ALAI Conference, October 2012, Kyoto

The right of communication to the public in the cloud: An EU perspective

Estelle Derclaye*

Contents

Introduction

This paper examines the law relating to the right of communication to the public with reference to cloud storage and retrieval. It does so under the WIPO Internet treaties and EU statutory and case law, with some references to Member State statutory and case law when relevant. It focuses therefore on the liability of the cloud computing provider and the user for communication to the public, which, according to the law, includes making protected content available to the public. I leave aside the private international law issues as they are addressed by other speakers.

I. The legal framework

A. Statutory law

This section details the relevant provisions which may apply in a scenario where the cloud computing provider and/or the user communicate copyright-protected content to the public. The two WIPO Internet Treaties of 1996 provide for a right of communication to the public which includes a right of making works and other protected subject-matter available.

Article 8 of the WIPO Copyright Treaty - Right of Communication to the Public

"Without prejudice to the provisions of Articles 11(1)(ii), 11*bis*(1)(i) and (ii), 11*ter*(1)(ii), 14(1)(ii) and 14*bis*(1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them."

The WPPT provides the same right for performers and producers of phonogram producers (art. 10 and 14 WPPT).

This text is reproduced almost word for word in article 3 of the EU's InfoSoc Directive[1] which implements the WCT and WPPT and it also gives the right to producers of first fixations of films and broadcasting organisations.

Communication to the public means communication to the public to an audience which is not present at the place of origin.[2] In the case of cloud computing, this is always the case: the provider, the users and the public are all in different locations. I exclude cloud computing which is done internally by an organisation and which only uses the facilities for its internal purposes so never communicates anything outside its 'walls'/personnel. This is because this type of communication does not involve any public and also because the most common type of cloud computing nowadays is by definition outside the control of the user.

As to enforcement, article 8(3) InfoSoc Directive provides that "Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right". This allows right holders to sue the cloud computing provider and require the court to order him to stop the third party infringement.

As cloud computing providers host content, articles 14 and 15 of the E-Commerce Directive (ECD)[3] are also relevant as they establish safe harbours for hosting and prohibit Member States from obliging hosts to monitor content generally.

"Article 14 - Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

---

* Professor of Intellectual Property Law, University of Nottingham. Unless otherwise stated, the quotations from the literature are cited without the footnotes.

[1] 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, OJ L 167, 22/06/2001, p. 10-19 (further referred to as InfoSoc Directive).

[2] See e.g. S. von Lewinski, *International Copyright Law and Policy*, Oxford University Press, 2008, p. 148, no. 5.138 and CJEU case law, see below.

[3] Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1.

(a) 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

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15 - No general obligation to monitor

1. 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.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."

Recitals 42, 43, 44, 47 and 48 ECD are also relevant.

"(42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

(43) A service provider can benefit from the exemptions for "mere conduit" and for "caching" when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission.

(44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of "mere conduit" or "caching" and as a result cannot benefit from the liability exemptions established for these activities.

(47) 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.

(48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities."

Finally, some articles of the Enforcement Directive[4] are also relevant:

"Article 3 - General obligation

1. Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.

2. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.

Article 8 - Right of information

1. Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who:
(a) was found in possession of the infringing goods on a commercial scale;
(b) was found to be using the infringing services on a commercial scale;
(c) was found to be providing on a commercial scale services used in infringing activities;
or
(d) was indicated by the person referred to in point (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services.

2. The information referred to in paragraph 1 shall, as appropriate, comprise:
(a) the names and addresses of the producers, manufacturers, distributors, suppliers and other previous holders of the goods or services, as well as the intended wholesalers and retailers;
(b) information on the quantities produced, manufactured, delivered, received or ordered, as well as the price obtained for the goods or services in question.

3. Paragraphs 1 and 2 shall apply without prejudice to other statutory provisions which:
(a) grant the rightholder rights to receive fuller information;
(b) govern the use in civil or criminal proceedings of the information communicated pursuant to this Article;
(c) govern responsibility for misuse of the right of information;
or

[4] Directive 2004/48 of the European Parliament and of the Council of 29 April 2044 on the enforcement of intellectual property rights, OJ L 157, 30.4.2004, and corrigendum OJ L 195, 02/06/2004, p. 16-25 (further referred to as Enforcement Directive).

(d) afford an opportunity for refusing to provide information which would force the person referred to in paragraph 1 to admit to his/her own participation or that of his/her close relatives in an infringement of an intellectual property right;
or
(e) govern the protection of confidentiality of information sources or the processing of personal data.

Article 9 - Provisional and precautionary measures

1. Member States shall ensure that the judicial authorities may, at the request of the applicant:

(a) issue against the alleged infringer an interlocutory injunction intended to prevent any imminent infringement of an intellectual property right, or to forbid, on a provisional basis and subject, where appropriate, to a recurring penalty payment where provided for by national law, the continuation of the alleged infringements of that right, or to make such continuation subject to the lodging of guarantees intended to ensure the compensation of the rightholder; an interlocutory injunction may also be issued, under the same conditions, against an intermediary whose services are being used by a third party to infringe an intellectual property right; injunctions against intermediaries whose services are used by a third party to infringe a copyright or a related right are covered by Directive 2001/29/EC;

(b) order the seizure or delivery up of the goods suspected of infringing an intellectual property right so as to prevent their entry into or movement within the channels of commerce.

2. In the case of an infringement committed on a commercial scale, the Member States shall ensure that, if the injured party demonstrates circumstances likely to endanger the recovery of damages, the judicial authorities may order the precautionary seizure of the movable and immovable property of the alleged infringer, including the blocking of his/her bank accounts and other assets. To that end, the competent authorities may order the communication of bank, financial or commercial documents, or appropriate access to the relevant information.

3. The judicial authorities shall, in respect of the measures referred to in paragraphs 1 and 2, have the authority to require the applicant to provide any reasonably available evidence in order to satisfy themselves with a sufficient degree of certainty that the applicant is the rightholder and that the applicant's right is being infringed, or that such infringement is imminent.

4. Member States shall ensure that the provisional measures referred to in paragraphs 1 and 2 may, in appropriate cases, be taken without the defendant having been heard, in particular where any delay would cause irreparable harm to the rightholder. In that event, the parties shall be so informed without delay after the execution of the measures at the latest.

A review, including a right to be heard, shall take place upon request of the defendant with a view to deciding, within a reasonable time after notification of the measures, whether those measures shall be modified, revoked or confirmed.

5. Member States shall ensure that the provisional measures referred to in paragraphs 1 and 2 are revoked or otherwise cease to have effect, upon request of the defendant, if the applicant does not institute, within a reasonable period, proceedings leading to a decision on the merits of the case before the competent judicial authority, the period to be determined by the judicial

authority ordering the measures where the law of a Member State so permits or, in the absence of such determination, within a period not exceeding 20 working days or 31 calendar days, whichever is the longer.

