EU study on the

Legal analysis of a Single Market for the Information Society

New rules for a new age?

6. *Liability of online intermediaries*

November 2009

DLA PIPER

Table of contents

This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.

Chapter 6
Liability of online intermediaries

1. Introduction

On 4 June 2008, the French Civil Court of Troyes ruled that auction website eBay was liable of counterfeit for the sale of a counterfeited luxury bag by one of its customers. eBay was ordered to pay 20,000 EUR in damages, as well as a maximum of 15,000 EUR for publishing the decision in four different magazines. The Court also considered that eBay's efforts to suppress counterfeit were not sufficient.

Less than one month later, the Commercial Court of Paris found eBay liable for infringing the selective distribution agreements of several perfume producers, and ordered eBay to pay 3,052,000 EUR in damages, as well as a maximum of to 15,000 EUR for publishing the decision. eBay was also ordered to remove from its systems all advertisements relating to the perfumes of these producers, under a penalty of damages of 50,000 EUR per day, despite eBay's claim that there exist no filtering mechanisms that can effectively filter out all such advertisements.

Only one month later, on 31 July 2008, the Court of Brussels decided in a very similar case against eBay that eBay's efforts to suppress counterfeit were sufficient, that eBay could not be held liable and that eBay cannot be required to actively monitor the auctions offered on its website. Almost one year later, the French Tribunal de Grande Instance issued a similar decision[1], squarely contradicting the aforementioned French decisions.

Meanwhile, in the United States, the District Court of New York had ruled on 14 July 2008 in a similar case of alleged jewellery counterfeit, that eBay could not be held liable for trademark infringements. The plaintiff did not even bother to invoke any allegations outside trademark law, as US law and established US case law shields online service providers such as eBay from almost any form of liability triggered by third party content.

Although it is not uncommon for different Courts to decide differently in complex cases, the European eBay decisions are particularly remarkable when considering that in each of the cases, there were arguments why eBay could be considered a "hosting provider", which is shielded from liability by a set of rules set forth in the eCommerce Directive. However, the precise scope of these special liability rules is not clear, so that it is actually not surprising that each court applied these rules differently: according to the Court of Paris, these special liability rules did not apply at all, because eBay's auction services do not only consist of hosting-related activities; according to the Court of Troyes, the rules only apply to a limited subset of the auction-related services; and according to the Court of Belgium, the rules simply did apply to eBay.

* *

The above cases are only the tip of the iceberg: across Europe, the special liability regime has been implemented in different ways in national systems, as well as diverging case law. Courts seem to have difficulties to apply the special liability regime, so that online intermediaries are increasingly exposed to lawsuits triggered by content provided by their users, which is particularly worrying in the "Web 2.0" era, where user-generated content has become a driving factor.

[1] Tribunal de grande instance de Paris, 3ème chambre, 13 May 2009, L'Oréal et autres / eBay France et autres

This chapter therefore investigates the various issues surrounding the liability of online intermediaries — such as internet access providers, web hosting companies, content aggregators, Web 2.0 service providers and other "online service providers" — in order to investigate whether the current rules are still suitable, and which balance should be found to balance the rights of all stakeholders and foster the position of Europe in today's information society.

It should be noted that this chapter does not deal with all aspects of online liability of intermediaries. More in particular, it does not deal with the *contractual liability* (such as exclusions of liability in online terms and conditions). Furthermore, this chapter is limited to the liability incurred by *intermediaries*, excluding direct liability issues that do not involve intermediary roles (*e.g.,* a party's own liability for harmful content created by it, or a party's own liability for direct copyright infringement). Also note that some of the issues touched by this chapter, are linked to topics investigated in other chapters, such as copyright and privacy issues. These issues will be discussed in the other chapters of this study.

2. Liability before the eCommerce Directive

This section provides a concise historical overview of how the liability of online intermediaries was treated by national laws and national case law. As will be explained below, the direction headed by case law and the divergences in national law have spurred to the adoption of the harmonising eCommerce Directive.

2.1. Introduction

As online service providers generally only have a limited degree of knowledge about the data they transmit or store, the liability allocation between online service providers and the persons who originally put such information online can be problematic[2]. Although the liability issues faced by online service providers are caused by their customers or users, the service providers are an attractive target for legal action, as they are visible, well known, and their financial strength is likely to be greater than that of their customers or users[3].

Hence, long before the rise of e-commerce, internet intermediaries were already accused of defamation, copyright infringement and obscenity and indecency issues[4]. As a reaction, some Member States started regulating certain aspects of their liability, often inspired by the established rules regarding publisher's liability. Pending such legislation, national judges mostly relied on general rules of contributory liability – including publisher's liability rules – to address the issue[5]. Due to the difficulties to apply the established principles of publisher's liability to the new media, case law varied significantly, both within one Member State and across Member States.

2.2. Member State overview: case law, legal doctrine and legislation

Austria – Austria regulated the liability of online intermediaries by approving a federal bill to enact the Federal Telecommunications Statute in 1997, which held that owners of *"broadcasting installations and terminals"* (such as computer servers) were held liable, unless they would have taken appropriate and reasonable steps to prevent wrongful use of their equipment.

---

[2] Commission Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, COM(1998) 586 final, 18 November 1998, p. 12. (hereafter the "Commission Proposal")

[3] I. J. LLOYD, *Information technology law,* Oxford, Oxford University Press, 2008, p. 572

[4] J. HUGHES, "The Internet and the Persistence of Law", *Boston College Law Review,* 2003, Vol. 44, No. 2, p. 383

[5] Study on liability of internet intermediaries, p. 30 and 47

France – To counter the protests arising after the confiscation of the computer equipment of two internet access providers Francenet and Worldnet, the Minister of Telecommunication introduced a bill in 1996 to limit the liability of online intermediaries[6]. This bill exempted online service providers from criminal liability for third party infringements, provided they did not participate in these infringements, they offered filters to prevent access to certain services, and their services were not disapproved by the Committee of Telematics[7]. The proposed amendment was, however, annulled by the Constitutional Council due to formal errors[8].

