may therefore offer platforms for processing programmes, computing technology and storing facilities.[26]

The definition in the UK report reads as follows:

> "The Cloud" generally refers to a wide ranging possible shapes and designs. Cloud computing broadly describes the service of providing computer storage and computing online facilities to its users who chose to transfer processing and storage facilities to a third party established at a different location.[27]

Use of works in and through the "Cloud"

If we consider the above-outline definitions of the "Cloud" and cloud computing, it can be seen that copyright-related cloud services had been used even before these concepts were defined and their use became fashionable. The most obvious examples are the internet-based e-mail systems (Gmail, Yahoo, Hotmail, etc.) where the customers use the providers' infrastructure and software applications by uploading messages, frequently with attachments containing works protected by copyright, which are then stored in and accessed through the providers' system. Social networks – like Facebook – are operated in a similar manner and, in the case of such networks, it is even more usual that all kinds of protected materials are attached to "posts" which then may be "shared" – in fact, made available in an interactive manner – to a number of users of the network (the scope of which tends to be much broader then in the case of e-mail communication and thus goes beyond what may still be considered private).

[25] Dutch Report, prepared by Arnaut Groen, at www.alai.jp/ALAI/program/national_report/Netherlands.pdf, p. 1.
[26] Swedish Report, prepared by Jan Rosen, Gunnar Karnell and Daniel Westman, at www.alai.jp/ALAI/program/national_report/Sweden.pdf, p. 1.
[27] UK Report, prepared by Brigitte Lindner, Florian Koempel, Gaetano Dimita and Paul Torremans, at www.alai.jp/ALAI/program/national_report/UnitedKingdom.pdf, p. 1.

"Virtual video recorders" form another category of services which, when they were launched were not called yet cloud-based services but – retrospectively – may be recognized as such. Such services allow consumers to record television programs in the storage space reserved for them in the providers' infrastructure and then to make the system to transmit the recorded programs be using the provider's software. (This may be a somewhat simplistic description of "virtual video recorders." As it is discussed below, in the case of some of the services referred to as "virtual video recorders," at least under certain national laws, it may be disputed whether truly the consumers or rather the providers perform the various acts covered by copyright.)

The following wave of business models – "cyberlockers" – were established at the time when the concept of the "Cloud" had appeared already in the internet-related terminology. "Cyberlockers" (such as those offered by Dropbox, RapidShare or Megaupload) are similar to "virtual video recorders" in the sense that protected works are included in specific storage spaces reserved for consumers in the providers' infrastructure and the consumers may get access to the works by using the providers' software. At the same time, there are two significant differences. First, not only television programs are stored in the "lockers" but various categories of works and, second, the works are normally uploaded by the customers. In principle, the links to the uploaded works are supposed to allow access only to the costumer concerned and, at maximum, to the members of his or her family and a limited number of closest friends (that is, who do not qualify yet as members of the public). It is well known, however, that some of these systems are not used in that way; through the links, protected works are frequently made available to the public without authorization. The impact is more or less the same as that of "file sharing" systems. (Although the impact is the same, the chances of copyright owners to enforce their rights might be somewhat better due to the fact that it is easier to control the limited number of "cyberlockers" as sources of illegal making available of works than the decentralized "file sharing" systems operated through powerful PCs and laptops dispersed around the world.)

Apple's iTunes-iPod system, which became the first truly successful legal channel for online making available of music, has also extended to cloud services; in particular as regards its *iCloud* and *iMatch* functions. It uses proprietary DRM and proprietary devices for lawful distribution. The iMatch function also allows uploading and "legalizing" illegal copies and then using them in legalized form (in principle, by the consumers concerned).

The three big cloud provider services of Apple, Amazon and Google have been already established in a way that they were referred to as cloud systems. They also use proprietary DRM and, in close connection, produce and make available their own proprietary devices (smart phones, tablets, etc.), *inter alia*, for the use of works.

These cloud giants serve for the use of different categories of works of different owners of rights. They tend to become indispensable channels for legal on-line use and, as a result, to obtain monopoly position (which then, as mentioned above, may also be misused in relation of both their customers and of the owners of rights concerned).

Owners of rights, however, may also establish their own systems to operate in fuller accordance with their legitimate interests. The *UltraViolet* cloud-based service established by a consortium with active participation of film producers (see below) is a good example for this.

THE "CLOUD" AND COPYRIGHT: THE THREE "INTERNET TREATIES," COPYRIGHT ACTS AND CASE LAW

The three WIPO "Internet Treaties" have adapted the international copyright norms to the digital on-line environment. In comparison with the existing WIPO conventions and the TRIPS Agreement – perhaps with the exception of the rights of performers, and in close connection with them, the rights of producers of phonograms (in the case of which the exclusive right of (interactive) making available to the public may truly be characterized as a new right) – they have not brought about real extension of the scope of protection. What they really mean is this: (i) clarification on how the existing treaty provisions (in particular those on the right of reproduction – and its corollary: the right of distribution – and on exceptions and limitations) may be applied in the new environment; (ii) a combination of the rights of broadcasting and communication to the public and the right of distribution in a way that it also covers the right of (interactive) making available to the public; and (iii) provisions to guarantee the applicability of technological protection measures and rights management information as new means of exercising and enforcing rights in the digital online environment (rather than new rights).

The purpose of this paper does not extend to offering a detailed presentation of the "Internet Treaties." The first two Treaties – the WCT and the WPPT – have been described and commented on in various books[28] and articles, and the analysis of the third one – the BTAP – has also begun.[29] The knowledge of their basic principles and provisions may be considered as granted among the participants in the Kyoto ALAI Congress. Thus, we may simply begin with a review of the typical acts performed in connection with the use of works by means of cloud computing and trying to judge which rights provided in the "Internet Treaties" apply for them, who are to be considered to perform those acts, and who may have direct or secondary liability for possible infringements.

There are no specific provisions on cloud-related acts in national copyright laws. Such provisions are not needed since the provisions of the Treaties – and of the national copyright act that have duly implemented them – are sufficiently technology-neutral. The right of reproduction is to be applied for any kind of reproduction "in any manner or form;" the provisions on the right of making available to the public has been adopted explicitly with the intention to cover all kinds of interactive uses in as neutral a manner as possible; and the provisions on the protection of technological measures and rights management information do not contain any technological specifications either.

At the same time, there is already quite rich case law available concerning the use of works in the "Cloud." The most relevant rulings are reviewed in the paper, below.

In the digital online environment – and the "Cloud" is part of it – usually three kinds of acts are relevant from the viewpoint of copyright: inclusion and storage of works in electronic memories, interactive making available to the public or non-interactive forms of

[28] *See* Jörg Reinbothe – Silke von Lewinski: „*The WIPO Treaties 1996 – The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. Commentary and Analysis*," Butterworth, LexisNexis, 2002; Mihály Ficsor: „*The Law of Copyright and the Internet – The 1996 Treaties, their Interpretation and Implementation*," Oxford University Press, 2002 (hereinafter: Ficsor – Oxford); Sam Ricketson – Jane C. Ginsburg: „*International Copyright and Neighbouring Rights – The Berne Convention and Beyond*," Oxford University Press, 2006.

[29] *See*, e.g., Mihály Ficsor: „*Beijing Treaty on Audiovisual Performances (BTAP) – first assessment of the third WIPO 'Internet Treaty'*" available at www.copyrightseesaw.net/archive/?sw_10_item=24.

communication to the public, and getting access to services through downloading or reception of streamed works (reception in domestic environment normally is not a qualified act under copyright, but it may also have a relevance when technological measures are applied).

"VIRTUAL VIDEO RECORDERS" AS AN OLDER CLOUD GENERATION – FIRST ANALYSIS OF CLOUD-RELATED ACTS

Cablevision: the mother (or grandmother) of cloud-related copyright cases

Three issues – two kinds of court decisions. The basic question is who performs and what kinds of acts when a work is uploaded in the "Cloud" and then downloaded or streamed on the basis of the uploaded "cloud copy." In this respect, the first court decision which was followed with very great attention and then intensively analyzed was the one adopted in the *Cartoon Network LP v. CSC Holdings, Inc.* – or "*Cablevision*" – case. It seems worthwhile analyzing this case in a detailed manner (perhaps, in the most detailed manner among the relevant cases) since it concerned all the basic questions regarding the copyright qualification of the relevant acts, and it identified all the important issues to be addressed, the possible options, and the problems which may emerge with certain solutions.

The report prepared by the US ALAI group in response to the congress Questionnaire describes the basic facts of the case as follows[30]:

> 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.[31] 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).[32] 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.[33][…] User copies were created by splitting the broadcast programming data into one stream constituting 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.[34] When a user wished to view the stored program, Cablevision's transmission would originate from that user's personal stored copy.[35] 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.[36]

It seems it was considered as granted that the act of recording broadcast programs for private and personal purposes is fair use (in general, it is regarded as a free use – with or without the

[30] US Report, p. 3.
[31] (Original note in the text quoted) 536 F.3d 121 (2d Cir. 2008).
[32] (Original note in the text quoted) 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.
[33] (Original note in the text quoted) *Id.* at 615.
[34] (Original note in the text quoted) *Cartoon Network, LP*,536 F.3d at 125.
[35] (Original note in the text quoted) *Twentieth Century Fox Film Corp.*, 478 F. Supp. 2d at 615.
[36] (Original note in the text quoted) *Cartoon Network LP*, 536 F.3d at 125.

payment of an equitable remuneration – also in those countries which do not apply the fair use doctrine but provide a more or less exhaustive list of exceptions and limitations in their copyright acts). Similarly, it did not seem to be disputed that, if it could be accepted as a fact that the customers make copies for their own personal and private purposes in the storage spaces (basically for time shifting), it could also be regarded as a fair use. The plaintiffs, however, did not agree with this kind of factual description.

The court had to decide three issues: (i) whether or not Cablevision made unauthorized copies in the buffer; (ii) whether or not it made unauthorized copies on its server, and (iii) whether or not it performed acts of unauthorized public performance when recorded programs were transmitted to the customers to view them later. The District Court gave an affirmative answer to all the three questions, but the Second Circuit reversed the ruling also on all them.

The author of this paper tends to agree with the District Court and, with due respect, to disagree with the Second Circuit. And he definitely agrees with Professor Jane Ginsburg' thorough analysis of the Second Circuit decision[37] which, as a minimum, has raised what seem to be justified doubts about the adequacy of certain aspects of the ruling. Furthermore, in accordance with this, as regards the issue of transitory copies, the author of this paper has more sympathy with the Copyright Office's DMCA Section 104 Report[38] than with the Second Circuit's findings.

Let us review the three issues mentioned above.

Buffer copy. It seems that the Second Circuit did not question the validity of the agreed statement adopted concerning Article 1(4) of the WCT (and through it concerning Article 9(2) of the Berne Convention) according to which the storage of a work in an electronic memory is also an act of reproduction.[39] Nevertheless, on the basis of the analysis of the definition of "fixation" in section 101 of the US Copyright Act in (fixation which, in turn, is a key element of the definition of "copies" – and, thus, implicitly also "reproduction") it still rejected qualifying what appeared in the buffer as a "copy."

In section 2 of the US Copyright Act, the decisive first sentence[40] of the definition of "fixation" reads as follows:

> A work is "fixed" in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.

The court interpreted the definition in this way:

---

[37] Jane C. Ginsburg: "*Recent Developments in US Copyright Law – Part II, Case law: Exclusive Rights on the Ebb?*", Colombia Public Law Research Paper No. 08-192, December 2008; published in January 2008 in the *Revue Internationale du Droit d'Auteur*; available on the website of the Social Science Research Network at www.papers.ssrn.com/sol3/papers.cfm?absracts_id=1305270 (hereinafter: Ginsburg).

[38] Available at www.copyright.gov/reports/studies/dmca/sec-104-report-vol-1.pdf.

[39] Agreed statement concerning Article 1(4) of the WCT: „The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention."

[40] The second sentence reads as follows: „A work consisting of sounds, images, or both, that are being transmitted, is 'fixed' for purposes of this title if a fixation of the work is being made simultaneously with its transmission."

> [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).[41]

On the basis of this interpretation, the court found that although the buffer embodied the works, the 1.2 second duration of the embodiment was too transitory to correspond to the "duration" criterion.

It is to be noted that the court, rightly enough, took it as granted that the embodiment of works in an electronic medium corresponds to the concepts of "copy" and "fixation." As mentioned above, this is in due accordance with the agreed statement adopted concerning Article 1(4) of the WCT.

It seems, however, that the court's findings contain a contradiction concerning the concept of sufficient stability of embodiments of works.

In the view of the author of this paper, the key element of the definition of "fixation" is this part: "*embodiment… sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated*." It was not disputed by the parties or by the court that the buffer copy was sufficiently stable to serve as a basis for subsequent reproduction on the server. In this respect, it may be worthwhile quoting the WIPO Guide on the issue of the duration of copies from the viewpoint of the concept of the reproduction:

> CT-1.44. The delegations which, at the diplomatic conference, opposed the second sentence of the agreed statement concerning storage of works in electronic memories raised some arguments which did not relate to storage in general but only to some kinds of temporary forms of storage, such as some technologically indispensable, but – from the viewpoint of the exploitation of the works concerned and the legitimate interests of owners of rights – completely irrelevant forms of temporary reproductions taking place during a transmission in interactive digital networks or incidentally to an authorized use of the work. Their idea was that "too temporary," "too transient" reproductions must not be recognized as reproduction. This, however, would have been in conflict with Article 9 of the Berne Convention under which the duration of the fixation (including the storage in an electronic memory) – whether it is permanent or temporary – is irrelevant (as long as, *on the basis of the [new] fixation,* the work may be perceived, reproduced or communicated).[42]

It does not seem to be appropriate to try to define the concepts of "copy" and "reproduction" on the basis of the duration of the embodiment expressed in a certain number of hours, minutes or seconds and to consider that, if the duration is one hour, one minute or one second less, it is not a copy and not an act of reproduction anymore. A functional definition may only be adequate, based on those criteria which are relevant for the exploitation of works. It is submitted that, if the embodiment of a work is sufficiently stable for allowing it to be "perceived, reproduced, or otherwise communicated," it should be regarded as a copy.

---

[41] See US Report, p. 4.

[42] Mihály Ficsor: „*Guide to the Copyright and Related Rights Treaties Administered by WIPO and Glossary of Copyright and Related Rights Terms*," WIPO publication No. 891 (E), 2003, (hereinafter: WIPO Guide and Glossary), p. 195.

Prof. Ginsburg outlined, in the following way, the reasons for which apparently the Second Circuit had erred:

> Despite its insistence that the Copyright Office and the plaintiffs were "read[ing] the 'transitory duration' language out of the statute," the Second Circuit may in fact have been reading "transitory duration" into the wrong part of the definition of fixation. Recall the definition: "A work is 'fixed' in a tangible medium of expression when its embodiment in a copy or a phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." The Second Circuit has equated the "it" in "sufficiently permanent or stable to permit it to be perceived . . ." with the work's "embodiment in a copy." Hence the court's inquiry whether the embodiment lasts for a period of more than transitory duration. But this construction is dubious both grammatically and as a matter of common sense. Grammatically, the "it" refers to the "work," not the "embodiment." […] Substantively, substituting "embodiment" for "it" would mean that the *embodiment* would be "perceived, reproduced, or otherwise communicated." But the embodiment – that is, the "tangible medium of expression" – is not what the user "perceives." Indeed, for digital storage media, particularly those internal to a computer, the user will never see the "embodiment," but the embodiment will enable the user to see the *work*, albeit "with the aid of a machine or device." By the same token, in the digital context, the "embodiment" is not "otherwise communicated," because the communication will produce new embodiments; the work contained in those embodiments is what is "communicated."[43]

She also reviewed the records of the legislative history of the definition of "copy" and "fixation" and other copyright-related legislative developments in which she had not found sufficient justification for the Second Circuit's position, but much more for the Copyright Office's DMCA Section 104 Report,[44] and then she added:

> Rather than seeking the correct characterization of the transient copy, it might make more sense to reassess whether the activity which the transient copies make possible is in fact infringing. In *Cablevision*, for example, the characterization of the buffer copies that Cablevision made becomes important because the court – probably incorrectly – determined that Cablevision did not make the copies that served as the source of the time-shifted transmissions, and furthermore – and equally dubiously – held that those transmissions were not public performances. That said, policy reasons may counsel concentrating on the intermediate copy when the end use can plausibly claim to be non-infringing. Where a commercial exploitation is at issue, if the intermediate copy is deemed too transient to trigger liability of its own accord, then one may anticipate an inclination to find an infringing act at the end of the chain. But if the end user is an

[43] Ginsburg, p. 9 (note left out).

[44] For the Report, see note 38, above; for the analysis, see Ginsburg p. 13: "The Copyright Office's suggestion that economic significance could supply the dividing line between copies within and outside the scope of the exclusive right of reproduction not only avoids the metaphysical quandary of determining the temporal frontiers of a 'reproduction;' it also offers a reason for excluding some 'purely evanescent or transient reproductions'; they do not undermine the author's exercise of her exclusive rights.[…] If, by contrast, transient reproductions do have value, but are neither subsumed within the public performance right nor trigger the reproduction right, then ruling these copies outside the scope of copyright effectively attributes to Congress an intent to create a two-track system, in which authors would control markets for fixed copies and for public performances and displays of protected works, but in which third parties could exploit whatever reproduction markets they could develop for 'unfixed' copies of those works.46 It is not likely that Congress would have anticipated such markets, and even less apparent what policies such a construction would advance. Instead, where unauthorized transient copies do compromise the exercise of exclusive rights (as in *Cablevision*), it would follow that these copies constitute actionable 'reproductions.'"