6. The competent judicial authorities may make the provisional measures referred to in paragraphs 1 and 2 subject to the lodging by the applicant of adequate security or an equivalent assurance intended to ensure compensation for any prejudice suffered by the defendant as provided for in paragraph 7.

7. Where the provisional measures are revoked or where they lapse due to any act or omission by the applicant, or where it is subsequently found that there has been no infringement or threat of infringement of an intellectual property right, the judicial authorities shall have the authority to order the applicant, upon request of the defendant, to provide the defendant appropriate compensation for any injury caused by those measures.

Article 11 - Injunctions
Member States shall ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC.

B. Case law

So far there is little EU case law on the important issue of the conditions of liability for Internet service providers (ISPs) and hosting sites (hosts) for copyright infringement. The questions referred to the Court of Justice of the European Union (CJEU) have only addressed these issues at the edges. It is not very surprising for three reasons: 1) ISPs and hosts rarely qualify for primary liability namely communication to the public/making available content protected by copyright and related rights 2) secondary liability is still governed by national law, and 3) ISPs and hosts often benefit from the safe harbours provided for in the ECD.

1. CJEU case law on copyright enforcement measures involving ISPs and hosts (Enforcement Directive and E-Commerce Directive)

The CJEU has shed light on two separate but related issues concerning copyright enforcement, which have a link with the communication right among others. First, ISPs and by analogy host sites may be forced to disclose the identities (name and address) of alleged infringers to right holders so that they can commence civil proceedings. In *Promusicae*[5] and *Bonnier*[6], the Court of Justice ruled that the combined interpretation of the EU Charter of

[5] *Promusicae v Telefonica*, Case C-275/06, [2008] ECR I-271. In that case, Promusicae (which represents producers and publishers of musical and audiovisual recordings in Spain) asked Telefonica (an ISP) to disclose the identities of customers who they suspected were sharing copyright works via the P2P software Kazaa. It asked for this information so that it could commence civil proceedings against those individuals. The national court referred a question to the CJEU.

[6] *Bonnier et al. v Perfect Communication Sweden AB*, Case C-461/10, 19 April 2012, available on www.curia.europa.eu The CJEU held that the national (Swedish here) law in question respects, in principle, the principle of proportionality and strikes a fair the balance between the protection of personal data and the protection of copyright.

Fundamental Rights, the several 'privacy/data protection' directives, the InfoSoc Directive and the Enforcement Directive allows but does not force Member States to take measures so that such intermediaries are obliged to give right holders personal information of clients who are suspected of copyright infringement. When Member States do so, the Court said that EU law obliges them to ensure a fair balance is struck between the several human rights at stake, namely the right of property of the copyright holders and the right to private life of the subscribers in this case. The Member States must also respect the principle of proportionality in their implementation of those directives.

Second, ISPs and hosts may be forced to filter content in some cases. In *Scarlet v SABAM*[7] and *SABAM v Netlog*[8], the questions asked by the Belgian courts to the CJEU were: may a Member State's court order an ISP (Scarlet) or a host (Netlog, a social network site) to put in place in respect of all its clients, in abstracto and preventively, at its exclusive charge and without time limitation, a system filtrating all its communications in order to identify files protected by copyright (namely audiovisual and musical works) and block their transfer?

As the injunction's characteristics would oblige ISPs to check all communications of all their users, identify files with protected works, determine if they were shared unlawfully and block the files (in short it would amount to perpetual, systematic and universal filtering), such court order would infringe two fundamental freedoms: the ISP's freedom to conduct business as it would have to install a costly, complicated and permanent computer system at its own cost and freedom of information as such filtering could block lawful content. It would also breach article 15 ECD (no general obligation to monitor) and article 3 of the Enforcement Directive which calls for equitable and proportionate measures. So in sum, in addition to the right holder's right to property, the right of ISPs and host sites to conduct a business and the right of subscribers to impart and receive information should also be taken into account when this balance between the three parties is struck.

In *L'Oréal SA v eBay*, which dealt with the unauthorised sale on eBay (the famous online marketplace) of L'Oréal products by eBay users, the CJEU ruled that right holders may also ask injunctions to prevent *future* infringements.[9] However, similarly to what the CJEU had said in *Scarlet* and repeated later in *Netlog*, right holders cannot ask an injunction so that the online provider actively monitors "all the data of each of its customers in order to prevent any future infringement of intellectual property rights via that provider's website".[10] This would breach article 15 ECD and 3 of the Enforcement Directive. All we therefore know is that a permanent order to filter all communications of an ISP's or of a host's users does not strike a fair balance between all the parties' fundamental rights. It may therefore mean that a special obligation to monitor is not ruled out (as recital 47 of the Infosoc Directive itself suggests) but to know the conditions, we would need a new CJEU decision. An indirect answer to this question should be given soon as an Austrian court has recently referred several questions to the CJEU, one of them asking whether it is compatible with EU law to require an access provider to take specific measures to make it more difficult for its customers to access a website containing material made available unlawfully if those measures require not inconsiderable costs and can easily be circumvented without any special technical knowledge. Whereas it does not concern filtering users' communications as such, it involves

[7] Case C-70/10 (2012), available on www.curia.europa.eu
[8] Case C-360/10 (2012), available on www.curia.europa.eu
[9] Case C-324/09 *L'Oreal SA v eBay* [2011] E.C.R. I-000, para. 131, available on www.curia.europa.eu (interpreting article 11 of the Enforcement Directive). The case involved trademark infringements.
[10] Ibid., para. 139.

a specific measure, namely the blocking of the access to a web site, which, unlike the filtering of all communications, does not involve inconsiderable costs.[11]

In addition to the two issues above mentioned, in *Google France v Louis Vuitton et al.*, the CJEU interpreted article 14 ECD for the first time.[12] Like in *L'Oréal v eBay*, the case did not concern copyright but trademarks, more particularly the system Google uses to reference web pages (Google search engine) along with its AdWords (advertisements which appear on the right hand side column of a web page next to the search results).[13] This activity is not properly what a cloud computing provider generally does (as they generally only provide storage) but the ruling is interesting for our purposes as the Court interpreted the general meaning of article 14 ECD. The French Supreme Court asked the CJEU whether article 14 ECD "is to be interpreted as meaning that an internet referencing service constitutes an information society service consisting in the storage of information supplied by the advertiser, with the result that that information is the subject of 'hosting' within the meaning of that article and that the referencing service provider therefore cannot be held liable prior to its being informed of the unlawful conduct of that advertiser."[14] After establishing that the referencing system is an information society service within the meaning of the ECD, the CJEU held that article 14's safe harbour applies only in "cases in which the activity of the information society service provider is 'of a mere technical, automatic and passive nature', which implies that that service provider 'has neither knowledge of nor control over the information which is transmitted or stored'".[15] In other words, the question is whether the ISP's role is neutral. Google plays an active role as it does choose the ranking of the results[16] and its role "in the drafting of the commercial message which accompanies the advertising link or in the establishment or selection of keywords is relevant."[17] Therefore, the CJEU ruled