In the meantime, French legal doctrine reverted to general tort law[9] and the general cascading system of liability for crimes committed by the press[10]. Nevertheless, case law varied considerably. For example, in 1996, a court rejected a request to block access to negationist messages, because *"an access provider [is] under no legal obligation to regulate the information available on the network (...) since the authors alone are liable in respect of such information"* [11]. Conversely, another court ruled in 1998 that a hosting provider was obliged to monitor content providers to whom it rents out space. According to this court, a hosting provider had to demonstrate it had fulfilled its monitoring obligations, and had taken the necessary technical measures to stop the illegal activity, in order to be exempted from liability[12]. In 1999, another French court assimilated a hosting provider with the director in charge of publications on an audio-visual communication service, but nevertheless concluded that control by the service provider was impossible because the transfer between the actual author and the public had taken place electronically and at high speed[13]. Yet another court ruled in the same year[14] that a hosting provider has a surveillance duty to not infringe third party rights.

The Netherlands – The liability of online intermediaries was first addressed in the Netherlands in *Bridgesoft v. Lenior*[15], in which a bulletin board operator was charged with direct copyright infringement, because it allowed its subscribers to upload and download pirated software. The court found the operator to be liable for copyright infringement, and also found that the operator had acted negligently since it should have been aware of the possibility of copyright infringements.

In the 1996 *Scientology-case*, several internet service providers were sued for copyright infringements, as they enabled the online publication of copyrighted work. In summary proceedings, the court's president found the providers not to be liable, on the grounds that "*they do no more than provide the opportunity to public disclosure, and that in principle, they are unable to influence, or even have*

---

[6] E. WERY, "Internet hors la loi? Description et introduction à la responsabilité des acteurs du réseau", *Journal des Tribunaux*, 1997, Vol. 5846, p. 417-428

[7] E. WERY, *l.c.*, note 120

[8] Decision 961378 DC, 23 July 1996, *J.O.* 27 July 1996, as referred to by E. WERY, *l.c.*, note 121

[9] Conseil supérieur de la propriété littéraire et artistique (Commission spécialisée sur les prestataires de l'internet), *Rapport de la commission*, 2008, available at www.cspla.culture.gouv.fr/travauxcommissions.html

[10] Act on the Regulation of the Press of 1881. With the Act on Audiovisual Communications of 1982, this system of cascade liability was extended to apply to audio-visual communications (see K. KOELMAN and B. HUGENHOLTZ, "Online Service Provider Liability for Copyright Infringement", *WIPO Workshop on Service Provider Liability*, November-December 1999, available at *www.ivir.nl/publicaties/hugenholtz/wipo99.pdf* (last viewed 20 January 2009)

[11] Paris Regional Court, 12 June 1996, Réf. 53061/96

[12] 1998 decision, referred to by R. JULIA-BARCELO, "Liability for On-line Intermediaries: A European Perspective", *l.c.*

[13] *Ava v. Infonie and others*, District Court of Puteaux, 28 September 1999

[14] Lacoste/Multimania, Esterel and Cybermedia, TGI de Nanterre, 8 December 1999

[15] District Court of Rotterdam 24 August 1995, *Informatierecht/AMI*, 1996/5, p. 101

knowledge of the things disseminated by those who have access to the Internet through them"[16]. This decision was later on confirmed[17].

The Dutch Penal Code also provides for a cascade liability system for publishers or printers. In 1998, a bill was introduced to rewrite these provisions, to ensure that they would apply to all intermediaries, including online intermediaries. The proposal exempted online intermediaries from liability if they would reveal the identity of the infringer, provide all information necessary to identify the infringer, and take all reasonable measures to prevent any further dissemination of the infringing materials[18]. The proposal was not accepted by the Dutch Parliament until after the introduction of the E-Commerce Directive.

United Kingdom – The United Kingdom was the first European country to specifically adopt legislation to limit online intermediary liability prior to the introduction of the E-Commerce Directive, although this legislation was limited to defamation issues. The Defamation Act of 1996 introduced an *"innocent dissemination"* defence for distributors of hard copy publications, as well as online service providers and internet access providers. It exempted online intermediaries from liability for third party materials, provided they could prove to have taken reasonable care with respect to the publication, and did not have any reason to believe that it contributed to the publication of a defamatory statement. However, in the first case in which these provisions were applied – *Godfrey v. Demon Internet*[19] – the court ruled that the service provider could not take the advantage of this defence introduced by the Defamation Act, as it had failed to comply with the plaintiff's request to remove offensive postings from one of its newsgroups. The court therefore found that Demon did contribute to the publication of the defamatory statement.

Germany – Felix Somm, general manager of CompuServe Germany, was prosecuted for facilitating access to violent and child pornographic content stored in newsgroups accessible by CompuServe's customers. As a reaction, the Teleservices Act and Multimedia Law was adopted in 1997[20], which established criteria for the liability of online intermediaries and exempted transmission providers and short-term storage providers from liability, unless they would initiate, select or modify the information. Long-term storage providers were not liable when they did not have actual knowledge of illegal information, and upon obtaining such knowledge, would act expeditiously to remove or disable access to such information[21].