> individual consumer rather than a commercial entity, we may sense some discomfort labeling her acts as infringement, particularly if she does them at home. Yet we also recognize that copyright markets are increasingly consumer-enabling. It may be desirable to alleviate the ensuing pressure on the copyright system by focusing on the burgeoning businesses that transit copyrighted works to consumers.[45]

This is probably so. At the same time, it is also possible to deem an intermediate reproduction in a buffer copy as an indispensable step – without any independent economic significance – to perform an act which is the really relevant one from the viewpoint of the exploitation of a work. One may say that, if the relevant act is lawful, it may justify exempting the temporary act from the application of the right of reproduction as under Article 5(1) of the EU Information Society (Copyright) Directive[46] or providing for an exception in another form (on the basis of the fair use doctrine or the *de minimis* principle). However, Prof. Ginsburg seems to be right. Although the exemption of such an intermediary copy may be justified where it is made for the use of the same private person as the one who performs the act of reproduction, it is not necessarily the case where it is made by another person; in particular if it is part of that other person's profit-oriented activity. As mentioned above, the second issue to be addressed in the *Cablevision* case was exactly the question of who made the more permanent copies in the individual storage spaces reserved for the customers.

More permanent copies made on server storage spaces. It was not disputed in the case that, in addition to – and as a result of – the buffer copies, more permanent copies were made on Cablevision's servers. The real issue was who made those copies: Cablevision or its customers? The Second Circuit found that the customers made the copies because copying was performed by means of a fully automated system and, thus, not the Cablevision's but the customers' acts had the "volitional" nature of actually making the copies.[47] To justify this finding, the court referred by analogy to different ways of making copies in copy shops and time-shifting in "traditional" video recorders (VCRs).

As regards copy shops, the court was of the view that the Cablevision system was similar to the case where a copying machine is just made available to the members to the public who then make copies, rather than where the owner or employer of a copy shop makes copies at the request of the customers. In the latter case, the copy shop operators may be direct infringers while, in the former case, the consumers perform the acts covered by copyright and, thus, the copy shop at most might only have contributory liability. The court also likened the Cablevision system to a virtual video recorder which was just made available to the customers to operate them from their home.

Prof. Ginsburg did not seem to be impressed by the analogies presented by the Second Circuit and she questioned even the basic principle that "volition" concerning the creation of copies

[45] Ginsburg, p. 13.

[46] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. Article 5(1) reads as follows: "Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:
(a) a transmission in a network between third parties by an intermediary, or
(b) a lawful use
of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2."

[47] (Note in Ginsburg) 48 536 F.3d at 131.

of concrete works is an indispensable element of infringement of the right of reproduction. She drew attention to the weak points of the court's findings in this way:

> The court's principal authority for a volition requirement, *Religious Technology Center v. Netcom On-Line Communications Services*,[48] concerned a "mere conduit" online service provider, who simply conveyed copies of works from one subscriber to another. By contrast, Cablevision's own transmissions are the *source* of the copies the subscribers request. Second, the copy shop analogy does not track the conduct at issue nor convey the extent of the entrepreneur's volition: one would have to imagine a copy shop engaged in a remote printing operation, in which the customer would select from the works in the copy shop's inventory, and then transmit a request to print out the document; the copy shop in turn would automatically print out the document, charge the customer's account, and store the printout for the customer's pick-up.[49] In this scheme, the entrepreneur arguably has demonstrated volition that any of its inventory be copied, even if it cannot be shown that any particular work be the object of any particular customer's request at any particular time.[50]

Prof. Ginsburg was of the view that a document delivery service could have been a more pertinent analogy. She drew attention to the fact that, similarly to Cablevision, services such as Lexis "sell[] access to a system that automatically produces copies on command,"[51] and added: "But, in *New York Times v Tasini*,[52] the Supreme Court appears to have assumed that, when a customer requests a particular article that was published in the New York Times, Lexis, not the customer (or at least, not only the consumer), creates that copy from its database containing the full contents of the collective work."[53] Then she quoted the *Tasini* court stating that "[t]he Electronic Publishers […] are not merely selling 'equipment'; they are selling copies of the Articles,"[54] and pointed out as follows:

> Although the court did not spell out "selling copies *that they made* of the Articles," the specification is implicit and follows from the Court's earlier determination that Lexis was reproducing and distributing the freelance journalists' articles. The court thus did not conceptualize Lexis' activities as selling its customers access to Lexis' automated retrieval system in order that the customers might make copies of plaintiffs' articles for themselves – even though the customer's computer, on receipt of the communication from Lexis, is embodying a copy in its temporary memory, so that perhaps *both* Lexis and the customer are reproducing the work. (In Cablevision's system, by contrast, the copy is embodied on the servers of Cablevision.) Moreover, Lexis was "selling copies" of articles whose automatic generation would, under the Second Circuit's analysis, have deprived Lexis of the requisite "volition" as to the identity of each article sold.[55]

The Second Circuit finally chose "traditional" video recorders as an analogy, and based its decision on a non-litigated implied understanding that, if a consumer is deemed to make copies on Cablevision servers for subsequent retrieval for viewing them, it is a kind of "time shifting," and as such, on the basis of the findings made in *Sony*, similarly to recording programs on traditional video recorders, it is not an infringing act.

---

[48] (Note in Ginsburg) 907 F. Supp. 1361 (N.D. Cal. 1995).
[49] (Note in Ginsburg) Thanks to Prof. Tony Reese for this analogy.
[50] Ginsburg, p 15.
[51] (Note in Ginsburg) 536 F.3d at 132.
[52] (Note in Ginsburg) 533 U.S. 483 (2001).
[53] Ginsburg, p. 16.
[54] *Id.* (Note in Ginsburg) Id. at 504 (meaning 533 U.S. 483 (2001) at 504).
[55] *Id.*

However, on the basis of the analysis presented above, it seems doubtful whether truly the customers make the copies. Reproduction on the provider's server – even if in separate storage spaces – may better be characterized as the first element of a double-on-demand service. At the first demand of a customer, the provider's automated system makes a copy of a work. The copy resides on the provider's server – in the "Cloud" – and, at another demand of the consumer, the work is transmitted to the consumer for viewing.

This description of the second on-demand element indicates, as a minimum, a strong similarity to the acts of (on demand) making available to the public covered by an exclusive right of authorization under Article 8 of the WCT, Articles 10 and 14 of the WPPT and Article 10 of the BTAP. It is true that only those members of the public may get access to the work at a time (and, depending on the specific aspect of the system, from a place) individually chosen by them who previously have also used the first on-demand element of the system – but *all of them* may do. It may hardly be denied that this kind of making available is a service of the provider and, as part of its business model, a profit-making activity. This is so, even if, from the viewpoint of the end users, the benefits from the system are similar to fixing programs on "traditional" video recorders. The only difference between an act of "typical" on-demand making available and the way works are made available through a Cablevision-type service – in both cases, through automated systems normally without any specific human intervention – is that, in the latter case, as many copies are recorded and made available for on-demand viewing as the number of members of the public which have used the first on-demand element of the service. The real impact from the viewpoint of the exploitation of works recorded and made available would not differ in a substantial manner if the provider simply made one copy on its server and made it available for viewing to any consumers who want to view it.

However, as it is described in the following paragraphs, the Second Circuit found that, when an on-demand transmission takes place from the server space to a consumer, it is a private communication (or private "performance"). As mentioned above, the author of this paper is of the view that this finding may not be necessarily well-founded, and, in this respect too, he shares the doubts expressed by Prof. Ginsburg in her analysis.

Transmissions from server spaces to customers. As mentioned above, the Second Circuit found that, when the copies made on Cablevision's servers are transmitted at a customers' demand through an automated system, no "public performance" takes place.

It is to be noted that, from the viewpoint of the categories under the US Copyright Act, the expression "public performance" may be regarded as a "short-hand" reference to the category defined in section 101 as "to perform or display a work 'publicly'" in the following way:

> To perform or display a work "publicly" means—
> (1) to perform or display it at a place open to the public or at any place where a substantial number of persons *outside of a normal circle of a family and its social acquaintances* is gathered; or
> (2) *to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) or to the public,* by means of any device or process, *whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.* (Emphasis added.)

As it can be seen, this concept of public performance also extends to communication to the public in accordance with the concept of such an act under Article 8 of the WCT, Articles 10

and 14 of the WPPT and Article 10 of the BTAP, and seems to be a suitable basis for the implementation of the provisions of the Treaties also as regards the acts of (interactive) making available to the public. (The provisions of the Copyright Act on the right of distribution may be the other means of implementation in accordance with the "umbrella solution"[56] adopted at the 1996 WIPO Diplomatic Conference. The problems created in this respect by the case law are discussed briefly below.)

It is submitted that, if one reaches the conclusion that the court's finding regarding the "private" nature of the transmissions between Cablevision's servers and the costumer is not correct, and that, therefore, "communication to the public" takes place, then, due to the interactive, on-demand nature of the communication, an act of making available takes place as provided in the three WIPO "Internet Treaties." There are sufficient reasons to reach such a conclusion. Prof. Ginsburg seemed to agree with this; at least, certainly as far as the public nature of the communication was concerned. She wrote about this in her article in the following manner:

> The court's parsing of the text of the Copyright Act is peculiar if not perverse. The key phrase in the definition is "to the public." "The public" in the case of a television transmission is the intended audience, or, in the case of a cable service, the subscribers. The phrase "members of the public capable of receiving the performance" is not intended to *narrow* the universe of "the public." On the contrary, its role is to clarify that a transmission is still "to the public" even if its receipt is individualized.[…] The "members of the public capable of receiving the performance" do not stop being "members of the public" just because they are "capable of receiving the performance" one at a time. By the same token, it should not matter whether "the performance" originates from a single source copy repeatedly transmitted to individual members of the public "in different places at different times,"[…] or from multiple copies each corresponding to a particular place and/or time.[57]

It is another matter that, as Prof. Ginsburg pointed out in her study, under the US case law, doubts have emerged on the applicability of the right of making available to the public on the basis of the right of distribution. It would go beyond the topic of this paper to analyze these specific problems in the US law. The author of this paper must be satisfied with the remark that he agrees with Prof. Ginsburg's legal analysis which outlined the possibility of an interpretation of the provisions of the US Copyright Act concerning the concept and right of distribution on the basis of which, in accordance with the WIPO "Internet Treaties," the right of making available could be recognized and applied.

Post-Cablevision case law in the US. The US response to the congress Questionnaire, after a brief description of the Cablevision case, offers a short review of the case law which was regarded a sort of follow-up to the Cablevision judgment. The cases listed concern different cloud-based business methods and mainly others than "virtual video recorder" services (the relevant rulings are dealt with below under other titles of this paper), but one of the cases mentioned in the report concerned the same kind of service.

It was the *ABC, Inc. v. AEREO, Inc.*[58] case in which the District Court ruled that *Cablevision* compelled a finding that the defendant's service, converting live over-the-air broadcasts into individualized Internet streams without authorization, did not "publicly" perform the broadcasters' works. (Aereo's service allows a subscriber to connect to a small antenna

[56] See WIPO Guide and Glossary, pp. 209-210.
[57] Ginsburg, p. 28 (notes left out.)
[58] (Note in the US Report) No. 12 CIV. 1540 AJN, 2012 WL 2848158 (S.D.N.Y. July 11, 2012).

located at Aereo's data center to receive broadcast television signals, to convert and store them in personalized files and then, at the subscriber's request, to pass the digital broadcast stream to the subscriber.[59])

"Anti-Cablevision" developments in other countries: less shadow, more sunshine for owners of copyright

Germany. On April 22, 2009, the German Federal Court of Justice (*Bundesgerichtshof* (*BGH*)) adopted its "Internet Video Recorder" ruling which concerned three cases[60] between German broadcasters RTL and SAT1 and two "virtual video recorder" services: Shift.tv and Save.tv.

The defendant companies allowed the recording of various television programs, including those of the plaintiffs, on personal storage spaces reserved for their customers. The customers were able to get access to the recordings at any time and from any place chosen by them. The actual technical details, however, had not been sufficiently clarified by the lower courts. Therefore, the BGH remanded the cases by determining what criteria should be taken into account to decide on the possible liability of the providers of these services.

The first issue was who, in fact, performs the acts of reproduction in a case where the service operates the reproduction and storage facilities and the customers initiate the copying of works on their storage spaces. The BGH held that the person performing the act of copying is the one who triggers it, even if he or she does so by means of technical facilities made available by the provider but that it depends on the concrete technical aspects of the system who may be deemed to be the direct infringer in case of unauthorized copying.

The "virtual video recorder" providers argued that, since their customers do not pay any fee for copying and retrieving the contents involved, Article 53(1) of the German Copyright Act applies (which allows making single copies on behalf of others for private purposes provided that it is done without a payment). The BGH disagreed and held that, where the service providers' objective is to gain, at least, indirect profit, their services are "made for payment." The court pointed out that it is irrelevant that the customers do not pay fees when the service providers may gain profit for the activity through other channels; in particular for advertisements placed on their websites (due to the number of visitors of the site as a result of the free-of-charge nature of the services). Thus, as regards the question of direct liability for possible infringements of the right of reproduction, the BGH adopted an "if… then…" type ruling.

As regards the right of communication to the public, the BGH found that it is infringed (unless the service providers obtain a license for the relevant acts) even if the customers trigger the transmissions from their storage spaces. The court held so in view of the fact that a sufficient number of customers were involved who jointly qualified as members of the public.

It seems, however, that the guidance offered by the BGH has not been sufficient to establish a completely harmonized practice in Germany concerning "virtual video recorder" services.

[59] US report, p. 5.
[60] BGH, Nos. I ZR 215/06; I ZR 216/06; I ZR 175/07 of April 22, 2009.

The report prepared by the German ALAI Group in response to the congress Questionnaire[61] refers to another court decision adopted in a *Save.tv* case (as discussed below it was not the only one that concerned Save.tv) by the Higher Regional Court (OLG) of Dresden[62] which dealt with the question of application of the right of making available to the public. The court adopted a narrow interpretation based on the analysis of the technical processes involved. It argued that the works recorded in the virtual video recording system had not been offered to the public out of Save.tv's sphere of access. They were recorded in the users' private storage spaces and, when they were within the sphere of access of Save.tv, they were not provided to the public but were retrieved by the individual users. The court was of the somewhat surprising view that it was irrelevant that the customers of Save.tv together might constitute a "public". Thus, it dismissed the claim that Save.tv. had infringed the right of making available to the public. At the same time, it found that Save.tv had infringed the broadcasters' rights since the broadcast signals had been transferred to the "virtual video recorders" of several clients who were not connected personally and therefore qualified as a "public."

The German report concludes the description of the case in this way: "the court held that the works were rendered accessible to the public in the sense of §§ 20, 87 I No. 1 Alt. 1 UrhG and thus the right of broadcasting had been infringed. Hence the 'narrower' interpretation of 'public' in § 19a UrhG was somehow 'compensated' by the broader interpretation of public in § 20 UrhG."[63]

On August 13, 2012, the Munich District Court I (*Landgericht (LG) München I*) in the *ProSiebenSat.v.Save.tv* case found also in favor of the plaintiff.[64] The court ruled that Save.tv had infringed the broadcaster's rights by using its programs to record and retransmit them without authorization. The ruling was in accordance with an earlier decision of the Higher Regional Court of Munich (*Oberlandesgericht (OLG) München*) which had found in favor of a broadcasting company in the *RTL Television GmbH v. Save.tv* case on November 18, 2010.[65] Previously, RTL had obtained a temporary injunction against Save.tv from the Munich District Court I for the infringement of the reproduction and retransmission rights under Articles 87 and 20 of the Copyright Act. The OLG upheld the decision with reference to the above-mentioned ruling of the BGH and prohibited Save.tv from allowing the use of RTL broadcasts in its virtual video recorder service.

Hungary. The Hungarian Copyright Experts Council, in its official opinion No. 31/2007, in the year following the BGH ruling adopted a similar legal position as the German courts on the issue of recording television programs on "virtual personal video recorders" offered by service providers – on storage spaces reserved on its servers – at their customers' digitally transmitted demand and then making the copies available to the customers for viewing the programs, again at their digitally transmitted demand.

Australia. The Australian "virtual video recorder" case had been launched by the National Rugby League (NRL), the Australian Football League (AFL) and Telstra Corporation

[61] German Report, p. 8.
[62] Referred to in the German report as OLG Dresden, MMR 2011, 413, 418.
[63] German Report, p. 32.
[64] LG München I, No. 7 O 26557/11 of August 13, 2012.
[65] OLG München No. 29 U 3792/10 of 18 November, 2010.

("Telstra") against Optus and its parent company Singtel Optus in respect of its Optus' "TV Now" service.

The subscription service allowed customers to record free-to-air television programs (including AFL and NRL games) on Optus' servers and play them back on any of four compatible devices: PCs, Apple devices, Android devices and 3G mobile devices. At issue were copies of free-to-air broadcasts of live and filmed AFL and NRL football games recorded by Optus customers using the TV Now service. It was alleged by NRL and AFL, as the owners of copyright in the broadcasts, and Telstra, as the exclusive licensee of internet and mobile telephony rights, that the TV Now service infringed their copyright.

First, on February 1, 2012, a single judge of the Federal Court found in favor of Optus[66] adopting the position that the acts of reproduction were performed by the customers of the service rather than by Optus, and that those acts were free as private copying for time-shifting purpose under section 111 of the Australian Copyright Act.

On April 27, 2012, the Full Federal Court reversed the decision[67] and found in favor of the appellants.

The Full Court held that Optus had made the copies, or Optus and the customers had made them together (without expressing definitive views on the two possibilities). It pointed out that the act "making" is a basic concept of the Copyright Act and that 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.

As regards section 111 of the Copyright Act concerning private copying, the court found that there is nothing in the language of the section which would suggest that it could be applied also for commercial reproduction at the request of members of the public.

FURTHER RETROSPECTIVE DISCOVERIES IN THE "CLOUD:" E-MAIL SERVICES, SOCIAL NETWORKS, UGC PLATFORMS

Cloudy hosting services and services with hosting in the "Cloud"

As analyzed above, the operation of "virtual video recorders" – although, at the beginning, this expression was not used for them – corresponds to the concept of cloud computing. The courts in the legal disputes concerning such services – although not necessarily in an optimal way – have dealt with certain issues that emerge also in the case of many other cloud-based systems, such as cyberlockers and cloud-based commercial services.

[66] [2012] FCA 34 (1 February 2012).
[67] [2012] FCAFC 59 (27 April 2012)

However, before we turn to the latter category of fully-fledged cloud services, let us review the copyright implications of some other "older" systems which, similarly to "virtual video recorders," began functioning before the conceptualization of the "Cloud." Among these "older" services, we may be found, for example, e-mail systems (such as Yahoo! Mail, Gmail, etc.) social networks (Facebook, Twitter, etc.) and "user-generated-content" (UGC) platforms (such as YouTube, Flickr, etc.).