[11] See *UPC Telekabel Wien*, Case C-314/12, available on www.curia.europa.eu. The questions are as follows: "1. Is Article 8(3) of the [Infosoc] Directive to be interpreted as meaning that a person who makes protected subject matter available on the internet without the right holder's consent is using the services of the access providers of persons seeking access to that protected subject matter?
2. If the answer to the first question is in the negative, are reproduction for private use and transient and incident reproduction permissible only if the original reproduction was lawfully reproduced, distributed or made available to the public?
3. If the answer to the first and second question is in the affirmative, and an injunction is therefore to be issued against the user's access provider in accordance with Article 8(3) of the Directive, is this compatible with Union law, in particular with the necessary balance between the parties' fundamental rights?
4. If the answer to the third question is in the negative, is it compatible with Union law to require an access provider to take specific measures to make it more difficult for its customers to access a website containing material made available unlawfully if those measures require not inconsiderable costs and can easily be circumvented without any special technical knowledge?"

[12] *Google France v Louis Vuitton et al.*, Joined Cases C-236/08 to C-238/08 (2010), available on www.curia.europa.eu, paras 106-120. See for a comment Francesco Rizzuto, "The liability of online intermediary service providers for infringements of intellectual property rights" [2012] *Computers and Telecommunications Law Review*, p. 4.

[13] The CJEU gives an explanation of how AdWords work at para. 23 of judgment.

[14] *Google France*, above n. 12, para. 106.

[15] Ibid., para. 113: "it follows from recital 42 in the preamble to Directive 2000/31 that the exemptions from liability established in that directive cover only cases in which the activity of the information society service provider is 'of a mere technical, automatic and passive nature', which implies that that service provider 'has neither knowledge of nor control over the information which is transmitted or stored'."

[16] Ibid., para. 115: "Google determines the order of display according to, inter alia, the remuneration paid by the advertisers."

[17] Ibid., para 118.

that article 14 ECD applies when the provider does not play "an active role of such a kind as to give it knowledge of, or control over, the data stored."[18]

What are the implications of this case law for cloud computing providers? If a user is infringing by communicating protected content to the public on a cloud computing provider's storage platform, right holders may use the notice and take down system in article 14 ECD against the cloud computing provider. In addition, they may also try to obtain an injunction against the cloud computing provider, but probably only against a specific act of a particular client (implicitly as per *Scarlet* and *Netlog*). The cloud computing provider will then have to block the infringing content posted by that user, arguably also for the future (as per *L'Oréal*). The question however poses itself whether national courts have to strike the balance between the different fundamental rights of the three stakeholders in all the cases where a permanent general injunction is not requested. It is not clear from *Scarlet* and *Netlog* whether the balance is only upset in case of such permanent general injunctions or may be upset in the case of certain specific injunctions. Arguably, national courts will be able to strike this balance without referring a question to the CJEU if they think that a specific injunction may in a specific case be too burdensome for the host or would encroach on freedom of expression.

It is unclear whether the *L'Oréal* decision means that courts can issue stay-down orders, and if so of which type. Recently, the French Court of Cassation held that such stay-down orders cannot be ordered against hosts (in this case Google).[19] Stay-down orders are those which oblige the host to prevent further postings of the same protected content if the right holder has already notified the host once about it. This is so even if the host has not been notified that the removed content has once again been re-posted. In short, one original notification is sufficient. The Court of Cassation held that a stay-down order imposes a general duty to monitor and thus goes against article 15 ECD. For the Court, such order obliges Google to block the content for an unlimited period of time and is a disproportionate measure in relation to the objective pursued. *L'Oréal* probably means that stay-down orders are not acceptable because if the host receives even just one notification for each customer in relation to one copyright work, it would have to check all postings of all its customers all the time to see if they do not re-post infringing content. Since URLs can change, if right holders are not obliged to further notify the host, it may in some cases put a heavy burden on the hosts' shoulders to identify the location of the content. In addition, as the Court said in *L'Oréal*, the measures cannot create barriers to legitimate trade and the ruling implies that the operator is not obliged to monitor the content notified which re-appears on its web site, as the Court says that "if the operator of the online marketplace does not decide, on its own initiative, to suspend the perpetrator of the infringement of intellectual property rights in order to prevent further infringements of that kind by the same seller in respect of the same trade marks, it may be ordered, by means of an injunction, to do so".[20] This also implies that the suspension

[18] Ibid., para 120: "It follows that the answer to the third question in Case C-236/08, the second question in Case C-237/08 and the third question in Case C-238/08 is that Article 14 of Directive 2000/31 must be interpreted as meaning that the rule laid down therein applies to an internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned."

[19] Cass. 12 July 2012, 1st ch. civ., *Aufeminin.com v. Google France*, available at http://www.courdecassation.fr/jurisprudence_2/premiere_chambre_civile_568/827_12_23881.html (photograph appearing and re-appearing again on Google Images).

[20] *L'Oréal*, above n. 9, paras 140-141.

of a user's account is a proportionate measure. So a host could be obliged to suspend or even maybe terminate a repeat infringer's account or at least warn them their account will be terminated if the host carries on receiving notifications from right holders, along the lines of the system of the 'three strikes and you're out' in place in France.[21] This system obliges ISPs to notify users who the right holders suspect of file-sharing that their account will be terminated if they carry on file-sharing despite 3 warnings. This type of measure (suspension) is probably proportionate and thus respects article 3 of the Enforcement Directive. Some hosts have indeed already written this type of measure in their contract terms.[22] So in effect, they already anticipate this problem and it should not pose itself too often. Nevertheless, *L'Oréal* is not entirely clear on the legitimacy of stay-down orders and a reference to the CJEU would help clarify the matter.

2. CJEU case law on communication to the public including making available to the public

More cases concerning the right of communication to the public were referred to the CJEU over the years. Most of the time they interpreted article 3 of the InfoSoc Directive but sometimes they involved articles 8 and 10 of the Rental and Lending Directive.[23] The cases involved distributing television signals in hotels generally (*SGAE*[24]), providing, in the hotel's bedrooms, apparatus (other than televisions and radios) and phonograms in physical or digital format so that the guests can hear them by means of the apparatus (*Phonographic Phonographic Performance (Ireland) Ltd v Ireland*[25]), transmitting broadcast works, via a television screen and speakers, in a pub (*Football Association Premier League*[26]) and distributing radio signals (music) in a dental practice (*Società Consortile Fonografici* (*SCF) v. Marco Del Corso*[27]).