Spain – Spain had not adopted any specific legislation regarding the liability of online service providers and did not have any relevant case law in this area either, which created considerable legal uncertainty for online service providers[22]. With respect to copyright, both the Spanish copyright law[23] and the general

---

[16] President of Court of 's Gravenhage 12 March 1996, *Informatierecht/AMI,* 1996/5, p. 96-97

[17] Court of 's Gravenhage 9 June 1999, *Computerrecht,* 1999, Vol. 4, p. 200

[18] Proposal Computer Criminality Act II, January 1998, Second Chamber, 1998-1999, 26.671, referred to by K. KOELMAN and B. HUGENHOLTZ, *l.c., p.* 23

[19] *Godfrey v. Demon Internet* [1999] 4 All ER 342

[20] However, this new Act could not stop Felix Somm from being convicted. In 1998, the *Amtsgericht* of Munich convicted Mr. Somm for facilitating access to violent and child pornographic content stored in newsgroups hosted by CompuServe Inc (AG Munich 12 May 1998, *Computer und Recht* 1998, p. 500). The court ruled that CompuServe Germany, a subsidiary of CompuServe US, could not invoke the Act, because access to the Internet was provided by the parent company, and not by CompuServe Germany. The court therefore considered CompuServe as a hosting service provider, and found that CompuServe had not done all the technically feasible to block access to the newsgroups concerned. The decision was later reversed by the *Landgericht* of Munich (LG Munich 17 November 1999, *Computer und Recht* 2000, p. 118)

[21] Y.A. TIMOFEEVA, "Hate Speech", *Journal of Transnational Law and Policy*, Vol. 12:2, p. 262

[22] R. JULIA-BARCELO, "Liability for On-line Intermediaries: A European Perspective", *E.I.P.R.,* 1998, Vol. 20, nr. 12, p. 1-10

[23] Royal Legislative Decree No. 1/1996 of 12 April approving the Revised Text of the Intellectual Property Law

tort liability rule[24] apply a with-fault liability standard. In addition, criminal law could impose civil liability for crimes committed by other persons. A majority of legal commentators considered article 120 of the Spanish Penal Code[25] to introduce a strict liability, applicable to online intermediaries to the extent they could be regarded as "*owners of any other method of communication*"[26]. Regarding defamation, the general tort liability rule would (hypothetically) also have applied, as well as the Spanish Press Act[27], which both maintain a fault-based liability standard. It remained unclear, however, whether an online service provider would have fallen into one of the categories set out in the Press Act (such as authors, publishers and editors).

Sweden – Sweden only regulated the liability of electronic bulletin board operators. The 1998 Act on Responsibility for Electronic Bulletin Boards required operators to monitor the bulletin board, supervise the activities of subscribers and remove any infringing material.

2.3. Reasons to adopt EU-level measures

The case law and legal doctrine referred to above illustrate the varying, often burdensome obligations and responsibilities imposed on online service providers in the EU, which entailed the risk that the further development of the Internet would be impeded[28]. Several Member States acknowledged this issue and reacted by adopting specific legislation. However, even such legislation failed to provide the online intermediaries with the necessary certainty[29]. Moreover, the divergences in national legislation, the divergences in case law between Member States – and even the divergence of case law within one single Member State – created additional legal uncertainty for online service providers in the EU, which faced almost as many legal regimes as there were Member States[30].

The European Commission recognised these problems in its proposal for the Directive on electronic commerce: "*There is considerable legal uncertainty within Member States regarding the application of their existing liability regimes to providers of Information Society Services when they act as "intermediaries", i.e. when they transmit or host third party information (information provided by the users of the service). These activities have been the subject of the different Member States' initiatives adopted or currently being examined on the issue of liability"* [31].

The Commission further referred to the "*divergent principles*" adopted by those Member States which have introduced new legislation. Despite the limited availability of case law in Europe regarding this issue, the Commission also found the "*divergences in rulings and reasoning by the courts*" to be an

---

[24] Article 1903 of the Civil Code

[25] "*(…) actors will incur civil liability regardless of their criminal liability, where they are (…) owners of any other method of communication of written, spoken or visual material for criminal offences carried out through such methods (…)*"

[26] R. JULIA-BARCELO, *l.c.*

[27] Article 65(2) of Act 14/1996 of 18 March regarding Press and Print.

[28] J. HUGHES, *l.c.*, p. 382

[29] See the Somm case in Germany and the Godfrey v. Demon case in the United Kingdom

[30] R. JULIA-BARCELO, "On-line Intermediary Liability Issues: Comparing EU and US Legal Frameworks", *Electronic Commerce Legal Issues Platform*, Deliverable 2.1.4bis, 16 December 1999, p. 5, available at *www.eclip.org* (last viewed 22 December 2008)

[31] Commission Proposal, p. 12

obstacle for the internal market[32]. The national approach was obviously found to be ineffective in trying to provide favourable conditions for Internet transactions and publications[33].

The E-Commerce Directive finally introduced a European regime, and intended to equalise service providers' obligations in all Member States. As further discussed below, these intentions have not been fully realised, so that the mosaic of case law and national regulations has again returned to the EU information society scene — particularly for services that do not neatly fit within one of the three categories predefined by the eCommerce Directive.

3. Liability under the eCommerce Directive

This section 3 provides an overview of the scope and features of the "special liability regime" introduced by the eCommerce Directive. The different issues linked to this special liability regime are not discussed in this section 3, but are instead discussed in section 4 below.

3.1. Introduction to the special liability regime

The eCommerce Directive introduced a set of special liability rules, which are set forth in Section 4 of the eCommerce Directive (articles 12 to 15). It provides for a "safe haven" regime, under which three types of service providers are exempt from liability under certain conditions. This safe haven was considered indispensable to ensuring both the provision of basic services and the provision of a framework which allows the Internet and e-commerce to develop[34].