These services are operated in what we call now the "Cloud," since the materials uploaded by their customers are stored on the providers' servers where they may be accessed from anywhere through internet connection. They differ from "virtual video recorders" – the other typical category of "pre-cloud-era" cloud-based services discussed above – in various aspects. "Virtual video recorders" serve basically for making copies of television programs and hosting them for subsequent retrieval. In the case e-mail services, social networks and UGC platforms, uploading works and then making them available to a narrower, broader or even an unlimited scope of people (qualifying already as members of the public) are normal functions. This is somewhat less typical in the case of net-based e-mail services; it is a more frequent phenomenon as regards social networks, and it is quite a fundamental function of UGC platforms.

Where a customer sends an e-mail to people who do not belong to the members of his or her family and his or her closest acquaintances (and thus who qualify as members of the public) and attaches to it a copy of a work, or does the same in the case of his or her Facebook "post" or his "tweet," it is an act of making available to the public. The same is true when someone uploads a work on the YouTube.

Liability for infringements

Direct (primary) and secondary liability. For the infringements of rights through such cloud-based systems, normally those customers have direct (primary) liability who upload and, thus, make available works to the public without authorization. In principle, it is possible to apply remedies and sanctions directly against them. However, in practice, this seems to be as difficult as in the case of p2p "file sharing" systems (about which very rich – and, from the viewpoint of owners of rights, not quite favorable – experience is available). The chance for stepping up against major or repeat infringers is much better if it takes place on the basis of the obligations of the operators of such systems – and of their secondary liability if they do not respect their obligations.

Secondary liability of cloud providers is a separate topic of this congress. This paper is mainly supposed to deal with the issue of how the WIPO "Internet Treaties" may be applied in the cloud environment. These Treaties – as the international copyright norms in general – do not address the question of secondary liability. The knowledge of a huge body of statutory and case law is needed for judging such issues appropriately; therefor, this is usually left to national legislation and jurisprudence.

Nevertheless, it is inevitable that this paper also review those cases where the issue of secondary liability has emerged, at least for two reasons. First, because secondary liability only applies where there is underlining direct liability (and in this respect, the applicability of the rights provided by the WIPO "Internet Treaties" is relevant). Second, because, as it may

be seen below in connection with certain court cases, there are borderline questions as to whether a cloud provider has only secondary liability or it is directly liable.

"Safe harbors" for hosting providers. The limits and conditions of liability of hosting providers – along with other internet service providers (or, as the EU rules refer to them, "information service providers") – for illegal acts, in general, or copyright infringements in particular, committed by their customers is regulated now in many countries. The rules in the US Copyright Act and the EU E-Commerce Directive[68] on the conditions of limitations of the liability of service providers ("safe harbors") are quite similar. It seems worthwhile reviewing these norms because the principles on which they are based seem to be valid also in other countries.

Section 512 of the US Copyright Act differentiates between four kinds of activities of service providers: (a) transitory digital network communications ("mere conduit" function), (b) system caching, (c) hosting information posted by users in their systems or networks; and (d) providing information location tools that may direct users to infringing material. Articles 12 to 15 of the EU Directive cover the first three categories, but not the last one. This means that the rules on possible "safe harbor" for hosting providers – which are the most relevant ones from the viewpoint of the topic of this paper – may be found in both sets of provisions[69] and they, as mentioned above, in substance are quite similar.

The US rules in section 512(c) may be summed up in this way. A service provider is not liable for monetary relief – but, in the cases determined in subsection (j), it is liable for injunctions – 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 it
- does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
- in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent;
- upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
- does not receive financial benefit directly attributable to the infringing activity in a case where has the right and ability to control such activity; and
- upon notification of claimed infringement – in accordance with the rules of a notice-and-take down procedure regulated in subsection (c)(2) and (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 EU rules are simpler. Under Article 14(1) of the EU Directive, where an information society service consists of storage of information provided by a recipient of the service, the EU Member States must ensure that the service provider is not liable for the information stored at the request of a recipient of the service, if the provider
- does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

[68] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
[69] Section 512(c) of the US Copyright Act and Article 14 of the EU Directive.

Under paragraph (2) of Article 14 of the Directive, these provisions do not apply when the recipient of a service is acting under the authority or the control of the provider. Paragraph (3) adds that the provisions of the article do not affect the possibility for a court or administrative authority, in accordance with the Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor affect the possibility for Member States of establishing procedures governing the removal or disabling of access to the information.

The most visible difference between the US and the EU regulations is that the EU Directive does not provide for a specific notice-and-take down system (but only refers to the possibility of apply such a system). This is partly due to the fact that the US norms only apply to copyright infringements, while the EU provisions have a "horizontal" application to cover all kinds of violations of law.[70] However, this is not an obstacle to Member States to introduce a notice-and-take down system specifically for copyright infringement. As the Hungarian report presented in response to the congress Questionnaire mentions it,[71] in Hungary, the Electronic Commerce Act[72] implementing the EU E-Commerce Directive provides for such a system, and it functions with success.[73]

Both legislations exempt service providers from general obligation to actively monitor their services in order to identify and eliminate infringing materials. In the EU Directive, Article 15(1) provides that "Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity." In the US Copyright Act, section 512(m) states that the "safe harbor" limitation on liability does not depend 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." However, it is important to note that, under sections 512(c)(1)(A) and 512(d)(1), service providers do have a duty to respond to "red flags" that make infringement apparent to a reasonable person. Where a website permits links to sites identified as "pirate" or "bootleg," some courts – such in the *Capitol Records, Inc. v. MP3tunes, LLC* case[74] – rightly enough, find that the service provider is no longer protected by the section 512 safe harbor provisions. (However, there are also cases where the courts may qualify even some deep-red flags as acceptably light pink. For example, in *Perfect 10, Inc. v. CCBill LLC* case, the court did not see any red flag popped up, although services were provided to such sources as "illegal.net" and "stolencelebritypics.com." The court tried to justify the decision – not in quite a persuasive

[70] While copyright infringements, in the overwhelming majority of cases, may be relatively easily identified, in the case of certain other violations of law – such as defamation, libel, instigating racist hatred, pornography, etc. – this is not the case.
[71] Hungarian Report, pp. 4-6.
[72] Act CVIII of 2001.
[73] As the Hungarian Report describes it, it is mainly ProArt – an anti-piracy alliance of Hungarian organizations representing owners of copyright and related rights – which delivers a number of notices. The statistical data received from ProArt on the last two years offer the following picture:
The total number of the notices sent in 2010 is 949.
The total number of removed cyberlocker links in 2010 is 156334.
The total number of the notices sent in 2011 is 766.
The total number of removed cyberlocker links in 2011 is 183859.
Providers do co-operate and fulfill their take-down obligations. No counter-notice has been presented.
[74] *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 643-44 (S.D.N.Y. 2011).

manner – by explaining that such terms are not necessarily a reference to illegal activity, since they may also be used "to increase appeal."[75]

Court cases – how much, and for what purposes, "safe harbors" should be safe?

Key "interoperable" cases in the US: YouTube, Veoh, YouTube, Veoh. The courts in the US and elsewhere have had to deal recently with the issues of the most typical group of the above-mentioned category of "retrospectively" discovered cloud-based systems; namely, with "user-generated-content" (UGC) platforms. They seem to deserve as detailed analysis as the *Cablevision* case in respect to "virtual video recorders."

YouTube (now owned by Google) is a well-known – possibly the most well-known – UGC platform. By now, its repertoire has become much broader and its copyright-related activities more diversified than before, and its readiness to cooperate with owners of copyright against infringements has improved in certain aspects. However, in the US, there is a lawsuit pending against it still from the older times when its activity was still more reduced to allow its customers to upload videos, to store them on its servers and then to make them available, in general, to any interested members of the public anywhere and anytime.

At first sight, the concept of "user-generated content" may seem to be unclear from the viewpoint of copyright and perhaps this expression has been coined on purpose to be like that. The reference to "UGC" – not only in journalistic language, but frequently also in legal discourse – may cover quite differing phenomena hopelessly mixed up together. If we remain with abbreviations and coin more, we can say that it may mean "UCWs" – user-created works – with which there is no copyright problem, of course, if their creators upload them and make them available to anyone they want. It may mean "UAWs" – user-adapted works – which may cover adaptations authorized by the owners of rights or by the law but may also consist of infringing misappropriations (with a lot of borderline issues which could be a juicy topic for a complete program of an ALAI congress; although some of them were already discussed at the ALAI Study Days held in Barcelona in 2006). And it may also mean "UUWs" – simply "user-used" works – in the case of which much depends on whether a user (meaning a user of the *platform' service*) becomes also the user of the *works* concerned by performing acts covered by copyright (in general, reproduction and making available to the public) with or without authorization by the owners of rights. (Experience shows that, of the latter two variants of "uses by users," the second one is quite typical.)

Viacom was certainly of this view when it launched a lawsuit against *YouTube* in the US. Due to YouTube's popularity and its outstanding position among UGC platforms, this suit has been followed with increased interest. It has produced some ups and downs from the viewpoint of both the plaintiff and the defendant and it is not completely settled yet. First, YouTube seemed to be the winner but some recent developments have been less favorable for the UGC giant. This seems to be the case, in particular, as regards another lawsuit in Germany between the authors' society *GEMA* and *YouTube* (see below).

[75] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007).

In the US *Viacom Intern., Inc. v. YouTube, Inc.*[76] case, Viacom claimed that the YouTube was both directly and secondarily liable for copyright infringement of a great number of works of Viacom which were posted on the platform's site, without authorization, by users between 2005 and 2008.[77] 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 into a format compatible with a multitude of platforms.

Before addressing other more substantive issues relating to the qualification of the various acts performed in the YouTube system, the court had to address the basic question of whether or not YouTube qualified for the status of hosting provider and, thus, for limitation of its liability under section 512(c) of the US Copyright Act for possible infringements committed by its customers. And this was the first issue in respect of which the mutual interaction between the YouTube and *Veoh* cases began.

The report of the US ALAI Group[78] prepared in response to the congress Questionnaire notes that, under section 512(c) of the US Copyright Act – provided that all the other conditions are met – online service providers are exempt from liability 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." As the response points out, a "conservative interpretation" (in view of the author of this paper, in fact, quite a reasonable, not unnecessarily extensive or restrictive interpretation) of this condition would have suggested that it applies exclusively to online *storage*. However, in *UMG Recordings, Inc. v. Veoh Networks, Inc.*, the District Court interpreted the expression "by reason of storage at the direction of a user" to include conduct consisting in facilitating access to user-stored copies.[79] According to the court's ruling, the acts of reproduction through the creation of differently-formatted or condensed videos, of performance when users stream the stored works to themselves, and of distribution of works when users access stored videos for downloading – all fall within the scope of activities covered by the exemption.[80]

In *Viacom v. YouTube,* Viacom claimed that 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). However, relying on the decision in the above-mentioned *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 that function "is closely related to, and follows from, the storage itself," and is "narrowly directed toward providing access to material stored at the direction of users."[81]

---

[76] 676 F.3d 19.

[77] During the time period covered by the suit, YouTube did not implement yet a filtering mechanism. In the meantime, it has done so.

[78] US Report, p. 23 and on.

[79] (Note in the US Report) UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081, 1088-89 (C.D. Cal. 2008).

[80] (Note in the US Report) *Id.* at 1087-88, 1092.

[81] (Note in the US Report) 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.).

Now that *Veoh* cases have been mentioned as regards the way it has influenced *Viacom*, let us review it briefly before reverting to Viacom.

The issues of Veoh's monitoring and takedown responsibilities were addressed by the Ninth Circuit in *UMG Recordings, Inc. v. Shelter Capital Partners LLC*.[82] 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 as in the case of YouTube. 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 the obligation under section 512(c) concerning takedown of infringing copies about which it receives notifications. In 2006, Veoh adopted a rudimentary filter system and upgraded it to an Audible Magic system the following year. Veoh argued that it attempted to filter out content that copyright holders had not authorized to appear on its system. Moreover, when content was taken down pursuant to a notification, Veoh used filtering technology to automatically disable access to identical videos and to block subsequently submitted duplicates.[83] Veoh also terminated 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, it should have sought out actual knowledge of other infringing videos and removed them. UMG also alleged that Veoh was aware of widespread infringement occurring on its system and, thus, it 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 the service could be used to post infringing material did not constitute knowledge sufficient to deny access to the section 512(c) safe harbor. According to the court, the Copyright Act places the burden of identifying infringements on the rightholders.[84] The court also rejected UMG's argument that Veoh had the right and ability to control infringing activity, pointing out that "right and ability to control" under § 512(c) requires control over infringing activity that the provider knows about.[85]

This ruling was followed in other cases. For example, in *Io Group, Inc., v. Veoh Networks, Inc.*, the court held that the activities stemming from Veoh's automated software were also covered by the "safe harbor" protection under section 512(c).[86] This was found in spite of the fact that Veoh's software, although automatically, processed the copies submitted by the customers and reconstructed them "in a user-friendly way." The court was of this view because "this [the software] is a means of facilitating user access to material on its website"[87]

[82] (Note in the US Report) 667 F.3d 1022.
[83] (Note in the US Report) *Id.* at 1028. (It is to be noted that this ruling corresponded to the "taken down and staying down" principle discussed below in connection with European cases.
[84] (Note in the US Report) *Id.* at 1038.
[85] (Note in the US Report) *Id*. at 1043.
[86] (Note in the US Report) Io Group, Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008).
[87] (Note in the US Report) *Id.*

Let us turn back to *Viacom v. YouTube* on which the Veoh ruling had an impact and to show how it has "reciprocated" in its interaction with Veoh.

Viacom alleged that YouTube's activities violated the company's exclusive rights of public performance, public display and reproduction. Specifically, Viacom alleged that YouTube was not eligible for the safe harbor protection 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 held – and the Court of Appeals affirmed – that the knowledge of such infringing activities had to be specific and the infringing copies identifiable. Then 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 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."[88]

As a consequence, Viacom was unsuccessful with its claim that YouTube had a duty to proactively identify and eliminate certain videos. 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 the case to the District Court on this issue.

Viacom also alleged that the District Court had erred in failing to rule in its favor despite evidence that YouTube was "willfully blind" to the infringing activity.[89] While the Court of Appeals held that the law does not provide for an affirmative duty to monitor a 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.

The Second Circuit 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.

The *Viacom v. YouTube* ruling also dealt with the scope of section 512 safe harbor protection. In that respect, the case has also been remanded to the District Court, which has not yet issued a final judgment at the time of the completion of this paper. If it finds that YouTube had awareness of or willfully blinded itself to specific infringements, YouTube will not qualify for safe harbor protection. (It is to be noted, however, that YouTube has significantly changed its service since the period complained of in the *Viacom* suit (for example, it applies filtering at least in certain cases).)

[88] (Note in the US Report) *Viacom*, 676 F.3d at 31.
[89] (Note in the US Report) *Viacom*, 676 F.3d at 35.

And this was the basis on which *YouTube* has had a consequence in the *UGC v. Veoh* suit. On June 7, 2012, the Ninth Circuit ordered a supplementary brief [90] for the potential taking into account of the ruling of the Second Circuit in YouTube. This may lead to a modified opinion of the Ninth Circuit along with a possible remand to the District Court as it was the case in YouTube.

Relevant CJEU rulings on service provider liability: from eBay through Scarlet to Netlog.
Recently, the Court of Justice of the European Union (CJEU) has adopted three preliminary rulings on the obligations of hosting service providers concerning intellectual property infringements committed by their customers. In principle, the objective of such rulings is to offer guidance how the already harmonized aspects of legal norms (the famous *acquis communautaire*) should be applied in appropriate and harmonized way. The special nature of the three rulings was that the tasks of harmonization also extended to the harmonization between a number of directives adopted in various fields on different legal issues others than those concerning intellectual property, such as electronic commerce, data protection, privacy and electronic communication. In addition, certain general human rights considerations have also been taken into account and the CJEU has also developed the doctrine of "freedom of conducting business" (and by this it might have wandered to quite a swampy terrain).

The first preliminary ruling – in *L'Oréal and others v. eBay and others*[91] (hereinafter eBay) – offered guidance which would have been suitable for judging the liability issues of internet service providers concerning intellectual property infringements in quite a well-balanced way. However, when the same kind of issues emerged in the over-hyped, over-politicized, over-ideologized, over-hystericalized and over-lobbied field of copyright in *SABAM v. Scarlet*[92] (hereinafter: Scarlet), the CJEU found itself in front of quite a complex task. The court, following the approach applied in the previous, similarly difficult *Promusicae v. Telefonica* case[93] – the focus of which was data protection – made great efforts to try to reach a balanced solution. However, its ruling was not favorable for copyright owners, since – as it has become so fashionable recently – it interpreted the task of balancing in a somewhat unilateral way; namely, as balancing just *against* copyright. Nevertheless, if eBay and Scarlet are considered together, it still may be said that the CJEU, at the crossroads of so many principles and rules, has made available a relatively reasonable virtual GPS programed to choose various possible further directions, including truly balanced ones where copyright owners could have received more than the kind invitation: "shut up!" (French translation: "*ta guele!*;" Spanish translation: "*¡callate, cierra la bocca!*"). But then the third preliminary ruling – in *SABAM v. Netlog*[94] (hereinafter: Netlog) – came where it seems the court had left home that GPS or had not switched it on, as a result of which it went in a dubious direction through *Scarlet* instead of revisiting *eBay* through which it would have been easier to find the right way. This kind of dis-harmonization of the CJEU practice appears to be an unfortunate (mis)step from the viewpoint of our topic since, by dealing with Netlog, the CJEU arrived in an area which, contrary to what had been the case in Scarlet, was already definitely "cloudy."

In *eBay*, the CJEU adopted a nuanced approach concerning the issue of liability of hosting service providers. The key statements of the ruling were as follows:

[90] Nos. 09-55902 and 09-56777.
[91] CJEU case C - 324/09 of July 14, 2011.
[92] CJEU case C - 70/10 of November 22, 2011.
[93] CJEU case C-275/06 of January 29, 2008.
[94] CJEU case C- 360 of February 16, 2012.