Importantly, in the latter case, the Court held that "the concepts appearing in Directives 92/100 and 2001/29, such as 'communication to the public' must be interpreted in the light of

[21] HADOPI 1, i.e. Law n° 2009-669 favouring the diffusion and protection of creations on the Internet of 12 June 2009 and HADOPI 2, i.e. Law n° 2009-1311 of 28 October 2009 concerning the criminal protection of literary and artistic property on Internet, available on www.legifrance.gouv.fr. The UK's Digital Economy Act (« DEA ») of 8 April 2010, available on http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1, establishes a similar system but is not yet in force.

[22] See below YouTube and Facebook.

[23] Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, OJ 2006 L 376, p. 28 (further referred to as Rental and Lending Directive).

[24] Case C-306/05, *Sociedad General de Autores y Editores de España (SGAE) v. Rafael Hoteles SA* [2006] E.C.R. I-11519 (art. 3 Infosoc Directive). Similar facts arose in a prior case, namely Case C-293/98, *Entidad de Gestión de Derechos de los Productores Audiovisuales (EGEDA) v. Hosteleria Asturiana SA (Hoasa)* [2000] E.C.R. I-0629, before the adoption of the Infosoc Directive. However, as the Satellite and Cable Directive did not enable the Court of Justice to answer the question and only national law applied, the court could not and did not in effect rule on the substance.

[25] Case C-162/10, 2012, available on www.curia.europa.eu (reference to interpret Articles 8 and 10 of Directive 2006/115), further referred to as *PPL*.

[26] Joined Cases C-403/08 and C-429/08, *Football Premier League v. QC Leisure and Karen Murphy v. Media Protection Services* [2012] F.S.R. 1 (the question was "whether 'communication to the public' within the meaning of Article 3(1) of the Copyright Directive must be interpreted as covering transmission of the broadcast works, via a television screen and speakers, to the customers present in a public house"), paras 183-207. The case is further referred to as *FAPL*.

[27] Case C-135/10, 2012, available on www.curia.europa.eu. Reference to interpret both art. 8(2) of the old Rental and Lending Directive (Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, OJ 1992 L 346, p. 61) and art. 3 Infosoc Directive. Note that the dentist was providing the radio signals free of charge and without any active choice on the part of his patients.

the equivalent concepts contained in those international agreements and in such a way that they are compatible with those agreements, taking account of the context in which those concepts are found and the purpose of the relevant provisions of the agreements as regards intellectual property."[28] The Court also refers to the definition of communication to the public in the WIPO Glossary of Terms of the Law of Copyright and Neighbouring Rights, which is not legally binding: "making a work, performance, phonogram or broadcast perceptible in any appropriate manner to persons in general, that is, not restricted to specific individuals belonging to a private group."[29] So it is clear that the CJEU firmly thinks that the WIPO treaties are crucial to interpret the concept of communication to the public in the EU legal order.

The InfoSoc Directive does not define 'communication to the public' but the CJEU held that apart from having to be interpreted in conformity with international law, the term must, according to recital 23 of the Infosoc Directive, also be interpreted broadly. To determine whether the acts in all these cases were communications to the public, the Court elaborated several factors: 1) public means an "indeterminate number of potential [television] viewers or [radio] listeners"[30] and a "fairly large number of people" 2) the public must be a new public i.e. "different from the public at which the original act of communication of the work is directed"[31], 3) the public must be targeted and receptive, 4) the public is present at the place of the operator's (hotel, pub, dentist) transmission, but is not present at the place where the communication originates, that is to say, at the place of the representation or performance which is broadcast[32], 5) the operator is intentionally distributing the works i.e. without the intervention of the hotel, pub or dentist, this new public cannot receive the signals,[33] and 6) the operator's communication is for profit (e.g. the hotel renders an additional service when communicating works to its clients and profits from it; the hotel's action is an additional service which has an effect on the standing of hotel and price of rooms and is likely to attract more guests).

Several factors are irrelevant: 1) whether the customers have or not switched the television or radio on - it is sufficient that the apparatus and the signal or protected content are provided (art. 3 Infosoc and art. 8 WCT say "in such a way that the persons forming that public *may*

[28] *SCF*, above n. 27, para. 55. See also para. 71.
[29] *SCF*, above n. 27, para. 85.
[30] In the several cases, the Court refers to its previous rulings in *Lagardère* (Case C-192/04 [2005] E.C.R. I-7199) and *Mediakabel* (Case C-89/04 [2005] E.C.R. I-4891) to say the notion of public refers to an indeterminate number of potential television viewers. In *SCF*, the court says "[a]s regards [...] the 'indeterminate' nature of the public, the Court has observed that, according to the definition of the concept of 'communication to the public' given by the WIPO glossary, which, while not legally binding, none the less sheds light on the interpretation of the concept of public, it means 'making a work … perceptible in any appropriate manner to persons in general, that is, not restricted to specific individuals belonging to a private group'."
[31] "When those authors authorise a broadcast of their works, they consider, in principle, only the owners of television sets who, either personally or within their own private or family circles, receive the signal and follow the broadcasts." *FAPL*, above n. 26, para. 198. In *PPL*, the court added on this factor that the hotel derives economic benefits from the transmission independent of those obtained by the broadcaster or producer of phonogram.
[32] *FAPL*, above n. 26, para. 203.
[33] In *PPL*, the Court refers to *SCF* and says at para. 30: "The user makes an act of communication when it intervenes, in full knowledge of the consequences of its action, to give access to a broadcast containing the protected work to its customers. In the absence of that intervention, its customers, although physically within the area covered by the broadcast, would not, in principle, be able to enjoy the broadcast work (*SCF*, paragraph 82)." Emphasis added. Same wording at para 42 of *SGAE*: "the hotel is the organisation which intervenes, in full knowledge of the consequences of its action, to give access to the protected work to its customers".

access it"[34]), 2) which technique is used to transmit the signal and 3) whether the place where the communication takes place is private or public.[35] Last but not least, the mere provision of physical facilities is not a communication to the public.[36]