The special liability regime can be briefly described as follows:

- **"Mere conduit" service providers** (article 12) deliver either network access services or network transmission services. The typical service providers targeted by article 12, are traditional internet access providers (which connect their subscribers to the Internet using dial-up modems, xDSL modems, cable connections or fixed lines) and backbone operators (which interconnect various subparts of the Internet). Both types of service providers transmit large amounts of data at the request of their subscribers.

  This liability exemption only applies when the service provider is *passively* involved in the transmission of data. When the transmission would be initiated, selected or modified by the service provider, or when the receiver of the data would be selected by the service provider, the exemption does not apply.

- **"Caching" providers** (article 13) temporarily and automatically store data in order to make the onward transmission of this information more efficient. The typical service envisaged by article 13 is a so-called "proxy server", which stores local copies of websites accessed by a customer. When the same website is subsequently accessed again, the proxy server can deliver the locally stored copy of the website, which avoids that the original web server needs to be contacted again, hence reducing network traffic and speeding up the delivery process.

---

[32] *Ibid.*

[33] L. EDWARDS, "Defamation and the Internet", in L. EDWARDS and C. WAELDE (eds.), *Law & the Internet, a framework for electronic commerce*, Oxford, 2000, p. 268

[34] First Report on the application of 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, COM(2003) 702 final, p. 13 (hereafter the *"First Report on the E-commerce Directive"*)

As information is locally stored by the caching provider during a certain period of time — which, depending on the configuration of the servers and websites involved, can be up to several months — various conditions need to be met by the caching provider in order to benefit from the liability exemption. The most important conditions impose that the local copy must be identical to the original information, and that the service provider must comply with the access conditions associated with the locally stored information[35]. Furthermore, the service provider must update the copy in the manner specified by the original website[36], and must remove (or block access to) the local copies when it obtains actual knowledge of the fact that the original data is removed, or access to the original data is blocked.

- **Hosting providers** (article 14) store data provided by their users. The data being stored is specifically selected and uploaded by a user of the service, and is intended to be stored ("hosted") for an unlimited amount of time. The typical service envisaged by article 14, is a webhosting company, which provides webspace to its customers, on which they can upload content to be published on a website.

  Hosting providers can only benefit from the liability exemption when they are *"not aware of facts or circumstances from which the illegal activity or information is apparent"* (when it concerns civil claims for damages) or they *"do not have actual knowledge of illegal activity or information"* (when it concerns other claims). Article 14 thus differentiates the level of knowledge, depending on the type of claim asserted against the service provider. Furthermore, service providers must expeditiously remove, or block access to, such information once they are aware of their unlawful nature.

3.2. Characteristics of the special liability regime

Passive, intermediary role – The eCommerce Directive requires the service providers to act as intermediaries and to maintain a passive role in order to benefit from the liability exemption. However, the level of passiveness differs among the three types of service providers.

Mere conduit service providers transport enormous amounts of data for recipients they even may not know, and are therefore envisaged as having a strictly passive role. If they want to benefit from the special liability regime, they are not allowed to take any initiative with respect to the transmission or interfere in any way in the data or the recipient selection process.

Compared to mere conduit service providers, caching providers can be more actively involved towards their users, as they are allowed to select the data or the recipient of the service (although they are not allowed to modify the local copy of the data stored by them). In fact, the ability to select the data or the receiver, is a key feature of a caching provider, which may want to restrict the access to its services, or which may want to filter the information made available to its users[37].

The required level of passiveness is the lowest for hosting providers, which are allowed to select and modify the data they store, as well as to select the recipient of the data. If, however, the user of their

[35] For example, when the service provider stores a local copy of website content protected by a password, other non-authorised customer should not be allowed to access this local copy.

[36] For example, a web server may specify the maximum period during which copies can be stored on a proxy server. After this period of time, the original web server should be contacted again by the proxy server in order to obtain a new copy of the data concerned.

[37] For example, proxy servers are frequently installed by employers to facilitate blocking of certain websites (e.g., sports websites or websites with adult content).

services would be acting under the authority or control of the hosting provider, the liability exemption will no longer apply.

Horizontal effect – The special liability regime installs a horizontal liability regime for the three types of service providers covered by it. Provided they meet the criteria laid down in Section 4, the service providers will be exempted from contractual liability, administrative liability, tortuous / extra-contractual liability, penal liability, civil liability or any other type of liability, for all types of activities initiated by third parties, including copyright and trademark infringements, defamation, misleading advertising, unfair commercial practices, unfair competition, publications of illegal content, etc[38].

It is important to note, however, that the special liability regime only protects the service providers from *liability* claims. Article 12.3, 13.2 and 14.3 explicitly state that courts and administrative authorities can still request the service providers to terminate or prevent infringements. Consequently, a service provider can be requested to take measures to terminate or prevent an infringement, even when the service provider cannot be held liable for this infringement.

No general obligation to monitor – Section 4 (article 15) of the eCommerce Directive sets forth the principle that the three types of service providers have no obligation to monitor the data they transmit or store, nor a general obligation actively to seek facts or circumstances that would indicate illegal activity.

However, despite this prohibition for Member States to impose general monitoring obligations, courts and administrative authorities can still request the service providers to terminate or prevent infringements, for example through injunctions[39]. According to recital 47 of the eCommerce Directive, such monitoring obligations must be limited to specific, clearly defined individual cases.

Application at the service level – The special liability regime applies to the services provided by a person, and not to the person itself. When a party would supply several types of services, this party may simultaneously qualify for articles 12, 13 and 14[40].