> [T]he Court has already stated that, *in order for an internet service 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…[95]
>
> *That 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*…[96]
>
> There, by contrast, *the operator has provided assistance which entails*, in particular, *optimising the presentation of the offers* for sale in question *or promoting those offers*, it *must be considered not to have taken a neutral position* between the customer-seller concerned and potential buyers *but to have played an active role of such a kind as to give it knowledge of, or control over, the data* relating to those offers for sale. *It cannot then rely*, in the case of those data, *on the exemption from liability* referred to in Article 14(1) of Directive 2000/31.[97]
>
> In view of the foregoing, the answer to the ninth question is that Article 14(1) of Directive 2000/31 must be interpreted as applying to the operator of an online marketplace where that operator has not played an active role allowing it to have knowledge or control of the data stored. The operator plays such a role when it provides assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting them.[98]
>
> Where the operator of the online marketplace has not played an active role within the meaning of the preceding paragraph and the service provided falls, as a consequence, within the scope of Article 14(1) of Directive 2000/31, the operator none the less cannot, in a case which may result in an order to pay damages, rely on the exemption from liability provided for in that provision if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously in accordance with Article 14(1)(b) of Directive 2000/31.[99]

Thus, the *eBay* court has differentiated between two situations: on the one hand, when the hosting provider plays an active role allowing it to have knowledge or control of the data stored (such a providing assistance, in particular by optimizing the presentation of certain contents or otherwise promoting them), and, on the other hand, where the provider does not have such a role. The provisions of the Directive on the limitation of the liability of service providers only apply in the latter case. This is in accordance with the agreed statement adopted concerning Article 8 of the WCT on the right of communication to the public (which, in the case of the WCT, also covers the acts of (interactive) making available to the public):

> It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention

It should be noted what kind of *a contrario* effect this agreed statement has. Namely, it has clarified that, *when a service provider goes beyond merely offering physical facilities, its activity may amount to communication (and, in case of interactivity, to making available to the public).* This is what was clearly and correctly stated in *eBay.*

[95] CJEU Case C324/09, point 112.
[96] *Id.*, point 113.
[97] *Id.*, point 116.
[98] *Id.*, point 123.
[99] *Id.*, point 124 (emphasis added).

When we turn to the *Scarlet* ruling, we have to emphasize that Scarlet is *not a hosting provider* (contrary to Netlog which is a hosting provider – and, as a matter fact, cloud provider). As it discussed below, this is relevant for considering whether or not it was appropriate for the *Netlog* court just to copy and paste the key elements in *Scarlet*.

Scarlet is a peer-to-peer service and it was qualified by the CJEU as *access provider* falling under Article 12 of the E-Commerce Directive basically with a *mere-conduit* function. The issue disputed in the case was the question of whether or not the national court might order Scarlet to apply a filtering system to prevent the infringements of copyright in the musical works administered by the Belgian society of authors SABAM. The Belgian court, in its referral for preliminary ruling, specified what kind of filtering system would have been involved:

> whether Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction imposed on an ISP to introduce a system for filtering
> - all electronic communications passing via its services, in particular those involving the use of peer-to-peer software;
> - which applies indiscriminately to all its customers;
> - as a preventive measure;
> - exclusively at its expense; and
> - for an unlimited period.[100]

The basic elements of the court's ruling may be found in the following points:

> 48.[S]uch an injunction *would result in a 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*, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, which requires that *measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly*.
>
> 49. In those circumstances, it must be held that the injunction to install the contested filtering system is to be regarded as not respecting the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual-property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business enjoyed by operators such as ISPs.
>
> 50. Moreover, the effects of that injunction would not be limited to the ISP concerned, as *the contested 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*, which are rights safeguarded by Articles 8 and 11 of the Charter [on human rights] respectively.
>
> 51. It is common ground, first, that the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be precisely identified.
>
> 52. Secondly, that injunction *could potentially undermine freedom of information* since that system might not distinguish adequately between unlawful content and lawful content, with the

[100] CJEU case C-70/10, point 29.

result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. Moreover, in some Member States certain works fall within the public domain or can be posted online free of charge by the authors concerned.

53. Consequently, it must be held that, in adopting the injunction requiring the ISP to install the contested filtering system, *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 other.

54. In the light of the foregoing, the answer to the questions submitted is that Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against an ISP which requires it to install the contested filtering system.

The court seems to have reached these findings quite lightly and, as a result, it has not succeeded in fulfilling its objective to strike a fair balance. The ruling appears to have been influenced by some fashionable anti-copyright slogans and become unbalanced to the detriment of copyright owners.

The CJEU has construed a strong "freedom of conducting business." However, it did not pay attention to the fact that the business the freedom of which it intended to protect was based, to a great extent, on (i) illegal making available of works by a huge number of customers of the "business," (ii) increasing by this the number of visitors of the website, and, (iii) as a result of this sort of popularity, obtaining income from advertisers. The court should have considered how strong or weak protection the freedom of such a "business" may deserve in view of its detrimental impact on the rights and interests of those whose creations and productions are used illegally and without which the "business" could not have a chance to succeed.

The court ruled that the proposed filtering system was too complicated and too costly – without any real analysis or calculation as to why it was the case. Before reaching such a finding so lightly, it should have considered some weighty questions, such as these: What about possible filtering systems that would be simpler and less costly (which, with the development of digital technology, might quite realistically appear) or that is not "permanent"? In contrast with the one suggested by SABAM, could such filtering systems be imposed? On the basis of the *a contrario* principle, an affirmative answer seems to be justified to this question. Why did not the CJEU try to offer some guidance in this respect? If it had done, we might not have the impression that the ruling is somewhat biased against the rights and legitimate interests of copyright owners.

Probably, the court did not intend to join the defendant in pretending blindness of the fact that a huge part of its business was based on massive illegal making available of works to the public. Could not then be expected from the court to state that not only the intellectual property rights of copyright owners cannot be construed as unlimited but that this principle is, at least, as much applicable concerning the "freedom of conducting business" by indirectly gaining income from the infringements of those rights? And as a consequence of such a logical finding, would not it have been justified to consider to what extent the ISP might have to bear the cost of a reasonable filtering system from that income?

The CJEU stated that the application of the filtering system in question "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." This sweeping statement is the most poorly substantiated element of the ruling. In fact, it is not substantiated at all; it is not supported by any analysis and justification. If the court had tried to offer some, it would have had to answer some further inevitable questions as a result of which it might have turned out quite easily that all to which it referred was not much more than a collection of slogans lent from anti-copyright activists and lobbyist of online intermediaries (slogans that could hardly stand any serious scrutiny). Why would a filtering system violate the protection of customers' personal data if it only consisted in the mere identification of illegal copies and their removal? In particular, why would it be so if an automatic system were involved and it functioned only in the relationship between the ISPs and their customers (where, otherwise, the online intermediaries do know not only some basic data of their customers but nearly everything about them and use those data aggressively for commercial purposes). The apparent position of the court according to which free unauthorized making available of, for example, freshly released films to the internet population is a matter of freedom of receiving and imparting information – with all due respect to the legal status of the court (but not to this aspect of the ruling), is superficial and erroneous. Such a ruling has nothing to do with balancing of interests in and around copyright.

The CJEU has presented only one concrete argument in connection with the alleged danger for freedom of expression. It has referred to the abstract possibility that the filtering system could also lead to the blocking of lawful communications. As it can be seen above, the court argues in this way: "Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. Moreover, in some Member States certain works fall within the public domain or can be posted online free of charge by the authors concerned." It seems easy to prove how huge exaggerations this unsubstantiated statement contains and how much it is badly founded. It is sufficient to refer to the successful operation of the filtering system applied, for example, by YouTube in accordance with the cross-industry agreement published on www.ugcprinciples.com as mentioned below. It is still a major understatement if we say that, in the extremely overwhelming majority of cases, the "matches" found by the filter are unequivocally infringing copies. Furthermore, the same UGC principles take into account, and take care of, the exceptional situations which form only a microscopic tiny fraction of the enormous number of cases involved.

In this case, the CJEU, in spite of its presumable good intentions, has not established an appropriate balance and has not adopted a ruling which could be characterized as being in due accordance with the *acquis communautaire*. However, the court has not fulfilled another important task. Namely, it has just listed and quoted the norms of the relevant EU directives, but has not offered a real legal analysis thereof. There is no answer in the ruling to the following quite important 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 the prevention of infringements*? How filtering to prevent making available to the public of infringing copies 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 copies in an online system other than filtering? What would be the meaning and value of this recital if,

although orders to prevent online infringements (rather than only acting when the infringing content has become available to the internet population) are possible, their only effective application would not be allowed? The effect of the CJEU's ruling seems to be just something like the latter case.

What does the prohibition of *general* obligation to monitor 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.)

In the *Netlog* case, the CJEU would have had the opportunity to choose an appropriate direction as indicated in *eBay*. This, however, did not happen.

As described in the ruling,[101] Netlog runs an online social networking platform where every person who registers acquires a "profile" which the user can complete himself and which becomes available globally. The most important function of the platform, which is used by tens of millions of customers is to build "virtual communities" through which they can communicate with each other. Thus, Netlog is somewhat similar to Facebook, the well-known social network. SABAM claimed that Netlog's social network also offers its customers the opportunity of using, by means of their profile, musical and audio-visual works in SABAM's repertoire, making those works available to the public in such a way that other users of that network can have access to them without SABAM's consent, and without any fee.

Since *the liability of a hosting provider* (a "traditional" cloud provider) *was involved*, the consideration of the *eBay* ruling as a precedent would have been logical and necessary. However, the court seems to have neglected this. It has automatically applied the findings in *Scarlet*. It did has not taken into account that, while Scarlet's activities were fallen under Article 12 of the E-Commerce Directive, Netlog was a hosting provider and, therefore, Article 14 of the Directive was applicable with stricter rules on the conditions of limitation of liability than under Article 12.

In *Netlog*, the CJEU has simply repeated, in a copy-and-paste verbatim manner, the above-mentioned statements of the Scarlet ruling concerning the "freedom of conducting business" and the alleged dangers for the protection of personal data, freedom of speech, and freedom of information. Similarly as in *Scarlet*, it has not offered any analysis on what the prohibition of general obligation of monitoring and the permission of obligating ISPs to perform monitoring in specific cases mean and what criteria may be applied concerning filtering systems in this respect. And it has not considered at all the applicability of the useful and correct principles laid down in *eBay* concerning the liability of service providers which *provide assistance entailing optimization of the presentation of the "contents" and/or promotion of their distribution.* If it had taken those principles into account, it might have judged Netlog's status and liability in a different way.

[101] See note 92.

United Kingdom: the "authorization" doctrine ready to be applied also for the "Cloud." The report of the UK ALAI group prepared in response to the congress Questionnaire notes that there has not been yet express reference in case law concerning cloud-based services, but that there have been rulings concerning the liability of Internet service providers for "authorizing" restricted acts (a special British form of secondary liability) which could be relevant in this field too. It is expected that these judgments will be applied to cloud services *mutatis mutandis*.

The report refers in particular to *Dramatico et alia v BSkyB et alia*[102] where the court has applied the definition of "authorization" relying on factors identified in the previous judgment in *20C Fox v Newzbin*[103]:

- the relationship between the alleged authoriser and the primary infringer,
- whether the equipment/ means supplied constitute the means used to infringe,
- whether it will be used to infringe,
- the degree of control of the alleged authorizer,
- whether he is taking any steps to prevent infringement.

The report refers to Judge Arnold's ruling who held that *the operators of the Pirate Bay* (which, as the report notes, *could be described as a service similar to a cloud service for the purposes of copyright*[104]) *authorized the infringing activities of its users* (both by copying or communicating to the public) and that their activities went *beyond merely enabling or assisting infringements*. In applying the factors established in the *Newzbin* case, according to the report, he found as regards the Pirate Bay as follows:

> Regarding the relationship between the alleged authoriser and the primary infringers, he held that the features offered by the alleged authoriser were plainly designed to provide users with the easiest and most comprehensive service possible, i.e. to promote the download of torrent files by its users. *It is not merely a passive repository of files but moreover goes to great length to facilitate and promote the download of files* by its users
> - the means supplied, i.e. the indexed torrent files constitute exactly the means necessary to infringe,
> - copyright infringement is not only inevitable but is also the main objective of the service,
> - the website operator has the required degree of control; the website states that torrents can and will be removed under certain condition,
> - the website operator is not taking any steps to prevent infringement; moreover they are expressly encouraging infringement.[105]

Germany: "umbrella solution" against dark clouds (as a minimum, what has been taken down should stay down). As regards UGC-related court cases in Germany, due to the great popularity of YouTube, the *GEMA v. YouTube* case attracted the biggest attention which is discussed below. However, it should be noted that German courts have dealt with different kinds of UGC platforms and adopted quite nuanced decisions the spectrum of which is quite broad from direct liability through "disturber" liability to the application a safe harbor rules.

The *YouTub*e case may be found somewhere in the middle of the quite colorful spectrum of cases addressing the issues of direct liability through secondary liability to no liability. Close

[102] UK Report, pt. 11 (ruling adopted in 2012).
[103] *Id.* (ruling adopted in 2010).
[104] *Id.*
[105] *Id., pt. 12.*

to the direct-liability end of the spectrum, there may be found a case – *Marions Kochbuch* – which reached the level of the Federal Court of Justice (*BGH*) which it made it possible for the court to offer guidance on the criteria of liability of UGC platforms. The BGH held that *the UGC web page www.Chefkoch.de had infringed the right of making available to the public* in photographs uploaded in the system.

The report of the German ALAI Group prepared in response to the congress Questionnaire describes the underlining facts as follows:

> The provider enabled third parties to upload recipes and photographs of dishes. Before unlocking this content to the internet community it controlled the content as to its completeness and correctness and whether the photographs seemed to be professionally made. The recipes formed the core content of the platform. On printed versions of the recipes the text and the pictures appeared under a big badge/emblem of Chefkoch. In its General Terms and Conditions the provider demanded the consent of the user to agree to duplications and transfer of their content. Chefkoch offered the recipes to third parties for commercial use.[106]

In view of these facts, the BGH found[107] that 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 the works in the form of making them available to the public*.

Let us turn now to *GEMA v. YouTube.*

In 2007, GEMA and YouTube concluded an interim licensing agreement which expired in March 2009 and has not been renewed. Since then, GEMA and YouTube had been negotiating on a new licensing agreement. However, in May 2010, GEMA abandoned the unsuccessful negotiations and launched a lawsuit against YouTube.

The Hamburg Regional Court (*LG Hamburg*) ruled on April 20, 2012[108] that *YouTube is liable for infringing music videos uploaded by its customers where it does not fulfill certain duties.* When notified of an infringement, it has the *obligation not only to remove or block access to infringing copies of videos without delay but also to take measures to prevent further infringements in respect of the same videos.* (This duty, however, does not extend to those videos which had been uploaded to the platform before the ruling.)

In the lawsuit, YouTube presented the well-rehearsed arguments of online intermediaries in trying to prove absence of liability: first, that it only provided platform for its customers and had neither made copies of the videos concerned nor uploaded them; and, second, it had taken all reasonable measures to prevent infringements. The court was not impressed by these arguments. Although it held that YouTube was not directly liable for having committed infringements (in the form of "*Täterhaftung*") it did have "disturber" liability ("*Störerhaftung*") by to the infringing acts. The court found that, as a "disturber," YouTube did not fulfill its duty to stop infringements by blocking access to the videos without delay after the plaintiff had notified it (as an extreme example, in certain cases, YouTube only blocked access to the videos *seven months after GEMA's warning*).

[106] German Report, p. 7.
[107] BGH No. I ZR 166/07 of November 12, 2009.
[108] LG Hamburg No. 310 O 461/10 of April 20, 2012.