In all the cases before the CJEU, the operator was providing the apparatus on which to view or hear the content (television, radio etc) and the content or signal enabling the content to be viewed and/or heard. The factors were met in the hotel and pub cases but factors 3 and 6 were not fulfilled in the dentist case. In addition, in the *SCF* and *PPL* cases, the Court of Justice held that the concept of communication to the public requires individual assessment.[37] The court carries on saying that "for the purposes of such an assessment, account has to be taken of several complementary criteria, which are not autonomous and are interdependent. Consequently, they must be applied individually and in their interaction with one another, given that they may, in different situations, be present to widely varying degrees (see *SCF*, paragraph 79)."[38] Nevertheless, then the Court assesses the concept of communication to the public with the same factors as under article 3 InfoSoc Directive, i.e. those mentioned just above.[39] So is the concept of communication to the public different in the Rental and Lending Directive and the Infosoc Directive?[40] It does not seem it is, at least at the moment, as the Court used the same criteria in all the communication to the public cases. However, it left itself the possibility of crafting a broader concept in relation to article 3 Infosoc Directive than to article 8 of the Rental and Lending Directive.[41] Depending how the Court would differentiate between authors on the one hand and performers and broadcasting organisations on the other, the Court will have to respect international conventions. So for instance, as per the Convention and the Rental and Lending Directive, it may restrict the broadcasting organisations' right to the showing of television programmes in places made accessible to the public only if the defendant does so against payment of an entrance fee.[42]

If we apply these factors to hosts, it seems clear a priori that they merely provide the facilities (storage, web site) but not the content. The content is provided by the users. However, if there is doubt as to whether the content is really only provided by the user, i.e. that the cloud computing provider intervenes in some way, all the other factors listed above are generally fulfilled and the case law would apply. Because of the rather simple nature of the facts of the cases referred to the CJEU, the case law does not envisage many types of involvement the operator or intermediary can have. But UK courts for instance have further elaborated on this concept.

---

[34] Emphasis added.

[35] According to art. 3 Infosoc Directive and 8 WCT. So the private nature of hotel rooms does not preclude the communication of copyright protected works from being public.

[36] This also appears in the agreed statement on article 8 WCT. See http://www.wipo.int/treaties/en/ip/wct/statements.html See also J. Reinbothe and S. von Lewinski, *The WIPO Treaties 1996: The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, Commentary and Legal Analysis*, Butterworths, London, 2002, p. 112, who add that the term 'mere' "means that this exclusion from the act of communication must be interpreted restrictively".

[37] See para. 29, *PPL* n. 25 above and para. 78, *SCF* n. 27 above.

[38] *PPL*, para 30.

[39] *SCF*, para 92. Ibid. in *PPL*.

[40] Alexander Ross and Claire Livingstone, "Communication to the public: Part 2" (2012) 23 (7) Entertainment Law Review 209-213, at 213, think not.

[41] The Rental and Lending Directive only concerns the performers' and broadcasting organisations' right of communication to the public.

[42] Art. 13 Rome Convention and art. 8(3) Rental and Lending Directive.

UK courts have generally followed the EU case law on the communication to the public by the letter.[43] However, in *Newzbin 1*[44], the High Court of England and Wales held that Newzbin itself, a website on a worldwide Internet discussion system called Usenet, was liable for infringement of the right of communication to the public, and not only the users who were uploading films on Newzbin. The report of the case summarises well how the site works so that the relevant passage can simply be quoted:
"In relation to binary (i.e. non-text) content, Newzbin provided premium members with a facility which extended considerably beyond indexing and categorisation. It identified all (or in the case of the RAW index, many) of the, perhaps several thousand, messages which made up a particular binary work and, in so doing, saved those members the very substantial task of manually locating and identifying each of them separately. Moreover, the reports in the Newzbin index provided a considerable body of very useful information in relation to each title. They included descriptive information, the URL and an NFO file which identified the individual user who posted the content to Usenet, the email address of that user, information from which the date on which the content was posted to Usenet could be deduced and the number of files making up the particular work. Newzbin also provided the "NZB" facility. Upon the press of a button, this system created an NZB file which was delivered to the member's computer where it could be stored. When run by the member it caused the news client to fetch all of the Usenet messages and reassemble the original binary work from its component parts and so, in the case of a copyright work, inevitably make an infringing copy. Once a work had been entered onto the defendant's Newzbin index, use of the NZB facility was bound to result in that work being copied."[45]

The court ruled that the factors were fulfilled. First, the site was for profit as the users had to pay a membership fee, Newzbin was not passive because it did not simply provide a link to sites where illegal copies of films were available, it provided an indexing and cataloguing system and the NZB facility to download the films at the press of a button allowed users to avoid "days of (potentially futile) effort in seeking to gather those messages together for themselves".[46] The users were a new public and Newzbin provided the service in full knowledge of the consequences of its actions.[47] The court does not discuss factors 1, 3 and 4 but they were obviously fulfilled in this case.

The facts are different from those in question in the CJEU case law because Newzbin did not store nor transmit the protected content. So the decision arguably goes beyond the CJEU's case law because in the facts before the Court of Justice, the hotel or pub provided the apparatus (TV, radio or other device) and the signal or the DVD or CD to its guests. As Ross and Livingstone say, "[u]ntil this [*Newzbin*] decision it was generally thought that a finding of infringement by way of CTTP required the defendant itself to store and make available the content. The case made clear that an intervention to assist in the process of transmission can also amount to CTTP. ... In *Newzbin*, the users would still have been able to access the content absent the Newzbin website, but with greater difficulty - the Newzbin software made

[43] The relevant case law is constituted basically by *Newzbin I* (see below) and *Dramatico et al. v British Sky Broadcasting et al.* [2012] EWHC 268 as the CJEU has not yet ruled in *ITV Broadcasting v TV Catch Up*, Case C-607/11, available on www.curia.europa.eu. See Ross and Livingstone above n. 40. The exception so far is the ruling in *FAPL* on remand because it goes further and also adds that there is a performance in public in addition to a communication to the public.
[44] *Twentieth Century Fox Film Corp v Newzbin* [2010] FSR 512.
[45] Ibid., at 513-514.
[46] Ibid., paras 118 and 125 of the judgment.
[47] Ibid.

the location and access to the content considerably easier. The judgment therefore takes the CTTP concept a stage further than *Rafael*."[48]

3. Relationship between the case law on the host's safe harbour provision and on the right of communication to the public

There is convergence between the EU case law on article 14 ECD on the one hand and on the right of communication to the public on the other. Under the right of communication to the public case law, the role of the operator must be that it intervenes to give access to the content in full knowledge of the consequences of its actions. Under article 14 ECD case law, to benefit from the safe harbour, the provider's role must be 'of a mere technical, automatic and passive nature', which implies that that provider 'has neither knowledge of nor control over the information which is transmitted or stored'. In other words, the question is whether the ISP's role is neutral. Arguably, intervention with knowledge on the one hand and having an active role or controlling on the other, are the same thing.

There may also be convergence between the CJEU case law and the secondary liability case law at national level. While this is beyond the scope of this paper, it is an issue worth looking into though as it may be that through the interpretation of article 14 ECD and 3 InfoSoc Directive, the CJEU is in fact harmonising (part of) of the national law on secondary liability by the back door.