> *For example, when an internet access provider connects its customers to the Internet through a proxy server, and also offers web space for a personal homepage, this provider will qualify as a mere conduit service provider (for the internet access provided), a caching provider (for operating a proxy server) and a hosting provider (for the web space offered). However, the liability exemptions will not apply to any additional services offered by this provider, such as a news portal, a localised search engine or a domain registration service.*

Additional protection – While the special liability regime constitutes an additional shield for service providers, it does not modify each Member States' underlying material law governing liability. The only effect of not (or no longer) meeting the criteria of article 12, 13 of 14 (*e.g.,* because data is modified during transmission, or when access to hosted data is not blocked upon awareness of the unlawfulness), will be the loss of the additional protection. Service providers will then become subject to the general rules of tortuous or penal liability, which may or may not hold the service provider liable, depending on each Member State's laws[41].

---

[38] E. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", in *Le commerce électronique européen sur les rails?*, Bruylant, Brussels, 2001, p. 276

[39] Articles 12.3, 13.2 and 14.3, as well as preamble 45, as further discussed in section 4.6 below

[40] See Commission Proposal, p. 28; First Report on the E-commerce Directive, p. 12; E. MONTERO, "Sites de vente aux enchères et offres de vente illicites", in *Revue du Droit des Technologies de l'information* - n° 33/2008, p. 528-533 (hereafter "MONTERO 33/2008"); E. MONTERO, "Les responsabilités liées au web 2.0", in *Revue du Droit des Technologies de l'information* - n° 32/2008, p. 368 (hereafter "MONTERO 32/2008")

[41] See also Commission Proposal, p. 27; G. TEISSONNIÈRE, "Quelle responsabilité appliquer aux plates-formes de commerce en ligne et autres intermédiaires de contenus?", *Revue Lamy Droit de l'Immatériel*, 2008/35, no 1165, p. 22

Specific rules for the online world – Together with the other provisions in the eCommerce Directive, the special liability regime creates specific rules for online services. Accordingly, service providers become subject to different rules, depending on whether they provide their services online or offline. This preferential regime was deliberately envisaged by the European Commission to allow the online service market to develop[42].

4. Issues linked to the special liability regime

The special liability regime introduced by the eCommerce Directive has contributed to the further development of online services, particularly in the initial years following the introduction of the Directive[43]. Even so, various problems have emerged over time, which have become more pronounced with the advent of new technologies and "Web 2.0" online services. These problems are discussed in detail in this section 4, and can be summarised as a lack of clarity, implementation differences between Member States[44], gaps in the scope, and the threat of injunctions.

4.1. Ambiguities in the definition of "information society services"

The special liability regime applies to *information society services*, which are defined as services that are *"normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"*, whereby the service *"is sent initially and received at its destination by means of electronic equipment for the processing [...] and storage of data"* [45]. Well-known examples of information society services include web shops, on-line information access tools and search engines[46].

The key elements of this definition are "normally provided for remuneration" and "by electronic means". The question arises how both elements must be interpreted. While this may seem obvious, there are many ambiguities when these concepts are studied in detail.

Please note that, while the ambiguities described in this section 4.1 are applied to the special liability regime for online intermediaries, the impact of these ambiguities is much larger, as it affects the entire scope of the eCommerce Directive. Accordingly, online service providers that do not meet the "normally provided for remuneration" and "by electronic means" criteria, will also be exempted from the transparency obligations of the Directive and rights of free establishment.

4.1.1. "Normally provided for remuneration"

"Information society services" are a subcategory of the general concept of "services", as defined in article 50 of the EC Treaty. Accordingly, any activity which would not fall within the scope of article 50 of the EC Treaty, will *a priori* not qualify as an information society service.

---

[42] First Report on the application of the E-commerce Directive (21 November 2003), p. 14: *"The limitations on the liability of intermediaries in the Directive were considered indispensable to ensuring both the provision of basic services which safeguard the continued free flow of information in the network and the provision of a framework which allows the Internet and e-commerce to develop."*

[43] In its First Report on the application of the E-commerce Directive, the Commission stated that *"the feedback received so far from the Member States and interested parties has, in general, been positive"*, although *"there is still very little practical experience on the application of articles 12-14"*.

[44] P. BALBONI et al, "Liability of Web 2.0 Service Providers - A Comparative Look", *Computer Law Review International Issue*, 2008, 3, p. 65

[45] Definition set forth in article 1(2) of Directive 98/34/EC (as amended by Directive 98/48/EC), as referred to by article 2.a eCommerce Directive.

[46] Examples taken from recital 18 of the eCommerce Directive

Recital 19 of Directive 98/48/EC, which introduced the concept of "information society services", explicitly refers to article 50 of the EC Treaty, as well as the corresponding case law of the Court of Justice, when giving background information regarding *"normally provided for remuneration"* [47] [48].

Although the existing case law[49] regarding the general concept of "services" upholds a relatively wide interpretation[50] – as it argues that any consideration for an economic activity can constitute "remuneration" – it is not unlikely that new case law would consider that some online activities are not included in the scope. Difficulties may therefore arise when applying the case law of article 50 EC Treaty – which targets issues dealing with freedom of movement for goods, capitals and persons – to emerging commercial models online, because this case law is focused on the question to which extent activities of a *State* fall within the scope of article 50. It may therefore be complicated to apply this case law to the typical online activities offered by online service providers.

Explicitly excluded – According to the case law of the Court of Justice regarding article 50 EC Treaty, some activities are explicitly considered as not "normally being provided for remuneration" (such as public education and governmental services[51]). Accordingly, taking into account that the core education activities offered by public schools and public universities are out of scope, it could be argued that elements that are part of this activity (such as providing internet access to classrooms) are excluded from the scope of the eCommerce Directive. It can be questioned whether this exemption is (still) justified[52], particularly when considering how the Internet is becoming an essential tool for education[53].