The court has stated that no disproportionate duties may be imposed on YouTube. Nevertheless, it has held that *it is a reasonably proportionate obligation to prevent future illegal uploads of the same musical works on the same recordings by using filtering software*. It has pointed out that such software was already available to the defendant developed itself (the Content-ID software). The court has also clarified that YouTube *should use the software itself and could not leave this to its users* and, furthermore, that it should additionally introduce a word filter for the same purpose.[109]

Netherlands: mixed rulings on the right of making available; specific monitoring obligations allowed. The Dutch ALAI group, in response to the congress Questionnaire,[110] reports on what it considers a "landmark" ruling in the country's case law. In the lawsuit between the *Scientology Church* and the hosting provider *XS4ALL* (it is worthwhile trying to pronounce the quite telling abbreviation: "excess for all," "access for all" or "excess in access for all"?), The Hague Court has held that such a hosting provider does not perform acts of making available to the public because it merely provides technical facilities for enabling communication to the public by others.[111] The court has referred to the agreed statement adopted concerning Article 8 of the WCT, which – as quoted above – clarifies that mere provision of facilities for communication does not qualify as an act of communication (including (interactive) making available) to the public. The same line of reasoning has been adopted with regard to file-sharing websites that do not themselves store content on their own servers (but only direct consumers towards websites that offer (infringing) content).[112] In the latter case, the court has been of the opinion that, technically, the intermediary cannot perform an act of making available because the works concerned are not stored on its own servers.[113]

The Dutch group reports on a ruling of the District Court of Amsterdam. However, before that, it draws attention on certain recent judgments of the CJEU, in which it, *inter alia*, had to interpret the concept of communication to the public (including broadcasting and making available to the public) under Article 3 of the Information Society (Copyright) Directive[114] (which implements Article 8 of the WCT).[115] The report notes that the CJEU takes a more "functional" approach to this concept. It has held that, in order to establish whether a user is

[109] This was found necessary because YouTube's Content-ID software was only able to identify the same music recording but would not detect other illegal recordings of the same work.
[110] Dutch Report, p. 4 and on.
[111] (Note in the Dutch Report) Court The Hague 9 June 1999, BIE 1999/489 (*Scientology/XS4ALL*).
[112] (Note in the Dutch Report) District Court The Hague 22 March 2011, IER 2011/44 (*Premier League/MyP2P*), District Court Haarlem 11 February 2011, IEPT 20110209 (*Brein/FTD*); Court of Appeal The Hague 15 November 2010, LJN BO3980 (*FTD/Eyeworks*); District Court Amsterdam 16 June 2010, IEF 8997 (*Brein/The Pirate Bay*); Court of Appeals Amsterdam 16 March 2010, IER 2010/78 (*Shareconnector*); Court of Appeals Den Bosch 12 January 2010, IER 2010/34 (*CMore/MyP2P*); District Court Utrecht 26 August 2009, B9 8127 (*Brein/Mininova*); District Court Den Bosch 8 July 2008, IEF 6425 (*Brein/Euroaccess*); Court of Appeals Amsterdam 3 July 2008, IEF 6399 (*Leaseweb/Brein*); District Court The Hague 5 January 2007, IEF 3191(*Brein/KPN*); District Court Amsterdam 24 August 2006, IEF 2531 (*Brein/UPC*); Court of Appeals Amsterdam 15 June 2006, IEF 2208 (*Brein/Technodesign*).
[113] (Note in the Dutch Report) Hosting providers are thus able to benefit from this technical approach in two ways: i) in case content is placed on their server it can be argued that the provider is merely providing technical facilities, ii) in case it is not placed on the own server it can be argued that it is merely providing access to a third party who is making available.
[114] (Note in the Dutch Report) Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.
[115] (Note in the Dutch Report) ECJ 4 October 2011, IER 2012/3 (*Premier League*); ECJ 13 October 2011, C-431/09 (*Airfield*); ECJ 24 November 2011, IER 2012/28 (*Circus Globus*); ECJ 15 March 2012, IER 2012/28 (*SCF/Del Corso*); ECJ 15 March 2012, IER 2012/28 (*PPL/Ireland*).

making a communication to the public, a judge must first consider whether or not the user "intervenes" in full knowledge of the consequences of its action to give access to a broadcast containing the protected work to its customers.[116] Furthermore, the court has held that it is relevant whether the intervention results in reaching a "new public." Finally, the Court has also noted that it is also a relevant factor to consider whether or not a communication is made for profit-making purposes.[117]

The Dutch report points out that, in its ruling of September 12, 2012, the District Court of Amsterdam applied the CJEU's guidance, in the internet environment, concerning the criteria of "intervention," "new public" and "profit-making."[118] The court held that the placing of link to a website with leaked pictures of a well-known person constituted an act of making available to the public (even though the content itself was not placed on the server of the defendant's blog). It was not for the first time that Dutch courts applied the "functional" approach. In 2010, the District Court of The Hague[119] also held that a Usenet forum with information regarding Usenet-files on different servers constituted making available to the public. Although that decision was overturned by the Court of Appeals of The Hague,[120] the District Court of Amsterdam held again that Usenet service provider News Service Europe had infringed copyright.[121]

The Dutch group has added the following comments to these cases which deserve due attention:

> *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). A more functional approach on the other hand seems to provide for less legal security.[122]

The report also refers to the way the principles of the CJEU's *L'Oreal – eBay* judgment were applied in the Netherlands by the Court of Appeals of Leeuwarden. The reason for which it was relevant was that, although the parties were a chair manufacturer (Stokke) and an online "market place" (Marktplaats), one of the issues to be dealt with was the status of hosting providers. The Court has found that Marktplaats can invoke the application of safe harbor norms as a hosting provider in accordance with the CJEU judgment since it took a neutral position between the persons who placed the content on its platform and the customers to whom the content was made available (and has clarified it could not have done so if it had played an active role between those parties). The Court has held that Marktplaats was neutral,

[116] (Note in the Dutch Report) ECJ 7 December 2006, Case C-306/05 (*Rafael Hoteles), §*42; ECJ 4 October 2011, IER 2012/3 (*Premier League*), §195
[117] (Note in the Dutch Report) ECJ 4 October 2011, IER 2012/3 (*Premier League*), §204
[118] (Note in the Dutch Report) District Court Amsterdam 12 September 2012, LJN:BX704 (*Playboy/Geen Stijl*).
[119] (Note in the Dutch Report) District Court The Hague 2 June 2010, IER 2010/20 (*FTD/Eyeworks*).
[120] (Note in the Dutch Report) Court of Appeals The Hague 15 November 2010, LJN BO3980 (*FTD/Eyeworks*).
[121] (Note in the Dutch Report) District Court Amsterdam 28 September 2011 (*BREIN/News Service Europe*).
[122] Dutch Report, p. 5 (emphasis added).

because it had no involvement with the actual content of the advertisements in question placed on its platform, and because it treated all different users who placed content online equally. The fact that Marktplaats was heavily advertising its platform – according to the Court of Appeals – did not mean that Marktplaats had an active role.

However, the reason for which it is particularly worthwhile referring to the Marktplaats case is the interpretation of the "no general monitoring" principle which, in substance, is the same as or at least very similar to what we have seen in the case of the German case law. In this respect, the Dutch report reads as follows:

> In the SABAM case, the ECJ stated that the Internet service provider cannot be obliged to install *a general* filtering system, covering all its users, in order to prevent the unlawful use of musical works, as well as paying for it. In the case between Stokke and Marktplaats the Court of Appeal in Leeuwarden [held] that *Article 15 E-Commerce Directive does not stand in the way of imposing obligations to monitor for infringements in specific advertisements*, 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). The Court clarifies however that injunctions have to remain reasonable and proportionate and are not allowed to become unreasonably expensive or result in obstructions of legitimate trade.[123]

France: taken down but not staying down; after nice white clouds, cold shower into the rightholders' necks. For a while, it seemed that French jurisprudence would go in the same direction as in Germany (as indicated, in particular, in the ruling of the Hamburg Regional Court discussed above). Recently, however, with two rulings of the Supreme Court, the so far friendly white clouds have turned menacingly dark.

In French case law, first, it was found that UGC websites as hosting providers have specific monitoring obligations. In *André Rau v. Google and Aufeminin.com*[124], *Google Inc. v. BAC Films et al.*[125], *Zadig Productions v. Google Video*[126] and *Flach film v. Google France,*[127] the courts held that, although Google was eligible for limitation of its liability as hosting provider, it was nonetheless subject to the duty *not only to block access to infringing copies of a work when it was notified but also to prevent the uploading of infringing copies of the same works by the same or different customers.*[128]

In contrast, in *Christian C., Nord Ouest Production v. DailyMotion,*[129] the French Supreme Court (*Cour de cassation*) found 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 such an automatic way in the DailyMotion case, the *Tribunal de Grand Instance* went in the same direction in its judgment in *TF et al v. DailyMotion*[130] on September 13, 2012 (the suit was launched still in 2007).

[123] *Id,* pp. 13-14 (emphasis added.)
[124] C.A. Paris, Febuary. 4, 2011, André Rau v. Google and Aufeminin.com.
[125] C.A. Paris, January 14, 2011, Google Inc. v. Bac Films, The Factory et al.
[126] TGI Paris, October 19, 2007, Zadig Production v. Google Inc, Afa.
[127] Comm. Court of Paris, February, 20, 2008, Flach Film v. Google France, Google Inc.
[128] Also. TGI Paris October 9, 2009 H & K SALR and M/A v. Google France.
[129] Arrêt n° 165 du 17 février 2011 (09-67.896)
[130] Tribunal de grande instance de Paris 3ème chambre, 4ème section; jugement du 13 septembre 2012.

Nevertheless, this does not mean that the ruling could have served as a basis for a beatification process of *DailyMotion*. It is true that it was recognized as a hosting provider rather than an „editor" (the court held that certain functions of the system such as *a posteriori* moderation and the application of a search engine were not sufficient reasons to change this finding, but it obligated DailyMotion to remove the terms "TF1" and "LCI" from the list of suggested key words). Nevertheless, at least, in respect of certain works, the court found that DailyMotion was secondarily liable for infringements because it had not blocked access to them promptly enough after having been notified (according to the court, four days were too had failed to take adequate measures against repeat infringers.

In balance, this judgment was not favorable for TF1 and the other owners of rights involved. Still it was a respectable decision, in particular if we take into account that the court felt being obligated to apply the principles of the not quite fortunate *Netlog* ruling.

This can hardly be said about the judgment of the Paris High Court in the *TF1 v. YouTube* case.[131] The court applied the recent rulings of the CJEU and the French Supreme Court. It held that YouTube was a hosting provider and, thus, it only had the duty to remove infringing copies of the same works when it was notified again and again. After having stated this principle, the court reached quite a weird conclusion: although it did agree with TF1 that the perceived five-day delay in removing the infringing materials after notification was unreasonably long, it held that YouTube still was not liability because, in its view, the conditions of Section L.216-1 of the Intellectual Property Code were not fulfilled taking into account that the users had free access to the service. The author of this paper does agree with the remarks made in the FrenchKat blog one day after the ruling:

> With all due respect to the Court, this last conclusion seems erroneous. Leaving aside the question of whether the mere fact that the removal delay was unreasonable is sufficient to incur liability, Section L.216-1 IPC clearly contemplates an infringement where programs (as broadcast) are telecast ("*télédiffusion*" in French) OR communicated to the public in a place open to the public in exchange for an entrance fee. In other words, while the right of communication to the public associated with this related right is narrower than the corresponding right under copyright, the difference is only relevant in cases of communication to the public OTHER THAN telecasts. Given the broad definition of telecasts in the IPC (Section L.122-2), it is clear that YouTube was telecasting the programs and therefore infringing the Section L.216-1 related right, irrespective of the issue of free or paid access to the site.[132]

However, the real cold shower into the rightholders' necks came from two parallel rulings of the French Supreme Court which applied the Netlog principles quite generously in favor of

[131] TGI, No. RG : 10/11205 of May 29, 2012.

[132] Published on the FrechKat blog on May 30, 2012. The court must have been in very bad form the previous day, since the blog, rightly enough, noted also some other serious errors:

> "Beyond the error referred to above, the Court makes a rather odd comment about TF1 being unable to invoke both its Section L.216-1 related right and copyright simultaneously. The Section L.216-1 related right protects the broadcaster's programs as embodied in the signal that is broadcast whereas copyright protects the underlying work. Contrary to the Court's assertion, there is no legal principle that would prevent a party from invoking both grounds simultaneously; the two rights are independent of one another and protect different subject-matter (the programs in the signal in one case and the work in the other). As regards the Court's analysis of standing under copyright, it is striking that it makes no reference to the longstanding judge-made rule that use of a work in the absence of adverse claims by the natural person authors crates a *presumption* of copyright ownership vis-à-vis third-parties accused of infringement (in fact the Court actually expressly cites Section L.331-1, paragraph 3 IPC in this context, a provision which deals solely with related rights)."

the giant UGC platform as possible. The downward eBay-Scarlet-Netlog-DailyMotion spiral seems to have reached the bottom from the viewpoint of owners of copyright. On July 12, 2012, the Supreme Court adopted rulings in the *André Rau v. Google and Aufeminin.com*[133] and the *Google Inc. v. BAC Films et al*[134] cases which reduced the obligation of the UGC-platform-type hosting providers to block access to infringing materials when they receive notice, without any duty to take measures to prevent uploading the same infringing materials by the same customer or by other customers.

The reasons for the court's judgment have been summed up in this way:

> When it [Court of Appeal] ruled in this way, obligating the society Google to prevent any uploading of infringing videos, even if where it is not alerted by another regular notice required in order that it may have effective knowledge about their illegal character and location and act promptly to remove it or make access to it impossible, submitted it, beyond the only faculty of ordering a measure appropriate to prevent or eliminate the damage linked to the actual content of the site in question, also to a general obligation to monitor the images stored and to seek those which are illegally uploaded, and prescribed, in a manner disproportionate regarding the objective to achieve, the application of a blocking system without any limit in time, the Court of Appeal has violated the above-mentioned provisions [the relevant EU and French norms reviewed by the Supreme Court].*[135]*

With due respect to its status, the French Supreme Court seems to have applied the CJEU's controversial *Netlog* ruling in too easy-going manner. As discussed above, the Netlog court did not to offer sufficient reasons for its findings concerning the key issues of the case, including the question of why it applied in a copy-and-paste manner the findings in Scarlet (in spite of the fact that, while Scarlet was a peer-to-peer system, Netlog was a cloud-based hosting service). The French Supreme Court, however, 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 prescribed by the lower courts. It has not offered any real explication why this obligation would be disproportionate. And it did not make any attempt to offer guidance on how the alleged disproportionality might be eliminated in order that a balanced solution might be applied; for example, how the only concretely identified aspect of disproportionality – the unlimited nature of the "notice and stay down" obligation – could be eliminated.

It is submitted that the model that the Supreme Court has intended to offer as a proportionate solution – namely to limit the intermediaries' obligations, at maximum, to a notice-and-take down system (which was considered as a means of creating an appropriate balance in the 1996-2001 period) – is not a proportionate one in 2012 in view of the substantial advancements in filtering and blocking technology (which now may be applied in a way that it would not endanger the privacy interests of customers of services).

---

[133] CCass, 12 juillet 2012, André Rau c/ Google & AuFeminin.com.

[134] CCass, 12 juillet 2012, BAC films c/ Google France.

[135] The original French text reads as follows: *„Attendu qu'en se prononçant ainsi, quand la prévention imposée aux sociétés Google pour empêcher toute nouvelle mise en ligne des vidéos contrefaisantes, sans même qu'elles en aient été avisées par une autre notification régulière pourtant requise pour qu'elles aient effectivement connaissance de son caractère illicite et de sa localisation et soient alors tenues d'agir promptement pour la retirer ou en rendre l'accès impossible, aboutit à les soumettre, au-delà de la seule faculté d'ordonner une mesure propre à prévenir ou à faire cesser le dommage lié au contenu actuel du site en cause, à une obligation générale de surveillance des images qu'elles stockent et de recherche des mises en ligne illicites et à leur prescrire, de manière disproportionnée par rapport au but poursuivi, la mise en place d'un dispositif de blocage sans limitation dans le temps, la cour d'appel a violé les dispositions susvisées."*

The contractual schemes applied by certain intermediaries – including in particular by YouTube itself – do show and prove the practical availability of such desirable solutions. They also may offer helpful suggestions for those courts which are ready to devote time and energy to outline a truly proportionate legal framework. In this way, the only concrete aspect of disproportionality identified by the French Supreme Court – namely, the unlimited nature of a possible "notice and stay down" obligation – could also be eliminated. The author of this paper refers by this to the "UGC principles" worked out and applied in practice by major intermediaries (including Google's YouTube) and producers (in particular film producers).[136]

Italy: no liability exemption for hosting providers playing active role. The report prepared by the Italian ALAI Group in response to the congress Questionnaire notes that, in accordance with the EU E-Commerce Directive and the Italian Decree 70/2003, cloud service providers are qualified, in general, as hosting providers. Concerning liability exemptions granted to such providers, the Italian courts have adopted a nuanced approach based on case-by-case evaluation.

The report points out that, although Italian case law does not cover specifically cloud services as such, the rulings concerning hosting providers may be relevant. The rulings differentiate between passive and active hosting activities and the courts tend to interpret the applicability of exemptions from liability restrictively where the activity is not deemed to be merely passive.

The report mentions two cases on the status of hosting services. In the ruling in *RTI-Mediaset v. YouTube*, the Tribunal of Rome found the liability of YouTube as hosting provider and its duty to remove the materials illegally uploaded upon notice. In the *RTI v. IOL* case, the decision of June 7, 2011, 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 according to whether an "active hosting" or "passive hosting" is involved. In the given case, active hosting was evidenced by the insertion of advertisements to accompany UGC videos and content indexing facilitating users' searches.

Japan: the country of rising sun and of cautious hope for owners of rights. The Japanese ALAI Group in its response to the congress Questionnaire,[137] reports on the High Court's ruling in the *TV Break* case. The court had to judge whether an operator of a video file-sharing site was liable for the unauthorized uploading of TV programs by its customers. The High Court found that the service provider was liable for unauthorized copying of the programs on its server and their subsequent transmission to its customers. The reasons for the ruling were that (i) the provider operated and controlled the site, (ii) the profit derived from the activity was obtained 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 service provider performed the infringing acts (it was a "sender" under e-commerce legislation (see below)), and therefore, the limitation of the liability of providers was not applicable in its favor.

The report states that there is no statutory provision or Supreme Court ruling specifically on cloud services. The Copyright Act of Japan does not have an explicit provision on secondary

[136] See www.ugcprinciples.com.
[137] Japanese report, p. 10 and on.

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.

In this connection, the Japanese report also outlines the provisions on the liability of service providers. In Japan, the "safe harbor" provisions corresponding to those in the US Copyright Act and EU E-Commerce Directive may be found in the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders. According to the Act, a provider is not liable to damages for distribution of infringing materials through its online service, except for the case where (i) a preventive measure is technically possible to avoid transmission of infringing content, (ii) (a) the provider is aware of the infringement, or (b) is aware of circumstances serving a reasonable ground to have knowledge of the infringement. However, if the provider is the "sender" of the infringing material, as found in the TV-Break case, the limitation of liability does not apply.

"CLOUD-NATIVE" SERVICES: CYBERLOCKERS

Cyberlocker cases in the US

The response of the US ALAI Group to the congress Questionnaire, after reporting on the Cablevision case, continues as follows: "Not surprisingly, given the decreasing cost of digital storage, *Cablevision* has spawned other business models built on automated copying and individualized transmissions."[138]

This "spawning" of business models as an impact of *Cablevison* has led to fully-fledged cloud services too, such as cyberlockers.

The response of the US ALAI Group reports on the *Capitol Records, Inc. v. MP3tunes, LLC*[139] (hereinafter: MP3tunes) case where the Southern District of New York dealt with the issues of liability of a service provider which, *inter alia*, acted as a cyberlocker operator (and thus as a cloud service provider). MP3Tunes sold music in mp3 format and also had a component that allowed users to store music in personal online "lockers" reserved on the provider's servers (that is in the "Cloud"). The system allowed playing the uploaded songs – in principle, by the users concerned – through any internet-abled device. In addition, 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 asked the customer if he or she wanted to have the song downloaded to his MP3tunes.com "locker."