In the following section, the above case law is applied to scenarios involving several possible activities of cloud computing providers.

II. Scenarios

There are several variables: type of

1) person involved: the cloud provider (private, public, hybrid cloud), the user (client of the cloud computing provider), the audience (the public)
2) copyright work or subject-matter protected by related rights including database *sui generis* right: generated by user, a third party, the cloud computing provider or derivative
3) act: public or private storage (hosting) or retrieval

First, by public, private and hybrid cloud, I refer to the public or private nature of the communication made via the cloud. If content stored on the cloud is accessible not only to the user who has contracted with the cloud computing provider but also to the wider world, then it is a public cloud and vice versa. A hybrid cloud is a cloud where some parts of the content stored in the cloud are available only to the user and its organisation, friends, family and part of the content stored is available to the public. The definition therefore used in this paper

[48] Ross and Livingstone, above n. 40, at 211. Note that CTTP = communication to the public. See also Maurizio Borghi, "Chasing copyright infringement in the streaming landscape" [2011] IIC, p. 320: "For instance, in *Twentieth Century Fox Film Corp v. Newzbin Ltd*, a UK court, referring to the CJEU decision in *SGAE v. Rafael Hoteles SA*, found that an infringement of the public communication right occurs by merely providing of access to otherwise inaccessible protected works, *regardless of whether the act of providing access* (by means of a cataloguing and indexing system) *is merely "passive" and does not engage in any actual transmission of the content to users*" (emphasis added).

should not be confused with the National Institute of Standards and Technology's definitions of public, private and hybrid clouds and other similar definitions.[49]

The question is when the cloud computing provider is liable for communication to the public and is twofold: when are cloud computing providers liable under article 14 ECD and does the communication to the public case law apply to them as well? As to the latter, first, virtually all cloud computing providers will be profit-making so that this factor is met. Second, it of course depends if the content that is stored is communicated to the public. But most importantly, one needs to see if the situation of a host or cloud computing provider is similar to that of a hotel or pub. Like hotels and pubs, host sites provide a web site or storage space ('apparatus') where users can upload content. However, they do not provide the signal, that's the ISP, nor the content, that's the users themselves. The simple provision of apparatus (for host sites the web site and software to upload content) without the content is not making the provider liable. But is this what the host or cloud computing provider is always doing? It depends on their (degree of) involvement. The scenarios below give answers to these questions under both article 14 ECD and the communication to the public case law. I have chosen some of the most well-known and most used types of cloud computing providers as examples.

A. Scenario 1 – 'private cloud' (e.g. email service, music locker)

(1) If the cloud computing service is private e.g. an email service or music locker, it does not mean that all is private and that neither the user nor the host is communicating anything to the public. If the user only emails works generated by himself or only listens to his own music alone (in private), then nothing is public and there is no communication to the public. However, a user could use his music locker to animate a party or email third party or derivative copyright works to a vast number of people. These are communications to the public made by the user as the conditions of CJEU case law on the communication to the public right are fulfilled. Unless the user is sheltered by an exception (e.g. educational use, parody...), the user infringes the communication to the public right.

As to the cloud computing provider (host), it is debatable whether factors 5 and 6 of the EU communication to the public case law (intervention and profit) are fulfilled. Indeed, without

[49] "The National Institute of Standards and Technology has determined four different cloud computing deployment models: private cloud, community cloud, public cloud and hybrid cloud.
Private cloud: The cloud infrastructure is obtained for private use by a single organisation, whether managed internally or by a third party hosted internally or externally.
Community cloud: The cloud infrastructure is provided for exclusive use by a specific community of consumers from organisations 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 organisations in the community, a third party or some combination of them, and it may exist on or off premises.
Public cloud: This is the most popular cloud computing model as it is available for open use by the general public. Here the cloud infrastructure is owned and operated by a third party, who provides cloud computing services to multiple clients (individuals or corporations) generally on a pay as you use model. This is the most preferred model as it provides computing services at the lowest cost, which is favourable for individuals and small business organisations.
Hybrid cloud: The hybrid cloud computing model is a combination of other cloud models (private, community or public), and this method is most commonly a cloud within a large organisation. An organisation may use a private cloud storage provider in the case of sensitive/proprietary data in order to have total control over them, or a public cloud storage provider in the case of less sensitive data. In simple terms, a hybrid cloud infrastructure is a combination of two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability." See Naqeeb Ahmed Kazia, "An overview of cloud computing and its legal implications in India" [2012] *Computers and Telecommunications Law Review* 47, at 49.

the site, the user could not communicate the works at his party in that form or *as easily* anyway. So factor 5 could arguably be fulfilled at least under *Newzbin*. As to factor 6, it may be said that the host site does not benefit from the communication in itself but isn't the question whether the *service* is for profit? Isn't the attraction or at least one attraction of these hosting platforms allowing the very possibility of using one's music locker at a party? The user can throw a party anywhere any time by just logging on the web. No need to transport all his or her music everywhere he goes; with the hosting site, it's always available everywhere, all of it in one place. This may be stretching it. Indeed, the cloud computing provider does not know what the user is going to do with the music. It differs from the pub owner or hotel. In any case, factor 3 will in all likelihood not be fulfilled as it is the user, not the host, who targets the audience. How about article 14 ECD? As we saw, article 14's safe harbour applies only in "cases in which the activity of the information society service provider is 'of a mere technical, automatic and passive nature', which implies that that service provider 'has neither knowledge of nor control over the information which is transmitted or stored', or in other words when the intermediary does not play "an active role of such a kind as to give it knowledge of, or control over, the data stored." Certainly in this situation, the cloud computing provider is just providing storage, its activity is passive. It does not know that the user is using the music to throw a party. So the cloud computing provider is sheltered by article 14 ECD.

(2) In a private cloud computing environment, the cloud computing provider could also communicate copyright works generated by the user, either intentionally or negligently for instance leaking the client's or third party protected content (emails or documents generated by the client or his or her music collection) stored in the cloud.[50] In this scenario, it is clear that under EU case law, the host communicates the work to the public. Article 14 ECD does not apply since it is clear that the host is active, even if as a result of a mistake or negligence. Of course, if there is a licence between the host and the user, no such infringement arises. Indeed, in some cases, the service agreement between the cloud computing provider and the user will say that the user transfers the copyright or gives the host a licence for all the content the user creates to the cloud computing provider. This is generally not the case for pure email accounts[51] but more often the case for other services such as social network sites, at least for most of the content posted.[52]

B. Scenario 2 – 'public cloud' (e.g. YouTube)

A public cloud computing setting (e.g. Wikipedia, YouTube), by definition, does not only involve a relationship between the client and cloud computing provider but between the client, the cloud computing provider and the public. Therefore, we are a situation very much like that we knew before the relatively recent explosion of cloud computing namely that of hosts envisaged in the ECD. So article 14 ECD is potentially applicable in various 'public cloud' situations. Several situations can occur depending on the involvement of the cloud computing provider.