Indirectly paid activities – The Court of Justice has clarified that an activity that is remunerated by a third party, can also qualify as a service *"normally provided for remuneration"* in the sense of article 50 of the EC Treaty, as this article does not focus on the specific nature of the remuneration, and does not require that the user him/herself pays[54]. Consequently, an activity paid for by advertisements was considered to fall within the meaning of article 50.

According to legal doctrine[55], this reasoning can be applied by analogy to online service providers that do not charge fees to their end users, but derive an income from commercial banners presented on their websites. The indirect remuneration established by such advertising revenue is indeed well known, and

---

[47] *"Whereas, under Article 60 [now 50] of the Treaty as interpreted by the case-law of the Court of Justice, 'services' means those normally provided for remuneration; whereas that characteristic is absent in the case of activities which a State carries out without economic consideration in the context of its duties in particular in the social, cultural, educational and judicial fields; whereas national provisions concerning such activities are not covered by the definition given in Article 60 of the Treaty and therefore do not fall within the scope of this Directive."*

[48] See also the Vademecum on Directive 98/48/EC, available at http://ec.europa.eu/enterprise/tris/vade9848/index_en.pdf

[49] See, for example, the Humbell case (Case 263/86 Belgian State v Humbel [1988] ECR 5365) and the case of Stephan Max Wirth v Landeshauptstadt Hannover (Case C-109/92, 7 December 1993).

[50] For example, private television broadcasting is regarded as a service provided for remuneration because it is paid for through advertising, and hospital services are also provided for remuneration, as hospitals are financed by health insurance companies

[51] As also repeated in recital 19 of Directive 98/48/EC

[52] Of course, it should be taken into account that the qualification of an "information society service provider" also entails some drawbacks from the service provider's point of view, as an information society service provider is required to comply with the various obligations set forth in the eCommerce Directive (information to be provided, order placement procedure, ...)

[53] Note that the Digital Millennium Copyright Act, which provides a special liability regime for copyright infringements similar to the eCommerce Directive, contains specific wording targeted at nonprofit educational institutions (see section 27 below). Furthermore, public authorities are also protected by the US Communications Decency Act (see section 5.3 below)

[54] See Case 352/85, Bond van Adverteerders v the Netherlands [1988] ECR 2085

[55] M. ANTOINE, "L'objet et le domaine de la Directive sur le commerce électronique", in *Le commerce électronique européen sur les rails?*, Bruylant, Brussels, 2001, p. 3

is frequently used in the offline context (*e.g.,* to sponsor journals), so that application to websites that are sponsored by banners, is immediately evident. Accordingly, the example of a website sponsored by commercial banners is typically cited by legal doctrine that discusses the scope of the eCommerce Directive[56].

Although activities sponsored by advertisements are explicitly considered as falling within the scope of article 50 by the case law of the Court of Justice, the question arises to which extent this case law can be applied to other services, for which the link between the service recipient and the remuneration / the remunerating party is far more indirect or remote.

- If, for example, an online activity is provided completely for free by an internet startup company (which, typically, hopes to establish an online presence and then later on find a lucrative business model) and no advertising revenue is generated, can it still be claimed that such service is provided "for remuneration"?
- How should services be qualified that are offered for free by a company, with the sole intention of creating goodwill[57]?
- Consider an amateur developer who offers an open source software package on its website. The website contains no sponsored advertisements and does not attract other types of revenue (such as value added services), so that the developer is not subject to the eCommerce Directive. At a certain point in time, a third party recognises the value of this open source software and offers the developer a job opportunity. Does the website now suddenly become subject to the eCommerce Directive?

It is difficult to predict how a court would react to these cases.

Meaning of "normally" – Another question relates to the term "normally"[58]. This word excludes entire categories of online services that are not funded by advertising revenue (such as banners), and are typically provided for free by most service providers — for example, online wiki's (such as the popular Wikipedia), photo-sharing sites (such as Flickr and Imageshack) and microblogging tools (such as Flickr and Jaiku).

The potential impact of this issue should not be underestimated, as many services on the Internet are offered for free (are not even paid by advertisements). Furthermore, the emerging business model on the Internet is the "freemium" model, whereby more than 95% of the users make free use of a service, and less than 5% of the users pays some kind of remuneration to the service provider (*e.g.,* to get access to restricted features, to get professional support, to get more storage capacity, etc.)[59]. When the "freemium" model and the "entirely free" model become the dominant business models within a certain

---

[56] See, for example, P. VAN EECKE, "Artikelsgewijze bespreking van de wetten elektronische handel", in P. VAN EECKE and J. DUMORTIER, *Elektronische handel - commentaar bij de wetten van 11 maart 2003,* die keure, 2003, p. 13; M. ANTOINE, *o.c.*, p. 3; M. SCHAUB, *European legal aspects of e-commerce*, 2004, p. 28; Belgian preparatory documents for the Act of 11 March 2003 (implementing the eCommerce Directive), p. 13-14; etc.

[57] *E.g.,* a free wireless hotspot service that would be offered in a certain area by a company, that can be used by anyone, and does not generate remuneration through advertising.

[58] It is not entirely clear from the case law of the Court of Justice at which level this the "normally" should be interpreted. Based on the impersonal wording (*"service that is normally provided for remuneration"* instead of wording such as *"a service that is normally provided by the service provider for remuneration"*) we assume it should be interpreted at a global level, *i.e.* on the level of the market and not at the level of a specific service provider. Hence, a service will be *in scope* when most of the service providers in the market provide the service for remuneration in most of the cases. We do not consider it unreasonable, however, to argue that the interpretation should instead occur at the individual service provider level, so that the criterion for a service to be *in scope* is whether the individual service provider concerned normally provides the service for remuneration. In this report, we will target at the interpretation at the market level, however.