EMI claimed that MP3tunes.com was not eligible for the section 512(c) safe harbor as hosting provider 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 found that the ISP responsibly implemented its repeat-infringer policy, terminating accounts where necessary, tracking users' identities and responding promptly to take-down

[138] US Report, p. 5.
[139] 821 F. Supp. 2d 627.

notices. It also held that MP3tunes.com was not liable for direct infringement because it was its users who chose what songs to upload, and because merely enabling a party to download infringing material is not an infringing act. The court ruled, 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. The court found that MP3tunes.com was contributorily liable for infringement of rights in such works, because it had reasons to know about the infringing activities and still provided the site and facilities for the infringing activities.

In *Disney Enterprises, Inc. v. Hotfile Corp*., the service provider allowed users to upload and download video files.[140] Hotfile did not behave as a provider that 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 that became frequently most downloaded were rewarded by certain benefits. 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.

In *Perfect 10 v. Megaupload*,.[141] the District Court (another) 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[142] could be regarded as amounting to volitional conduct.[143] Thus, the court held that Megaupload was directly liable for the infringement of the relevant acts covered by copyright[144] (which, from the viewpoint of the WIPO "Internet Treaties" meant the right of reproduction and the right of making available to the public).

Adventures of RapidShare and other "locker" providers in Germany: copyright owners are not left alone in the dark.

In Europe, two cyberlocker cases have attracted the greatest attention. Both cases took place in Germany and concerned the Swiss-based locker provider RapidShare.

On March 14, 2012, the Higher Regional Court in Hamburg (*OLG Hamburg*) adopted three rulings at appeals against judgments of lower courts in suits against RapidShare of which the most important one was where GEMA, the German authors' society was the plaintiff (in the other two cases, German publishers were the plaintiffs). In 2010, the Regional Court of Hamburg found basically in favor of GEMA.[145] The Hamburg OLG agreed with the ruling.[146]

The OLG's decision confirmed that RapidShare must implement effective measures to prevent uploading illicit copies. Although RapidShare was ready to take down infringing materials when it had been notified, it did not take any measure against uploading copies infringing copyright in the same works by the same or different users of its service. The court

[140] Disney Enterprises, Inc. v. Hotfile Corp., 798 F. Supp. 2d 1303 (S.D. Fla. 2011).
[141] (Note in the US Report) Perfect 10, Inc. v. Megaupload Ltd., No. 11CV0191-IEG BLM, 2011 WL 3203117, at *2 (S.D. Cal. July 27, 2011).
[142] (Note in the US Report) *Id. at* *6.
[143] (Note in the US Report) *Id.* at *4.
[144] (Note in the US Report) *Id. at* *6.
[145] GEMA v Rapidshare AG, Landgericht Hamburg, File nº 310 O 93/08.
[146] OLG Hamburg No. 5 U 87/09 of March 3, 2012.

obligated RapidShare to implement additional measures – in practice, a filtering system – to prevent a copyright infringement 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).

In *Atari v. RapidShare*, where the issue was the use of illegal copies of the video game "*Alone in the Dark*," first, the locker provider seemed to be the winner. The Regional Court (*LG*) of Düsseldorf, similarly as 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.[147] The court made some statements which were somewhat surprising in view of the well-known activities of the website, such as that "most people utilize RapidShare for legal use" and that, if the contrary were assumed, it would mean "a general suspicion against shared hosting services and their users which is not justified." This was quite a strange way of arguing: it would not be appropriate to have such suspicion; therefore, it should be presumed that most people utilize the services for legal use. 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*) saw the factual situation more realistically[148] and deduced from it more adequate findings. It reversed the ruling of the Düsseldorf OLG.[149] Although it stated that, in principle, file hosting services are to be recognized as an appropriate business model, it also ruled that they should duly cooperate with copyright owners not only by removing illegal copies from their system but also by preventing repeated uploading thereof (that is, if illegal copies of a work are taken down, they should stay down). If RapidShare does not apply a reasonable filtering system for this purpose, it will be liable for the infringements.

The German response to the congress Questionnaire reports on another case where direct liability was found by the court.[150] As the report describes it, until June 2011, Kino.to was the biggest German-language internet site. The unauthorized copies were stored „on the servers of third parties (professional providers of online storage and streaming solutions, so called 'filehoster')" – that is in the „Cloud" – but the service was controlled by Kino.to. The users of the service uploaded the works to their personal „lockers" and received links to them. As the German response reports „[e]verybody having access to the internet could also access those links and hence either stream the connected movies or download them on user-owned storage devices."

The Regional Court of Leipzig held[151] that Kino.to had communicated works to the public in the sense of interactive making available to the public. The court found that the relevant act of exploitation was the uploading of the works on the Internet and that of no importance was whether or not the works were accessed, if accessed how frequently and by what kind of technological means. As the German report stresses, the court differentiated between "deep links" and "other links". It held that offering deep links to contents that were saved

[147] OLG Düsseldorf, I-20 U 59/10 of December 21, 2010.
[148] It is reflected, for example, by the remark that after all „[t]he company is called RapidShare and not RapidStore."
[149] BGH, Urt. v. - I ZR 18/11 of July 12, 2012.
[150] German Report, p 6.
[151] (Note in the German Report) LG Leipzig, No.11.04.2012, File number 11 KLs 390 Js 183/11 of April 11,2012.

somewhere else, in general, does not correspond to the criteria of Article 19a of the German Copyright Act. However, in the Kino.to system, it was exclusively through the links that it was possible to find and access the films. The court stressed that „this scenario was therefore held to be comparable with integrating the links in one's own web presentation especially since employees of Kino.to had controlled all links as to whether the named movies were complete and if they included a reference to Kino.to in the beginning and the end." Kino.to was better known and more broadly used in Germany than Megaupload, the big pirate cloud network of Kim Dotcom, the other German living in New Zealand (which was shut down in January 2012, and „Dotcom" was detained). The Leipzig court sentenced Dirk. B., the main operator of Kino.to to four-and-a-half-year imprisonment for infringements of copyright. Other operators of the service also received prison sentences.

EXCEPTIONS AND LIMITATIONS AND EXHAUSTION OF RIGHTS IN THE "CLOUD"

Exceptions and limitations; in particular as regards private copying

Is it private copying at all? 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 those on the three-step test itself 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. In certain cases, 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.

As it is discussed above, it has been a disputed question from the beginning of the first lawsuits on cloud-type hosting services, such as *Cablevision*, whether, when the copying is triggered by a user of a service (possibly by a simple click) on the servers of a cloud provider and it is kept there (even if in a storage space reserved for the user), it is the user who makes the copy, or the service provider, or both of them. There are national laws under which the private copying exception or limitation does not apply where a commercial service makes copies for private purposes. Furthermore, even where there is no specific provision of this kind, it may be clarified that the exception or limitation is not applicable where the copying is made for direct or indirect economic advantage – for example, as in the case of Article 5(2)(b) of the Information Society (Copyright) Directive.

The report prepared by the French ALAI Group in response to the congress Questionnaire expresses the view that the status of "private copying" is not sufficiently clear under the European *acquis communautaire* and the French legislation. Under French jurisprudence, in order that a copy may qualify as a result of private copying, the copier and the user of the copy should be the same person. As soon as a third person intervenes, he or she becomes the copier and must have an authorization from the owner of the exclusive right of reproduction.[152] 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, there is no "private copy."[153]

[152] French Report, p. 7.

[153] *Id.*

However, the French report refers to „another analysis," according to which neither the French Intellectual Property Code nor the *acquis communautaire* (the 2001 Information Society (Copyright) Directive) 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 since it seems that it has reconciled the existence of a „copying service" with the private copying exception.[154]

The author of this paper votes for the first „analysis." As regards the French Intellectual Property Code, it appears quite clear that the copier and the user must be the same person, since it provides for an exception in respect of copies „reserved strictly for the private use of the copier and not intended for collective use."[155] Thus, if it is found that the a service provider is the maker of the copy, the exception does not apply.

It is submitted that, just because the *Padawan* decision[156] refers in certain sentences to copying services, it does not mean that the French law would be in conflict with the *acquis communautaire*.

It is true that the decision contains such references in points 46 and 48 in the following context:

> 44. Copying by natural persons acting in a private capacity must be regarded as an act likely to cause harm to the author of the work concerned.
> 45. It follows that the person who has caused harm to the holder of the exclusive reproduction right is the person who, for his own private use, reproduces a protected work without seeking prior authorisation from the rightholder. Therefore, in principle, it is for that person to make good the harm related to that copying by financing the compensation which will be paid to the rightholder.
> 46. However, given the practical difficulties in identifying private users and obliging them to compensate rightholders for the harm caused to them, and bearing in mind the fact that the harm which may arise from each private use, considered separately, may be minimal and therefore does not give rise to an obligation for payment, as stated in the last sentence of recital 35 in the preamble to Directive 2001/29, it is open to the Member States to establish a 'private copying levy' for the purposes of financing fair compensation chargeable not to the private persons concerned, but to those who have the digital reproduction equipment, devices and media and who, on that basis, in law or in fact, make that equipment available to private users *or who provide copying services for them*. Under such a system, it is the persons having that equipment who must discharge the private copying levy.
> 47. It is true that in such a system it is not the users of the protected subject-matter who are the persons liable to finance fair compensation, contrary to what recital 31 in the preamble to the directive appears to require.
> 48. However, it should be observed, first, that the activity of the persons liable to finance the fair compensation, namely the making available to private users of reproduction equipment, devices and media, *or their supply of copying services*, is the factual precondition for natural persons to obtain private copies. Second, nothing prevents those liable to pay the compensation from passing on the private copying levy in the price charged for making the reproduction equipment, devices and media available or in the price for the copying service supplied. Thus, the burden of the levy will ultimately be born by the private user who pays that price. In those circumstances, the private user for whom the reproduction equipment, devices or media are

[154] *Id.*
[155] Article L. 122-5(2) of the Intellectual Property Code (in French: "*strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective*").
[156] CJEU, case C-467/08 of October 21, 2010.

made available or who benefit from a copying service must be regarded in fact as the person indirectly liable to pay fair compensation.

It is to be noted, however, that the court neither here nor in other points of the ruling seems to define "copying services" – what they mean, in which cases and under what conditions they might correspond, if at all, to the concept of private copying. There is no legal analysis in the decision in this respect, and this is quite understandable since the CJEU 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.[157] Therefore, serious doubts may emerge whether there is "*res iudicata* in this respect. It seems that national courts may have good reasons to just apply Article 5(2)(b) of the Information Society (Copyright) Directive which quite clearly exclude the application of a private copying exception or limitations in cases where a commercial service make copies for private purposes.

Let us look at 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 use*, 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.)

As it can be seen, the recital speaks about "*private copying*." It is true that it also refers once to copies "*for private use*" (and this is understandable since it is obviously this is supposed to

[157] The referral included the following five questions (in which there is no word about, no reference to, copying services):
"1. Does the concept of "fair compensation" in Article 5(2)(b) of Directive 2001/29/EC entail harmonisation, irrespective of the Member States' right to choose the system of collection which they deem appropriate for the purposes of giving effect to the right to fair compensation of intellectual property rightholders affected by the adoption of the private copying exception or limitation?
"2. Regardless of the system used by each Member State to calculate fair compensation, must that system ensure a fair balance between the persons affected, the intellectual property rightholders affected by the private copying exception, to whom the compensation is owed, on the one hand, and the persons directly or indirectly liable to pay the compensation, on the other, and is that balance determined by the reason for the fair compensation, which is to mitigate the harm arising from the private copying exception?
"3. Where a Member State opts for a system of charging or levying in respect of digital reproduction equipment, devices and media, in accordance with the aim pursued by Article 5(2)(b) of Directive 2001/29 and the context of that provision, must that charge (the fair compensation for private copying) necessarily be linked to the presumed use of those equipment and media for making reproductions covered by the private copying exception, with the result that the application of the charge would be justified where it may be presumed that the digital reproduction equipment, devices and media are to be used for private copying, but not otherwise?
"4. If a Member State adopts a private copying "levy" system, is the indiscriminate application of that "levy" to undertakings and professional persons who clearly purchase digital reproduction devices and media for purposes other than private copying compatible with the concept of "fair compensation"?
"5. Might the system adopted by the Spanish State of applying the private copying levy indiscriminately to all digital reproduction equipment, devices and media infringe Directive 2001/29, in so far as there is insufficient correlation between the fair compensation and the limitation of the private copying right justifying it, because to a large extent it is applied to different situations in which the limitation of rights justifying the compensation does not exist?" (Point 19. of the CJEU ruling.)

be one of the conditions of the applicability of the exception; the copies 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 copies are made by a public service – in particular, where a direct or indirect profit motive is involved – it is definitely not "private copying" but, at maximum, copying for the purpose of subsequent private use.

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 completely clear that the private copying exception does not apply when the copy is made by a service (since it can hardly qualify as a natural person) for direct or indirect commercial purposes. Article 5(2)(b) only allows that a natural person other than the potential user (usually a member of the family or a close acquaintance) make the copy in the private sphere and for private use.

Therefore, the French law is in accordance with the Directive and 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. However, it is submitted again that this question was not supposed to be covered by the referral and the court has not really analyzed this question.

Does a right to remuneration (or "fair compensation") apply? Special questions may emerge also from the viewpoint of the applicability of the right to equitable remuneration (or as the Directive calls it "fair compensation") as provided in the said provision of the Directive. 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.

It seems that doubts may emerge as regards the legal basis of the applicability of the right to equitable remuneration for a "cloud copy" in any of these three cases. In a case mentioned under (i), the "cloud copy" is clearly not a private copy and, in the case of downloading for private purposes, TPM (as a minimum, an access code) is applied which excludes the application of the exception or limitation. 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 in respect of already existing lawful copies. Finally, as regards the case under (iii), as clarified under several national laws, any exception for copying from – at least, obviously – illegal sources[158] is in conflict with the three-step test and, furthermore, the copies made in this manner are subject to the obligation of the cloud provider to take them down rather than to pay compensation for the infringements. (In the "Cloud," the issue of illegal copies emerges in a

[158] For the prohibition of copying from obviously illegal sources, see, for example, Article 53(1) of the German Copyright Act.

way different from the use of recording equipment and material in domestic environment where the taking down of infringing copies is not a reality. This paper does not deal with the latter situation.)

The Commission Staff Working Document mentioned above[159] also seems to be skeptical about the applicability of the private copying levy system in the cloud environment. The document states as follows under the telling title "Cloud computing services challenges to the private copying levies regime:"

> Some of the technologies applied in the digital context, such as streaming, have the potential of reducing the number of copies which are actually made on consumer devices. Cloud computing services, where end-users are actually replicating less on their personal local devices have been seen as a game changer, making the private copy levy concept less appropriate, as digital technology advances…
>
> Increasingly, cloud based services make it possible to measure authorised uses of creative content allowing for a precise licence-based remuneration (and not exception-based compensation) of right owners. This should clearly be the case where a specific cloud-based service has been established following a licensing agreement with rightholders. Furthermore, streaming of music (or audiovisual content) does not require consumer storage capacity…In such cases, applying levies on the basis of memory size does therefore not seem to be aligned with the way music or audiovisual content are consumed…
>
> With the emergence of new business models, consumer-friendly access to attractive legal offers of digital content should be more focused on licensing than on private copying levies. The more digital content and authorised usage consumers are able to acquire as part of a fully licensed service, the less need there is for private copy levies by way of compensation… Fair and efficient transactions between rightholders and cloud services providers as well as between cloud service providers and consumers should allow equitable and efficient remuneration of rightholders. It is essential to take proper account of the opportunities offered by the current development of new business models. Such models deliver new forms of authorised access to copyright protected content. They should at the same time enable rightholders to better control the use of their content and the manner in which they are remunerated for it.[160]

Exhaustion of rights in the "Cloud"

Exhaustion under the WIPO Treaties. The WIPO "Internet Treaties" leave it to Contracting Parties whether or not they provide for exhaustion of the right of distribution and, if they do, in which way[161] (in particular, whether they provide for international exhaustion or territorial exhaustion).

ReDigi: fully-fledged online music store in the guise of a "resale" forum. However, in the cloud environment, there are certain specific aspects of the issue of exhaustion. The *ReDigi*

---

[159] See note 6 *supra*.
[160] Commission Staff Working Document, pp. 19-20.
[161] For example, Article 6(2) of the WCT reads as follows:
„ (2) Nothing in this Treaty shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the exhaustion of the right in paragraph (1) applies after the first sale or other transfer of ownership of the original or a copy of the work with the authorization of the author." Agreed statement concerning Articles 6 and 7: "As used in these Articles, the expressions 'copies' and 'original and copies' being subject to the right of distribution and the right of rental under the said Articles, refer exclusively to fixed copies that can be put into circulation as tangible objects."

case reported in the response of the US ALAI Group to the congress Questionnaire is a good example for this.

As the US ALAI Group reports,[162] *Capitol Records* has filed a lawsuit recently against *ReDigi.com*, an online marketplace of "used digital copies of recorded music."[163] The service allows users to store their recordings in online lockers and "sell" them through the "Cloud." If the customers wish to "sell" a "used" digital recording through the system, they have to download ReDigi's software. The software allows a user to designate the recordings legally purchased from iTunes Store or ReDigi that they wish to sell from his or her device. In such a case, ReDigi removes the eligible recordings from the seller's device and stores them in the ReDigi cloud for "sale." Buyers are able to view a list of recordings that are for sale, and purchase and download them.

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.[164] Among other claims, the plaintiff alleges that ReDigi engages in unauthorized reproduction, distribution, and public performances of the plaintiff's works and assists users in making unauthorized copies and sales. In response to some of these allegations, ReDigi has claimed fair use and the first sale doctrine as a defense.[165] Although the first sale doctrine traditionally applies only to hard 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 time, should enjoy the same exemption from copyright liability as do tangible used books and records. (At the time of the preparation of the report of the US ALAI Group, the process was in a stage where Capital Records had requested a preliminary injunction.)

In the opinion of the author of this paper, ReDigi's claims might hardly stand any serious scrutiny.

The exhaustion of the right of distribution (with the underlining right of reproduction) is hardly applicable in case of such a service. 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; a new copy is made and, where that copy is "sold," still another is made. Thus, not the right of distribution, but the right of reproduction is concerned in the case of which no exhaustion applies.