---

[50] See e.g. http://www.bbc.co.uk/news/technology-19699205 and http://archives.lesoir.be/facebook-publie-par-erreur-des-messages-prives-sur_t-20120924-023UFW.html?query=facebook&firstHit=0&by=10&sort=datedesc&when=-1&queryor=facebook&pos=6&all=4203&nav=1 (in September 2012, there were allegations that Facebook leaked users' private conversations as a result of a bug).

[51] See e.g. clause 3.1 of the Microsoft Services Agreement, available at http://windows.microsoft.com/en-US/windows-live/microsoft-services-agreement

[52] See e.g. clauses 2 and 5 of Facebook's terms available at http://www.facebook.com/legal/terms, which relate to intellectual property rights.

Let us take first the example of YouTube. A priori, YouTube is the perfect example of a typical application of article 14 ECD so it should be off the hook. However, it may not be so clear-cut. Typically, when a user searches for a video, YouTube suggests other similar ones, which would potentially interest the user. Even, simply by accessing the YouTube URL before typing a search request, the site suggests videos based on video searches one has done before or on more generally based on one's browsing history. It even controls the order of the videos its web page shows after a user's search. In this case, it cannot be said that YouTube is merely passive or does not know or control the information displayed. Therefore, it would be liable under article 14 ECD. Does this behaviour (suggestions) amount to communicating to the public according to the factors elaborated by the CJEU? Arguably all factors are fulfilled including factors 3 and 5 (targeted and receptive public and YouTube is not merely passive). Even if without the intervention of YouTube, users would have access to the content it would be far more difficult for them to access it or even they would not have accessed it as they would not have thought about it and searched for it. The factual situation is close to that in the *Google France* CJEU case.[53] Of course, even if YouTube suggests other content, since all content on YouTube *should* be lawful (YouTube has been put on notice content is unlawful and acted expeditiously to remove it or it is users' content and they have by definition given permission to the public to view the content they upload[54]), even if YouTube communicates that content to the whole wide world, it does not amount to copyright infringement. As stated above in section I, YouTube and similar social sites' terms and conditions incorporate information about the notice and take down system and warn users that their account will be terminated if they repeatedly infringe.[55] Some national courts have had to deal with these aspects of YouTube and have come to diverging conclusions. Some courts considered YouTube as not sheltered by the safe harbour because they think it plays an active role (e.g. it presents videos as its own content, proposes links to other videos). However, a French court considered DailyMotion, a similar video-sharing site, as sheltered.[56]

---

[53] A recent French case involving Google's search engine involves somewhat similar facts but communication to the public was not strictly in issue. The national union of phonogram publishers sued Google because its search engine's auto-complete function pointed towards illegal downloading web sites (the auto-complete function suggests sites based on the number of searches done by users). The Court of Cassation held that the search engine suggestion function provided a means of copyright infringement and that by disabling this function Google could make the finding of such illegal sites more difficult. See Cass., 1st ch civ., 12 July 2012, *SNEP v. Google France*, available at http://www.courdecassation.fr/jurisprudence_2/premiere_chambre_civile_568/832_12_23884.html The basis of the judgment was articles L. 335-4 et L. 336-2 of the French Intellectual Property Code, which provide in the main that courts can order injunctions to prevent or stop infringements against those who can contribute to prevent or stop them.

[54] See YouTube's terms of use, available at http://www.youtube.com/static?gl=GB&template=terms, esp. clauses 7.2 and 8.1, accessed 24 September 2012 (user retains ownership rights but grants limited licenced rights to YouTube i.e. a worldwide non exclusive royalty free transferable licence to use, reproduce, distribute, prepare derivative works, display and perform the content). E. Valgaeren and N. Roland, "YouTube and social networking sites – New kids on the block?", in A. Strowel & JP Triaille (eds), *Google et les nouveaux services en ligne, Impact sur l'économie du contenu et questions de propriété intellectuelle*, Larcier 2008, p. 207, at 208: "any uploader grants YouTube a licence to distribute and modify the uploaded material for any purpose as long as the uploader has not deleted the material from the site."

[55] See e.g. Facebook terms, above n. 52, clause 5.5.; clause 6 of YouTube terms, above n. 54, states that a repeat infringer is someone who has infringed more than twice. Valgaeren and Roland, above n. 54, at 226: "While Youtube and similar social sites increasingly become the subject of lawsuits arguing "massive" copyright infringements, some commentators consider rather that, unlike Grokster and Napster cases, YouTube and some of the other related platforms events have demonstrated a conscious effort to satisfy the notice-and-take down procedures as well as establish a termination policy for repeat infringers".

[56] See the decisions referred to by the Commission Staff Working Document, *Online Services, including E-Commerce, in the Single Market*, (Accompanying the document Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the

Facebook also makes suggestions to its users. For instance, it notifies Facebook users when a friend is listening to music and suggests a link to that music. However, it only links to Spotify which is a legal music web site that users need to register for. So even if its role is arguably active, it does not infringe.

In a hybrid cloud situation (e.g. in most cases Picasa, Facebook, Google Documents), part of the storage may be publicly available, part private. So the developments made above under I.A and II.B apply respectively.

As can be seen from the above examples, cloud computing providers/host sites in both private and public situations are well advised to write down in the contracts for user storage and retrieval that they are not responsible for the user's use of third party copyright content. As we saw above, many cloud computing providers include this in the terms of their service agreements. For instance, some services (e.g. Hotmail[57]) bind the user by a clause which puts the entire responsibility on the user for the content s/he transmits or stores via its services. Some agreements add that cloud computing providers will act if they notice or are put on notice of illegal activity, including copyright infringement, by the user. The agreement sometimes adds that the cloud computing provider may even terminate the user's account if this happens (e.g. YouTube and Facebook policy for repeat infringers). The terms put the user on notice that if they upload infringing content they will have to bear the consequences. Does this mean that cloud computing providers are never communicating to the public? They cannot evade such liability by contract. Indeed, the contract only binds the user but the communication to the public is done with reference to the right holder who is not bound by the contract. Thus such a clause does not prevent liability in case the host site intervenes for instance by suggesting content.