[59] See C. ANDERSON, *Free - the future of a radical price*, 2009

online model, the risk exists that courts would consider that all service providers within this market will fall outside the scope of the eCommerce Directive.

> *The question also arises which market or category of service providers should be taken into account when assessing "normally". For example, should photo-sharing websites and photo selling websites be considered as being part of the same category? If this is the case, then all of the free photo-sharing websites would be "normally provided for remuneration"; if this is not the case, then even the paid photo-sharing websites would not be considered "normally provided for remuneration", because most of the photo-sharing websites are provided for free.*

Evaluation – Although no case law exists regarding the application of the criterion "normally provided for remuneration" to online services, there is a risk that some online activities could be deemed to not meet this criterion. Accordingly, such online activities will not be able to take advantage of the freedom of establishment, the freedom of online service delivery and the special liability protection.

Considering the potentially large impact of this potential issue, we therefore advise that, if it would not be resolved by case law, it could be envisaged to decouple the scope of the special liability regime from article 50 of the EC Treaty[60].

4.1.2. By electronic means

The definition of "information society services" requires a service to be provided *by electronic means*, i.e. on top of existing network infrastructure and telecom-related services[61]. Conversely, telecom-services and network infrastructure deal with low-level, physical signal transmission, and are defined as *"electronic communications services"* in Directive 2002/21/EC[62].

According to the definition of electronic communications services, information society services and electronic communications services need to be clearly distinguished, because *"[an electronic communications service] does not include information society services, as defined in article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks"* [63].

The definition of "information society services" itself also implies that information society services cannot consist of signal conveyance, as an information society service *"is entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means"* . In other words: an information society service *itself* is being transmitted, conveyed and received by some physical means.

As these definitions make it very clear that information society services cannot consist of low-level signal transmission, the question arises whether it is actually correct to assume that traditional internet access provision falls within the scope of article 12 of the eCommerce Directive, considering that the very essence of internet access provision consists of physical signal transmission. This issue is not widely

---

[60] It could also be a solution to decouple the scope of "information society services" from article 50 of the EC Treaty, as this would resolve this potential issue for the entire eCommerce Directive (instead of online the special liability regime). However, such would require a change of the EC Treaty.

[61] Typically at the application layer (layer 7) of the OSI network reference model: see L. GOLENIEWSKI and K. W. JARRETT, *Telecommunications Essentials, Second Edition*, 2006, part II, Chapter 5

[62] Article 2.c of Directive 2002/21/EC: *"'electronic communications service' means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting (...)"*

[63] *Ibid.* (underlining added)

discussed[64] – and most legal doctrine qualifies typical internet access providers as "mere conduit" providers[65] – although it seems to be recognized in Germany, France and Poland[66].

4.2. Ambiguities in articles 12 (mere conduit)

Communications network – Taking into account the aforementioned discussion regarding the definition of information society service and the lack of a definition of a *"communications network"*, one could argue that operators of chat networks, instant messaging networks or even peer-to-peer networks, are to be considered as mere conduit providers, as they *"provide access to a communications network"*. This may not be in line with the original intentions of the European legislator.

Select or modify information – In light of the growing amount of online threats (malware, server attacks, botnets, etc.), Internet access providers are increasingly inclined – or even legally required – to take measures to filter the internet traffic received by their customers. Furthermore, new revenue models are emerging, where internet access providers insert banners in webpages visited by users, in exchange for free internet access. Also, Voice-over-IP operators may want to periodically introduce spoken publicity during conversations, in exchange for a free service. As another example, operators of chat networks (to the extent they qualify as mere conduit service providers) may want to automatically block profanity wording and/or sexually oriented conversations.

Although recital 43 of the eCommerce Directive clarifies that *"manipulations of a technical nature which take place in the course of the transmission" should be allowed "as they do not alter the integrity of the information contained in the transmission"*, it is not clear whether traffic filtering, insertion of advertisements and textual filtering of chat conversations can be considered as such "manipulations of a technical nature". Hence, it is not clear whether these parties can still benefit from the liability exemption introduced by article 12.

4.3. Ambiguities in article 13 (caching)

Article 13 lists the conditions under which a caching service is exempted from liability[67]. This article 13 illustrates the technology-dependent drafting of the eCommerce Directive, as it was clearly conceived to protect traditional "proxy-servers"[68]. Although article 13 clearly targeted one specific technology (proxy-servers), the conditions set forth in article 13 can also be applied to other technologies, although such may not be in line with the original intentions of the European legislator.

---

[64] See, however, J. HARRINGTON, "Information society services: what are they and how relevant is the definition?", *Computer Law & Security Report,* Vol. 17, no. 3, 2001, p. 179. In this article, it is suggested that the provision at individual request may also not be fulfilled for access providers.

[65] See, however, I. WALDEN, "Discussion of Directive 2000/31/EC", in *Concise European IT law*, 2006, Kluwer law international, p. 248-249 (arguing that mere conduit access providers are subject to both article 12 and the telecommunication directives)

[66] Study on the liability of Internet intermediaries, p. 32. [*Drafting note: the study on the liability of Internet intermediaries refers to country reports of Germany, France and Poland, which are not available to us. This issue therefore needs to be further investigated, once the country reports are available.*]

[67] Article 13 describes caching as *"the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request"*.

[68] This is particularly illustrated by conditions (c) and (d) of article 13, which require the provider to comply with updating rules and hit counting rules "widely recognised and used by industry". These conditions only seem for proxy servers.