Furthermore, when the copy made on Re.Digi's server is offered for sale, the right of making available is implied which, under the WIPO "Internet Treaties" – in contrast with the right of distribution concerning tangible copies – is not covered by the principle of exhaustion of rights either.

[162] US Report, pp. 6-7.
[163] (Note in the US Report) Complaint, Capitol Records, LLC v. ReDigi, Inc., 2012 WL 32056 (S.D.N.Y. Jan. 6, 2012) (No. 12 CIV 0095).
[164] (Note in the US Report) Complaint, *Capitol Records v. ReDigi*, 2012 WL 32056.
[165] (Note in the US Report) 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.

In the last-but-one paragraph above, the words "in principle," is stressed. What may happen in principle does not necessarily happen in practice. If a ReDigi customer wishes to continue using the recording, it does not have to do anything else but to save it on an external device. Let us consider this "in principle" aspect in the light of the level of law abidance of online users as reflected in what is taking place in p2p systems or on UGC platforms. Someone should be – or may pretend to be – extremely naive to believe that ReDigi clients will give up possession of copies that still represent any value or interest for them. The "obligation" to remove the original copy would not seem to be more realistically applicable than trying to ensure the life of a rabbit placed in a tiger's cage by putting an inscription into his neck with the text: "Prohibited to eat it!"

UsedSoft: the CJEU tries to extend the doctrine of exhaustion of rights to where it is not applicable. The Court of Justice of the European Union has adopted a ruling on possible application of the principle of exhaustion of rights in digitally distributed computer programs

In *UsedSoft v. Oracle*, the subject matter of the dispute was Oracle's computer programs concerning the application of end-user license agreements (EULAs). A EULA contains a term forbidding the licensee to transfer the program to a third party. UsedSoft, a company based in Germany, was "reselling" these "licenses" (and, thus, the programs) to the customers of its service.

The CJEU, in its *UsedSoft v. Oracle* ruling,[166] held that the exhaustion of the right of distribution is also applicable for digitally distributed computer programs. The preliminary ruling reads as follows:

> 1. Article 4(2) of Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs must be interpreted as meaning that the right of distribution of a copy of a computer program is exhausted if the copyright holder who has authorised, even free of charge, the downloading of that copy from the internet onto a data carrier has also conferred, in return for payment of a fee intended to enable him to obtain a remuneration corresponding to the economic value of the copy of the work of which he is the proprietor, a right to use that copy for an unlimited period.
>
> 2. Articles 4(2) and 5(1) of Directive 2009/24 must be interpreted as meaning that, in the event of the resale of a user licence entailing the resale of a copy of a computer program downloaded from the copyright holder's website, that licence having originally been granted by that rightholder to the first acquirer for an unlimited period in return for payment of a fee intended to enable the rightholder to obtain a remuneration corresponding to the economic value of that copy of his work, the second acquirer of the licence, as well as any subsequent acquirer of it, will be able to rely on the exhaustion of the distribution right under Article 4(2) of that directive, and hence be regarded as lawful acquirers of a copy of a computer program within the meaning of Article 5(1) of that directive and benefit from the right of reproduction provided for in that provision.

The ruling closely concerns also, for example, such cloud services as *Steam* and *Origin* for distribution platforms of video games. In principle, where such a game is made available on those platforms, under the UsedSoft ruling, the owners of rights would have to allow free transfer of the games in the form of "resale."

[166] CJEU case C-128/11.

The court has tried to provide certain "guarantees" against the infringement of the rights of reproduction and distribution. It has stated that the "re-seller" of a copy must make it unusable on its own devices (and has clarified that a multi-user license must not be split into separate units for "re-selling" purposes). However, as pointed out above – in view of easily available ways of saving a copy of what is "resold" – these kinds of guarantees may not have too much value.

The same may be said about this case as on *ReDigi* in the US. The distribution right applies to the resale of, or other transfer of rights in, the same lawfully obtained *tangible* copies. In the given case, it is obvious that no resale of copies takes place; new copies are created and, thus, the right of reproduction is concerned. In the case of an act of reproduction, there is no resale; the application of the exhaustion doctrine cannot emerge.

The court has created new law and, by this, it seems to have gone beyond what its competence would have allowed in the EU's constitutional structure. Therefore, its validity for Member States is questionable. The more so because the new law created by the court appears to be in conflict with both the international treaties and the *acquis communautaire*.

It is difficult to understand how the court maneuvered itself into such a situation since it had correctly listed the relevant international and EU provisions that it was supposed to apply (but with which it got into conflict).

It seems the court has misinterpreted the meaning of the right of making available to the public under the Article 8 of the WCT and Article 3(1) of the Information Society (Copyright) Directive and its relationship with the right of reproduction and the right of distribution.

The CJEU 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 ways of implementing the right of making available to the public. This was clarified at the 1996 Diplomatic Conference on the basis of the "umbrella solution."[167] However, there are two things which the court seems to have disregarded.

First, the Information Society (Copyright) Directive, 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 it is provided in Article 8 of the WCT; that is, within the framework of a broad right of communication to the public. Second, choosing "distribution" as legal qualification does not change the fact that what takes place in the case of interactive online transmissions is not the transfer of property in a copy of the work, but making a *new copy* in the computer memory in which a work (including a computer program) is downloaded. The Advocate General erred (and the court erred along with him when it adopted his theory) when it stated that, in case of downloading, the act of making available to the public is transformed into an act of distribution.[168]

It should always be kept in mind that, although it is possible to speak about "distribution" in the case of certain forms of making available to the public, a very special distribution is involved; namely, *distribution though reproduction through (interactive) transmission*. The right of distribution may be exhausted by the first sale of *tangible* copies, but the right of reproduction is not exhausted when a copy is *made*. Furthermore, Article 3(3) of the

[167] See note 56, *supra*.
[168] See pt. 52 of the preliminary ruling.

Information Society (Copyright) Directive excludes the exhaustion of the right of making available to the pubic – irrespective of whether it is construed as a separate right as under Article 3(2) (concerning related rights), or as part of a broad right of communication to the public as under Article 3(1) (concerning copyright), and irrespective of whether it is implemented by being *characterized* as a separate right of making available to the public, a right of communication to the public, or a right of distribution.

Recital (29) makes this crystal-clear:

> *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.* (Emphasis added.)

This is just a confirmation of what follows from the provisions of the WIPO "Internet Treaties" and the Directive which has faithfully implemented the Treaties. The court quoted this recital, but it seems it did not agree with the relevant norms of the Treaties and the Directive, and it decided to replace them by new rules. Let us make an understatement: in our view, the CJEU's competence hardly extends to this kind of law making.

The application of the right of distribution as a way of implementing Article 8 of the WCT is allowed under the concept of "relative freedom of legal qualification" of acts covered by copyright. However, as this concept is defined in the WIPO Glossary of Copyright and Related Rights Terms, [169] the freedom applies only where, although through rights characterized in different way, the minimum obligations prescribed by the international treaties are fulfilled. Thus, for example, it would be possible to qualify certain forms of interactive making available as "broadcasting" and to apply the right of broadcasting, but this

[169] The definition reads as follows:
"*Legal characterization of acts and rights; principle of relative freedom of ~*
"1. It is a broadly applied practice in national legislation to use terms other than those appearing in the *international norms on copyright and related rights* concerning certain acts covered by such rights, and consequently by the rights themselves; that is, to characterize the acts and rights concerned in a way different from the way they are characterized legally in the said international norms. For example, several countries grant a "*right of public performance*" in a way that it covers more or less all *non-copy-related rights* (in particular, also the *right of broadcasting* and the *right of communication to the public by cable (wire)*, which, in the *Berne Convention* are construed as separate rights), or it is also frequent in national laws that a broader *right of broadcasting* is provided which also covers the *right of communication to the public by cable (wire)*, a separate right under the *Berne Convention*.
"2. Such a practice is accepted and regarded as legitimate, provided that the level of protection granted by the legislation of the given country, in spite of the differing legal characterization of the acts and rights concerned, corresponds to the minimum level of protection prescribed by the relevant *international norms on copyright and related rights* (such as in respect of the nature of the rights – whether *exclusive rights* of *authorization* or a mere right to *remuneration* – or the scope of *exceptions* to *and limitations* on them). For example, if the concept of *broadcasting* is extended also to *communication to the public* and even to (interactive) *making available to the public*, this does not authorize the legislators of the country concerned to extend the *limitations* allowed in Article 11*bis*(2) of the *Berne Convention* (*non-voluntary licenses* or *obligatory collective management*) beyond the scope of the *right of broadcasting* determined in the *Berne Convention* (in its Article 11*bis*(1); that is, it is not permitted to apply the same *limitations* to *cablecasting* (of *cable-originated programs*) and to (interactive) *making available* of *works to the public*. For this reason, the principle of freedom of legal characterization of acts and rights should be referred to as the "principle of relative freedom of legal characterization of acts and rights." (WIPO Guide and Glossary, p. 294).

legal characterization would not allow to the Contracting Party concerned to introduce compulsory licenses on the basis of Article 11*bis*(2) since, in the case of the right of making available to the public (for the implementation of which the right of broadcasting would be chosen), no such compulsory licenses are allowed.

The agreed statement concerning Article 6 and 7 of the WCT should be interpreted in the light of this concept. It clarifies that the right of distribution only applies for *tangible* copies. This means *minimum obligation* under the Treaty. It does not exclude the possibility for a Contracting Party to apply the right of distribution in a broader scope as what is prescribed, namely also in respect of intangible copies. However, as regards the question of exhaustion of the right, the agreed statement does not provide for a minimum obligation but *the maximum of the applicability of a limitation of a right*; namely, the right of distribution. Just because the right of distribution may be been chosen as one of the ways of implementing the right of making available to the public, it does not mean that it is allowed to provide for the exhaustion of the right of making available when it is implemented in that way. Thus, the application of Article 3(3) of the Directive is inevitable. As a result of downloading (which, as mentioned above, may be characterized as distribution through reproduction through transmission), there is a copy in the end-user's computer memory. Where a copy is included in a website as UsedSoft and is offered for "sale," no transfer of property takes place. A new copy is made. The act is covered by the right of reproduction and, since the copy is offered for online "sale," also the right of making available to the public is involved. Neither of these rights may be exhausted under the WIPO "Internet Treaties" and the Information Society (Copyright) Directive.

The court seems to have found that, although, under the Information Society (Copyright) Directive, exhaustion does not apply for intangible copies, it may still apply under the Compute Programs Directive,[170] since, in its view, the relevant provisions of the latter directive may to be regarded as *lex specialis*.

The nature of certain provisions of the Computer Programs Directive may truly be characterized as such (for example, the provisions on back-up copies and decompilation). However, the concept of distribution and, in connection with it, the concept of "sale" do not belong to that category. The court stated that these concepts were not determined, and that it was its tasks to determine them.[171] However, if this had been truly the case, what might have been the reason not to apply the same concepts which follow from the WIPO "Internet Treaties" and the Information Society (Copyright) Directive? It is submitted that there was no such reason; no justification for not applying the *lex generalis* under the Information Society (Copyright) Directive in the absence of any *lex specialis*.

One may ask the question of whether or not the new exception to the exclusive right of reproduction not existing under any EU directive (although, for its applicability, in the closed system of exceptions and limitations of the directives, it would have to be provided) but invented by the CJEU, might be in accordance, at least, with the three-step test.

A negative answer would be justified to such a possible question. It is doubtful whether the newly introduced exception to the right of reproduction is limited to a special case and, thus, whether it is in accordance with the first condition of the test. However, it appears that it may fail the second condition since it has the potential of getting into conflict with a normal

[170] Directive 2009/24 codifying Council Directive 91/250/EEC of May 14, 1991.
[171] See pts 40 to 42 of the preliminary ruling.

exploitation of the works concerned. Online distribution – with its efficiency, speed and viral nature – creates a new situation, quite different from what is known where the exhaustion of the right of distribution has its adequate field of application. Such kind of new exception may undermine, for example, what is now one of the most important ways – if not the most important one – of exploiting video games: duly controlled online distribution.

It should also be seen that the application of the newly construed exception would be particularly detrimental to the exploitation of works whose use is of a "consumptive" nature in the sense that, after having been used once, their value is lost or, at least, substantially decreased for the given end-users (for example, films or fiction books). At the same time, for those who have not used the same works yet, the value thereof is still intact. In spite of this, through an online "resale" network, such persons may obtain copies at a price lower than the market value of new copies (of course, the expressions "resale" and "used copies" do not express reality; in fact, what takes place is downloading – making – brand new and perfect digital copies). If this kind of reuse became widespread – and experience shows that, on the Internet, this usually happens when people may get works freely or at a lower price – it might create a downward spiral of the market value of the works concerned and, thus, it might undermine the chance of creators and producers to recoup their investment. Thus, such online "resale" services may get in conflict with a normal exploitation of the works concerned (and therefore with the three-step test).

Let us presume that the exhaustion of the right of distribution were still applicable – but in reality it is not – when new copies are made on the server of an online "resale" forum and then in the system of the new "buyer." Would then it be acceptable that the extension of the first sale doctrine the way the CJEU has foreseen would create conflict with the normal exploitation of the works concerned due to the reasons mentioned above?

In this context, also the question may emerge whether or not the three-step test might have a role in respect of the exhaustion of rights. Considering the text of the relevant international provisions (Article 9(2) of the Berne Convention, Article 13 of the TRIPS Agreement, Article 10 of the WCT, Article 16 of the WPPT and Article 13 of the BTAP), this does not seem to be an unjustified question. The three-step test is to control exceptions to and *limitations* of rights and, after all, a provision on exhaustion of the exclusive right of distribution with the first sale of copies, according to the ordinary meaning of the word, may qualify as a limitation of that right. Such a possible interpretation may be strengthened by those provisions of the WIPO "Internet Treaties" (Article 6(2) of the WCT, Articles 8(2) and 12(2) of the WPPT and Article 8(2) of the BTAP) which make it clear that exhaustion is not an indispensable constituting element of the concept of the right of distribution; Contracting Parties are allowed to provide for exhaustion on the basis of the same kind of language as what is used in the treaty provisions on exceptions and limitations. Let us take, as an example, the text of Article 6(2) of the WCT:

> Nothing in this Treaty shall affect the freedom of Contracting Parties to *determine the conditions, if any,* under which the exhaustion of the right in paragraph (1) applies after the first sale or other transfer of ownership of the original or the copy of the work with the authorization of the author.

In the text quoted above, emphasis is added to the term "determine the conditions" which is the same as in Article 11*bis*(2) of the Berne Convention allowing limitations of the right of

broadcasting (and related acts). Emphasis is also added to the words "if any" to underline that, in principle, a Contracting Party may also decide not to provide for exhaustion of the right.

If the three-step test were applied to the limitation consisting in the exhaustion of the right of distribution, it would be a suitable basis to claim that allowing the use of works through certain online "resale" forums would be in conflict with the test since it would conflict with a normal exploitation of the works concerned (it would enter into an economic competition with the rights of copyright owners and would undermine the legitimate market for them).

The regulation of the right of rental is a good example to show that, irrespective of whether it takes place through the application of the three-step test or through specific legislative norms, in certain cases, it is not justified to extend the scope of exhaustion of copy-related rights beyond the field where it relates to real resale of (or other transfer of property in) tangible copies.

In certain countries, the concept of distribution also covers rental of copies (although rental does not mean transfer of property, but only transfer of possession).[172] In accordance with this, the exhaustion of the right of distribution may also apply for rentals. However, where the exhaustion of the, thus, extended right of distribution conflicts with a normal exploitation of the works concerned (in particular, in respect of the right of reproduction), it is not applied for rental. This kind of connection between exhaustion and possible conflicts with the normal exploitation of materials protected by copyright or related rights may be witnessed, for example, in Article 14(3) of the TRIPS Agreement, Article 7(2) of the WCT, Articles 9(2) and 13(2) of the WPPT and Article 9(2) of the BTAP. Those provisions allow the limitation of the exclusive right of rental to a right to equitable remuneration – or, under the BTAP, an exception to its application – provided, however, that this does not give rise to any "*material impairment*" of the exclusive right of reproduction (a kind of synonym of conflict with a normal exploitation of protected productions).

Having discussed these aspects, it should be noted again, however, that, the reason for which the extension of the scope of application of the exhaustion of rights foreseen in the CJEU ruling does not seem to be in accordance with the international and EU norms is much simpler; namely, that it concerns certain rights – the right of reproduction and the right of making available to the public – in the case of which those norms do not allow exhaustion.

THE ROLE OF DIGITAL RIGHTS MANAGEMENT, IN PARTICULAR TECHNOLOGICAL PROTECTION, IN CLOUD SERVICES

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

Since the adoption and then the entry into force of first two WIPO "Internet Treaties," sufficient experience has been accumulated on how the provisions on technological measures (Article 11 of the WCT, Article 18 of the WPPT and Article 15 of the BTAP) and on rights

[172] The Computer Programs Directive also qualifies rental as a part of the concept of distribution, but, in the case of rental, it excludes the application of the exhaustion of the right. This is so since Article 4(2) of the Directive reads as follows: „ *The first sale* in the Community of a copy of a program by the rightholder or with his consent *shall exhaust the distribution right* within the Community of that copy, *with the exception of the right to control further rental* of the program or a copy thereof." (Emphasis added.)

management information (Article 12 of the WCT, Article 19 of the WPPT and Article 16 of the BTAP) should be interpreted and applied.