C. Other problems that cloud computing providers may face

As per the scenarios above, the law seems easy to follow for cloud computing providers and many hosts have incorporated terms to reflect the law. However, the national case law interpreting the relevant provisions of the ECD has led to a number of uncertainties, owing on the one hand to technological developments since the adoption of the ECD and second, to the vagueness of some terms used in the ECD. The Commission launched a consultation on the ECD and drafted a paper to address the concerns raised by the responses.[58] In the main, the uncertainties relate to:

- The lack of clarity of the definition of intermediary activities in articles 12 to 14
- The lack of clarity of the conditions for benefiting from the safe harbour in articles 12 to 14
- The variety of "notice-and-takedown" procedures

Regions, A Coherent Framework to Boost Confidence in the Digital Single Market of E-Commerce and Other Online Services, COM(2011) 942 final, SEC(2011) 1640 final), Brussels, 11.1.2012, SEC(2011) 1641 final, available at http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf, p. 27-28.

[57] See clause 3.1 of the Microsoft Services Agreement, available at http://windows.microsoft.com/en-US/windows-live/microsoft-services-agreement "3.1. Who owns the content that I put on the services? Content includes anything you upload to, store on, or transmit through the services, such as data, documents, photos, video, music, email, and instant messages ("content"). Except for material that we license to you that may be incorporated into your own content (such as clip art), we do not claim ownership of the content you provide on the services. Your content remains your content, and you are responsible for it. We do not control, verify, pay for, or endorse the content that you and others make available on the services."

[58] See http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm

- The extent of the degree of monitoring allowed under Article 15.[59]

First, national courts diverge as to who can be considered a host. For instance, an Italian court considered the Pirate Bay as a P2P file-sharing service, while in Sweden it was considered as a host.[60] Second, national courts diverge as to what activities are sheltered under article 14. For instance, some courts consider video-sharing sites as not sheltered because of their active role while others do.[61] Some national courts have used this element of control to find the host liable, for instance if a blog exercises editorial control on its users' posts.[62] As we saw, the *Google France* and *eBay* cases have however taken away some of this confusion. Also national case law is contradictory on the conditions of article 14 such as what is meant by 'expeditiously' and 'actual knowledge'.[63] The *eBay* ruling has not entirely cleared up the second of these terms. A third concern has to do with the notice-and-take-down procedures. Many hosts have included such procedure within their terms of service and thus can decide on their own account to take down material which they themselves think is infringing copyright without a notification of right holders or a fortiori without a court order. Some respondents worry that these removals may chill speech as intermediaries are not judges and cannot always[64] know whether content is illegal.[65] The actual procedures in any case differ a lot between Member States and stakeholders are divided on how the procedure should be revised. An example, which was addressed also above, is whether stay-down orders should be allowed. Many stakeholders also note that the user should be able to defend the legality of the content.[66] In this respect, some hosts' contract terms include the possibility to appeal.[67] The Commission has therefore announced the launch of an impact assessment on procedures for notifying and acting on illegal online content in 2012 in order to determine whether the EU needs to act. The final main concern relates to the extent of monitoring allowed under article 15. As we addressed above, the problem is going to be for national courts to assess in each case if a specific obligation to monitor respects the balance between the fundamental rights of all the parties involved. In this respect, further guidance from the CJEU, or better, revision of the ECD, may be necessary.

All these uncertainties may thus affect cloud computing providers as they host user content.

Conclusion

What can be said in conclusion? First, the 1996 WIPO Internet treaties are as such not outdated in relation to cloud computing. The provisions on communication to the public fully apply to them. In addition, the Beijing Treaty has now filled the gap in relation to communication to the public of audiovisual performances both unfixed and previously fixed

[59] See Commission Staff Working Document, *Online Services, including E-Commerce, in the Single Market,* above n. 56, p. 25.
[60] See ibid., p. 30.
[61] See ibid., p. 27-28.
[62] See ibid., p. 29 referring to *Kaschke v Gray Hilton* [2010] EWHC 690 (QB), available at http://www.bailii.org/ew/cases/EWHC/QB/2010/690.html
[63] See Commission Staff Working Document, *Online Services, including E-Commerce, in the Single Market,* above n. 56, p. 32-38.
[64] Except in flagrant cases (an obvious example is child pornography).
[65] See Commission Staff Working Document, *Online Services, including E-Commerce, in the Single Market,* above n. 56, p. 41.
[66] See ibid., p. 43-44.
[67] See e.g. Facebook terms, n. 52 above, clause 5.4: "If we remove your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal".

in audiovisual fixations (articles 2, 6, 10 and 11 of the Treaty).[68] However, the case law over the years has generated a number of questions and the legal framework should be made more precise to remove uncertainties. The Commission has started to address these issues in its Staff Working Document "Online Services, Including E-Commerce, in the Single Market". The Commission's imminent initiative on notice-and-take-down procedures will hopefully also lead to a clearer and harmonised framework which will help cloud computing providers clarifying their liability for the content they store on behalf of their users. In view of the global nature of the issues, it would be best if clarifications and additions were made to the WIPO Internet treaties and the Beijing Treaty but the usual slowness may be a hindrance.

The CJEU's *TV Catch Up* upcoming decision may provide more details on the notion of communication to the public but probably nothing will come out which helps answering the questions this paper addressed, namely cloud computing provider liability.[69] On the other hand, the CJEU decision in *UPC Telekabel Wien* should shed some more light on the extent of an obligation of specific monitoring.[70]

For the moment, according to the case law, in essence, whether the host is liable will depend on its level of involvement. As can be seen from the different scenarios addressed and from the case law, there are different shades in this respect. All one can say is that, like the idea/expression dichotomy (the more detailed the idea is the more likely it is to be an expression), the more involved the host is, the more likely s/he will be liable under articles 8 Rental and Lending Directive, 3 Infosoc Directive and 14 ECD. Right holders will be able to use injunctions for present and future infringements relating to a single or more repeat copyright infringers acting on the cloud computing provider/host's platform. But stay-down injunctions are unlikely to be acceptable. In any case, many hosts' terms already provide for suspension or termination of a user's account in case of repeat infringements. The problems with these suspensions and terminations are the danger of censorship and lack of a possibility of defence from the user (this happens of course only if the notice is not followed by a court order which has assessed the illegality of the content). Nevertheless, hosts need business and are unlikely to terminate users' accounts if they are not entirely convinced of the egregiousness of the infringement.

In sum, the most important question for cloud computing providers is to determine the precise contours of their liability under the right of communication to the public and article 14 ECD. Some of these contours have now emerged more clearly as a result of the CJEU's case law even if partially. And more clarifications are already forthcoming from the CJEU and also in the form of legislation or soft law following the Commission's future actions in response to the stakeholders' decade of experience with the ECD.

[68] Bejing Treaty on Audiovisual Performances, available at http://www.wipo.int/edocs/mdocs/copyright/en/avp_dc/avp_dc_20.pdf
[69] Above n. 43.
[70] See above n. 11.