Technological protection measures (TMPs) and digital rights management information (RMI) are frequently applied together 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 the protection of 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. The volume of this paper would not allow, and its objective would not necessitate, offering a detailed description and analysis in this respect. It seems to be sufficient to outline the most important elements of the said standards concerning TPM protection; namely
- since the treaty provisions obligate Contracting Parties to provide adequate protection and effective remedies for all TPMs, they must be applied for both access-control and copy-control (or more generally: right-control) measures;
- no adequate protection may be granted for TPMs if only the very acts of circumvention are prohibited; the defense line should be established in the stage of "preparatory acts" (manufacturing and distribution of unauthorized circumvention devices and offering unauthorized services);
- the obligation of granting adequate protection is not limited against the acts of circumvention that may result in infringements of copyright; it also extends to circumvention of any TPMs applied by the owners of rights in connection with any form of exercising rights (thus, also any TPMs ensuring conditional access for certain uses that are not covered by copyright – such as getting access for viewing a streamed film – but without the control of which the protection and exercise of rights, in certain cases, would be impossible);
- the obligation to provide effective remedies against circumvention should mean the application of both civil remedies and, in particular in the case of "preparatory acts" performed on a commercial scale, criminal punishments;
- where TPMs are used by the owners of rights, appropriate measures (provisions and mechanisms) are justified to ensure the applicability of certain exceptions and limitations that are indispensable from the viewpoint of the public interest, but (i) preference should be given to voluntary measures between the owners of rights and the beneficiaries of exceptions and limitations, (ii) in view of this, beneficiaries, in general, should not be allowed to circumvent TPMs by simply citing exceptions and limitations, but rather only through the operation of a well-balanced intervention mechanism; and (iii) the way the measures for the applicability of certain exceptions and limitations should be provided and used with full respect for the conditions prescribed in the "three-step test" test.[173]

The last important criterion mentioned in the preceding paragraph concerning the role of the three-step test in the intervention mechanisms has been stated in a particularly clear manner in the ruling of the French Supreme Court (*Cour de cassation*) in the *Mulholland Drive* case.[174]

[173] For analysis of these issues, see Mihály Ficsor: „*Protection of DRM under the WIPO 'Internet Treaties' – Interpretation, Implementation and Application*," in „Copyright Enforcement and the Internet" (edited by Irini A. Stamatoudi), Walter Kluwers, 2010, pp. 257-302.
[174] *Cour de cassation*, (2006) 37 I.I.C. 760 of February 28, 2006.

Que choisir, the French consumers' association asked the court to rule that it is allowed to circumvent the copy-control TPM used in DVDs containing films (CSS) in order to be able to exercise the "right to make private copies." The court clarified that no such thing exists as a "right" to private copies. Although adequate exceptions and limitations may be provided for private copying in accordance with Article 5(2)(b) of the Information Society (Copyright) Directive, those exceptions and limitations are also subject to the three-step test (under Article 5(5) of the Directive and relevant international norms). In accordance with this, the court held that allowing circumvention of the TPM protecting films in DVDs to make private copies for mere convenience such as place-shifting or device-shifting as claimed by *Que choisir* would be in conflict with the test (since the removing of the TPM protection would facilitate the unauthorized making available of films in the digital online environment and would create a conflict with normally exploitation of the films).

This important principle clarified and laid down in *Mulholland Drive* was 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 themselves must be in accordance with the three-step test, but the implementation of the measures to make the enjoyment of certain exceptions and limitations must also be controlled by the test.[175]

In *Mulholland Drive*, one of the reasons for which *Que choisir* demanded that the circumvention of DSS technological protection should be allowed to consumers was that, without this, the films cannot be used on other devices and cannot be made available to other members of the same family, although in both cases, the acts of reproduction would qualify as private copying.

It is important to note that the application of cloud technology may also solve the "problems" of alleged inconveniences about which *Que choisir* was complaining. And it may be done exactly by means of using DRM protection in a flexible and user-friendly manner – in accordance with one of the basic elements of the concept of cloud-based systems; namely that they make it possible using works anytime, anywhere and on a great variety (but a determined number) of devices.

The recently launched UltraViolet (UV) system is a good example for this. Wikipedia seems to offer an appropriate description of the system:

> *UltraViolet (UV)* is a digital rights authentication and *cloud-based* licensing system that allows users of digital home entertainment content to stream and download purchased content to multiple platforms and devices….

[175] The agreed statement reads as follows: "It is understood that nothing in this Article prevents a Contracting Party from adopting effective and necessary measures to ensure that a beneficiary may enjoy limitations and exceptions provided in that Contracting Party's national law, *in accordance with Article 13* [on the three-step test], where technological measures have been applied to an audiovisual performance and the beneficiary has legal access to that performance, in circumstances such as where appropriate and effective measures have not been taken by rights holders in relation to that performance to enable the beneficiary to enjoy the limitations and exceptions under that Contracting Party's national law. Without prejudice to the legal protection of an audiovisual work in which a performance is fixed, it is further understood that the obligations under Article 15 are not applicable to performances unprotected or no longer protected under the national law giving effect to this Treaty." (Emphasis added, note inserted.)

> UltraViolet adheres to a "buy once, play anywhere" approach that allows users to store digital proof-of-purchases under one account to enable playback of content that is platform- and point-of-sale-agnostic…
>
> UltraViolet is deployed by the 74 members of the *Digital Entertainment Content Ecosystem* consortium, which includes film studios, retailers, consumer electronics manufacturers, cable TV companies, ISPs, network hosting vendors, and other Internet systems and security vendors…
>
> Content consumers create a free-of-charge UltraViolet account, either through a participating UltraViolet service provider, or through the UltraViolet website, with six accounts allowed per household. An UltraViolet account provides access to a Digital Rights Locker where licenses for purchased content are stored and managed irrespective of the *point of sale.* 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). Once downloaded, an UltraViolet file 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. Compatible devices include set-top boxes as well as Internet-enabled devices such as computers, game consoles, Blu-ray players, Internet TVs, smartphones, and tablets…
>
> UltraViolet content is downloaded or streamed in the *Common File Format*, using the *Common Encryption* (CENC) system… Because every UltraViolet title arrives in this format, it will generally play on any UltraViolet branded device.
>
> DECE members developed a common file format (CFF) designed to play in all UltraViolet players and work with all DECE-approved *DRMs*.

As it can be seen, UV is an extremely flexible and user-friendly service. Although the DRM system supporting it – in quite an understandable manner – applies certain limits, it offers a convenient and broad framework for user experience. It hardly has any of the possible characteristics for which DRM systems, and in particular TPMs, have been criticized both by activists and by consumers. At the same time, it seems suitable to ensure adequate protection and exercise of copyright in the online environment. In a way, it is a symbol of a promising "coming of age" of TPMs and DRM. As such, it particularly justifies that the above-outlined standards of TPM protection be fully and duly applied to support it.

Combination of software and firmware TPMs for cloud services; fight against illegal "modchips"

Treaty obligations on adequate protection of firmware TPMs. As described in the introductory part of the paper briefly, and as also mentioned above in connection with the UltraViolet platform, legal cloud services, in general, use DRM systems, and within them TPMs frequently in a combination of software and firmware (or hardware) measures embedded in devices. Firmware TPMs, beyond any doubt whatsoever, correspond to the concept of technological measures under the relevant provisions of the WIPO "Internet Treaties" and the national laws duly implementing them. They provide efficient guarantees for adequate protection and exercise of rights since their circumvention tends to be more difficult than in the case of merely software-based TPMs.

Firmware TPMs deserve adequate protection, at least, in the same way as "traditional" software-based TPMs. However, due to the fact that they are key elements of the defense line against game piracy, they may deserve even greater attention and support.

The attempts 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-based 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 firmware protection for video games. The attacks take the form of manufacturing, distributing and using "*modchips*" (modification chips removing firmware-based technological protection) to circumvent such protection built in video consoles. There are attempts to try to "legalize" this form of commercial-scale unauthorized circumvention of firmware TPMs. Although, at the moment, these mainly concerns video consoles, it is clear that, if the attacks succeeded, the other promising cloud-distribution-cum-firmware-TPM-controlled-device systems might fall as victims too. Therefore, it is worthwhile reviewing the current battles around "modchips" more in detail.

US: attempt at (mis)using administrative rulemaking to try to remove firmware protection and open the way for game piracy. It seems that the best way to outline the problems of "modchips" and their role in game piracy may be on the basis of what is taking place in this respect in the current three-annual rulemaking proceeding at the US Copyright Office as mandated by section 1201 of the Copyright Act. As it is known, as a result of such proceedings, the Librarian of Congress may designate 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 console." As it turns out from the minutes of the hearings on this proposal,[176] such interoperability – according to the proposal – 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.

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

The principle adopted by the French Supreme Court in the *Mulholland Drive* case mentioned above may be of useful 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.

[176] *See* www.copyright.gov/1021/hearings/2012/agenda, and in particular www.copyright.gov/1201/2012/heraings/transcripts/heraing-5-17-2012.pdf.

In the given case, it also seems to be doubtful whether there is truly any non-infringing use that is supposed to be guaranteed 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 must not cause a conflict with the "three-step test." This criterion is now clearly stated in the agreed statement concerning Article 15 of the BTAP in relation with its Article 13 as discussed above. The three-step test controls not only the exceptions and limitations themselves but also the impact of the measures used for their applicability in case of use of TPMs.

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 undermine the possibility of 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.

For a commentator who tries to judge the proposal made by the EFF from the viewpoint of the relevant international norms, it seems quite clear that it would hardly be acceptable from the viewpoint of those norms. However, the same seems to be case as regards the criteria applicable in the US administrative rulemaking proceedings. The impression is that the real objective of the proposal is not just to introduce and exception to the prohibition of circumvention of TPMs, but rather to simply remove the protection by the TPMs which are indispensable for sustainable production by – and even for the very survival of – the game industry.

This seems to fit in the well-known strategic objective of the EFF revealed on many occasions. Its real objective is not just being bothered by trying to achieve some exemptions to the prohibition of circumvention of TPMs but to eliminate any such prohibition which it opposes on a kind of ideological basis.

However, this objective happens to be in conflict with the existing – and duly justified – international and national norms.[177]

Europe: mixed rulings with healthy trends (so far). The Information Society (Copyright) Directive has faithfully implemented the provisions of the WCT and the WPPT. The provisions of Article 6 of the Directive, and in particular the definition of "effective technological measures" in paragraph (3), do not leave any doubt that the Member States must provide adequate protection and effective remedies also against the circumvention of firmware-based TPMs, including preparatory acts, such as manufacturing and distributing such unauthorized circumvention devices as the modchips.

There are now ever more EU countries where the courts, sometimes after some detours in the not necessarily right direction, have interpreted and applied Article 6 of the Information Society (Copyright) Directive adequately.

[177] After the completion of this paper – and the Kyoto ALAI Congress – on October 26, 2012, the Librarian of Congress published the list of works covered by the exemptions to prohibition on circumvention of access-control TPMs. In the list, the above-discussed EFF proposal is mentioned among the rejected proposals. See www.federalregister.gov/articles/2012/10/26/2012-26308/exemption-to-prohibition-on-circumvention-of-copyright-protection-system-for-access-control&4-20.

For example, in the *United Kingdom*, where in the *Gilham v. the Queen* case,[178] the defendant was condemned for criminal offence because it had distributed modchips. 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 modchip cards for copyright infringement and unauthorized circumvention of TPM.[179] The card was able to circumvent the firmware DRM of Nintendo DS applied to verify whether a game card inserted is genuine. As a result, it became possible to download illegal copies of video games from the internet.

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."

In other countries, as mentioned above, court practice has taken time and again some detours before reaching appropriate findings on the application of anti-circumvention norms against modchip manufacturers and distributors.

In *Spain*, in 2009, the Court of Salamanca adopted a weird ruling in a procedure initiated by *Nintendo* against *Movilquick*[180] which consisted in disregarding the international, EU and national norms on the protection of TPMs. One may form no other impression in reading the report on the ruling. The court found that Movilquick's modchip served for circumventing the TPM applied by Nintendo in its video console for the protection of games. It also recognized that this opened the gate for the use of pirated games. However, the court still dismissed Nintendo's claim by referring to the possibility that, when the TPM was circumvented, the console might be used not only for illegal objectives but also for certain legal purposes. The court did not interpret the provisions on prohibition of unauthorized circumvention of TPMs in a narrower or broader way; it simply neglected them (probably they were not in accordance with the judge's personal views).

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[181] the importers and sellers of R4 card modchips for circumvention of the firmware TPM applied in Nintendo video consoles. One of the defendants was condemned to imprisonment; heavy fines were applied; and the payment of substantial damages was ordered.

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 video consoles. It did not condemn the perpetrators, but two years later, the Court of Appeals in Paris issued a guilty

[178] EWCA Crim. 2293 of November 3, 2009.
[179] EWHC 1932 (Ch) of July 28, 2010.
[180] The ruling was adopted in November 2009 by the Salamanca court. Its text has not been available. However, various reports have been published on it; e.g. on the *Techdirt* website on November 23, 2009 (which, of course, celebrated the ruling); at www.techdirt.com/blc.
[181] Decision of the Criminal Court of Palma de Mallorca, October 26, 2010.

verdict[182] imposing suspended imprisonment, high criminal fines and a big amount of damages.

In *Italy*, since the verdict of the Supreme Court (*Corte di Cassazione*) adopted in 2007[183] – confirmed by another one in 2011[184] –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 Tribunal of Milano (*Tribunale di Milano*) turned to the CJEU with a referral for preliminary ruling in the *Nintendo Co., Ltd and Others v PC Box Srl and 9Net Srl.* case.[185] It submitted the following two questions:

> 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?
>
> 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?

It is difficult to decipher the meaning of these complicated questions. Nevertheless, the first question seems to boil down to asking whether or not firmware TPMs are TPMs. In the light of the clear norms in the international treaties and in the *acquis communautaire*, the answer to this question will not be difficult. However, the second question is quite foggy. Does it seek to clarify whether or not it is allowed under Article 6(4) of the Directive to circumvent a firmware TPM if the device in which it is included may be used not only for illegal activities but also for some legal activities? Hopefully, it will be helpful for the CJEU that now the majority of EU courts answer with a healthy "No" to this question no matter whether it is put in such a complicated way or in a simpler manner.

It is worthwhile quoting Recital (48) of the Directive mentioned in the referral (but, since it begins with the words "such legal protection," together with Recital (47)):

> (47) Technological development will allow rightholders to make use of technological measures designed to prevent or restrict acts not authorised by the rightholders of any copyright, rights

[182] Decision of September 23, 2011 of the Court of Appeal.
[183] Cass. penale 33768/07.
[184] Cass. penale 8791/11.
[185] CJEU case C-355/12.

> related to copyright or the sui generis right in databases. The danger, however, exists that illegal activities might be carried out in order to enable or facilitate the circumvention of the technical protection provided by these measures. In order to avoid fragmented legal approaches that could potentially hinder the functioning of the internal market, there is a need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect.
>
> (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.

In the last-but-one sentence of Recital (48) on which the Milan court seems to concentrate in a somewhat isolated way, two principles may be found.

The first principle is proportionality which is, of course, as a basic principle should be taken into account. 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* from the viewpoint of 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.

The second principle is that devices or activities that have a commercially significant purpose or use other than to circumvent TPMs should not be prohibited. The calculation of the significance of this principle concerning the question of whether or not the manufacture and distribution of modchips may be considered legal is quite easy. The result is obviously: zero. The recital refers to 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 would apply. However, *modchips* are not such devices. Their exclusive purpose is circumventing firmware TPMs (irrespective of for what purposes the *consoles* concerned will then be used). The last- but-one sentence of Recital (48) has nothing to do with modchips.

SUMMARY

1. From the viewpoint of the application of the provisions of the WIPO „Internet Treaties," 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 individual customers of the cloud services (and, at maximum, to persons in their private sphere) or, in general, to the members of the public – normally at any place and at any time chosen by them.

2. 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 to the public – may be involved.

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

4. However, from the very beginning of legal disputes on this issue, it has been controversial whether, in a case mentioned in the preceding point, it is truly the customer who should be deemed to be the maker – or the only maker – of a "cloud copy." This is so since the copying system is under the control of the cloud provider and the copy normally stays in its infrastructure. There are countries under whose laws a private copying exception or limitation does not apply where a third person makes a copy for subsequent private use – 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 private copying exception or limitation and, thus, the exclusive right applies.

5. Where cloud providers make copies on the servers used by them, their acts are obviously covered by the exclusive right of reproduction. This may be the case also where, as a matter of "simplification," "rationalization" or some other reasons, 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 may be used by their customers.

6. Where, from a website in the "Cloud," works uploaded by the cloud provider 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. In such a case, the cloud provider must obtain license from the owners of rights.

7. The legal situation is less clear and more complex where the customers of a cloud service retrieve works from the cloud provider's servers in the form of either streaming or downloading – in principle from any place and from any time chosen by them. Even where they 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 to a copy or copies made by the cloud provider.

8. 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 a 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 the infringing materials and/or actively promote certain infringing contents or activities.

9. It is recognized as a basic obligation of cloud providers – as also of any other hosting providers – that they must act promptly to remove or block access to infringing copies when they receive notice or get red-flag knowledge about infringements.

10. General monitoring obligations may not be prescribed under current legislative norms. In contrast, it is allowed and justified to obligate cloud providers to apply reasonably targeted monitoring (filtering) systems to block uploading infringing copies of works that have already been identified as such, in particular in a notice-and-take down procedure. In such cases, the principle that what has been duly taken down should stay down should prevail.

11. 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, special considerations may be necessary as regards private copying exceptions or limitations. The basis for the application of private copying levies for copies in the "Cloud" may shrink and fade away.

12. The principle of exhaustion of rights is not applicable when intangible copies are downloaded from the "Cloud." In such cases, the right of making available to the public may be applied by being characterized as distribution (in the form of distribution through reproduction through transmission). However, the acts do not cease to be covered by the right of making available to the public in the case of which no exhaustion applies. Where it is alleged that a "used" intangible copy of a work is uploaded to a cloud website to offer it to be downloaded from there, in fact, 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.

13. 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 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.

14. Cloud-based business models guaranteeing adequate and effective but still flexible and well-balanced exercise of copyright frequently use firmware TPMs in devices through which protected works may be used in a duly controlled way ensuring a normal exploitation of works. Firmware TPMs are protectable TPMs without any doubt whatsoever. The reason for which it is justified to pay special attention to them 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 to obtain legalization of manufacturing and distributing of devices to circumvent such TPMs with reference to marginal conveniences they might create. At present, the attacks are directed mainly against firmware TPMs used in video consoles where mainly (but far from only) the game industry is concerned. The objective is legalizing the use of "modchips" to circumvent firmware protection which then 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. The more so since, as an agreed statement adopted concerning the relevant provisions of the BTAP has also made it clear, the three-step test is supposed to control not only what exceptions and limitations may be applied but also the possible measures taken for the applicability of certain exceptions and limitations in those cases where TPMs are used by owners of rights.

-.-.-.-.-.-.-.-