For example, the question has arisen whether "Usenet" newsgroups can be considered to be a form of caching. Usenet is a system in which users post messages to a newsgroup, which are then automatically broadcasted to, and mirrored on, other servers using a wide variety of networks[69]. Each server then retains the messages in each newsgroup for a limited amount of time. Although it is questionable whether this automatic redistribution of newsgroup messages is really performed *"for the sole purpose of making more efficient the information's onward transmission"*, the German Regional Court of Munich qualified the Usenet service as a caching provider. Meanwhile, other courts[70] qualified the Usenet service as a hosting service.

Similarly, various decentralised content distribution systems could also be qualified as caching providers, although only limited case law has emerged on this topic[71]. For example, the Domain Name System (DNS) uses a hierarchy of servers to distribute information across the globe regarding the mapping of each internet domain name to specific IP-addresses. Such system meets all the criteria set forth in article 13, although it is questionable whether such qualification would be in line with the spirit of article 13, which clearly targets proxy-servers. However, taking into account the increasing amount of domain name disputes, it is not unlikely that a court will face this question, when a plaintiff would request a top-level DNS-provider to block access to a specific domain name.

It would be even more controversial to qualify each peer-to-peer user[72] as a caching provider, although such could be in line with the letter of the eCommerce Directive[73].

4.4. Ambiguities in article 14 (hosting)

Out of all articles in Section 4 of the eCommerce Directive, article 14 has clearly spawned the greatest amount of discussion and case law.

> *This ambiguity was plainly recognised by the French artistic commission, who issued a report dedicated to this subject. Analysing the French and European legislation, it stated that "the Commission cannot conclude how participatory Web 2.0 websites should be qualified (...) so that one arrives at the boundaries of the concept of hosting provider" [74]. Accordingly, the Commission notes that the case law is dispersed on this subject.*

---

[69] C. REED, *Internet Law: Text and Materials*, London, Buttersworth, 2000, p. 26

[70] LG Düsseldorf, 23 May 2007, 12 O 151/07, MMR 2007, 534 (535); Queen's Bench Division, 10 March 2006, *Bunt v. Tilley,* as mentioned in T. VERBIEST, G. SPINDLER, G.M. RICCIO, A. VAN DER PERRE, *Study on liability of Internet intermediaries*, ordered by the European Commission, November 2007 (hereafter *"Study on the liability of Internet intermediaries"*), p. 34

[71] For example, according to German Courts the liability exemptions do not apply to domain name registries, as these exemptions only refer to the provision of content: see the (rather old) cases mentioned by the Study on liability of Internet intermediaries, p. 105

[72] leaving aside the question of whether participation in peer-to-peer networks meets the ambiguous "normally provided for remuneration" criterion described above in section 4.1.1

[73] For example, the popular Bittorrent protocol distributes information in a decentralised manner, whereby each user simultaneously downloads and uploads information from and to other users. This protocol is clearly intended to *"make more efficient the information's onward transmission to other recipients of the services"*. Furthermore, users do not modify the information that is being exchanged (condition a), there are generally no *access* conditions or *updating* conditions that apply (conditions b and c), there are no widely recognised technologies used by industry to obtain data on the use of the information (condition d) and it occurs only rarely that *"the information at the initial source of the transmission has been removed from the network, or access to it has been disabled"* (condition e). Each Bittorrent user may therefore qualify as a caching provider, although it should be recognised that this would require a rather literal interpretation of conditions (b) and (e) of article 13

[74] Conseil supérieur de la propriété littéraire et artistique, Commission spécialisée sur les prestatiares de l'internet, Rapport, 2008, p. 50, available at http://ec.europa.eu/internal_market/e-commerce/docs/expert/20080915_report_fr.pdf

"Consists of" – According to article 14, a hosting service *"consists of the storage of information provided by a recipient of the service"*. This *"consists of"* criterion is used to distinguish mere hosting providers (who are not involved in the creation of the content) from content providers (who are themselves involved in creating the content, and do not benefit from the special liability regime). Although this criterion may be very suitable for the traditional services for which it was conceived[75], its weaknesses become apparent when applied to other services[76], and particularly cloud computing services and other Web 2.0 services where storage is just one aspect of the entire service package.

The criterion's weakness essentially boils down to its failure to specify *to which extent* a service should relate to hosting: is it sufficient that *some* aspects of the service deal with hosting, should the *majority* of aspects deal with hosting, or should *all* aspects of the service deal with hosting? Due to the margin of appreciation left by the "consists of" criterion, courts have adopted various interpretations:

- The Court of Paris[77] ruled in June 2008 that *"the essence of eBay's service is to mediate between buyers and sellers"*, so that eBay cannot benefit from article 14, as *"it deploys a commercial, auction-related activity that is not limited to hosting"*. Such interpretation excludes article 14 when the hosting-related aspects of a service are not the **most important aspects of the service**.
- Several courts seem inclined to qualify a web service as a publishing activity when the service provider offers **editing tools**, or forces its users to adopt a **certain structure** in the content.

  For example, in the famous Lafesse v. MySpace case[78], the Court of Paris ruled in 2007 that, although social website MySpace indeed hosts information provided by its users *"[MySpace] does not limit itself to this function; indeed, by clearly offering a presentation structure via frames to its users, and by displaying banners during each visit from which it clearly draws profits, [MySpace] is an editor, and must take on the responsibilities of an editor"* [79]. Meanwhile, the Court of Paris did recognise video platform YouTube as a hosting provider in 2009[80], stating that the presentation structure and search facilities offered by YouTube did not influence its qualification as hosting provider.
- Instead of focusing on the editing tools / content structure, some German and Italian case law and doctrine focus on the question of whether the service provider has **"adopted" the third party content**, or has instead (seriously) distanced itself from this content. This doctrine refuses to qualify online service providers as hosting providers when the third party content *appears to be* the provider's own content[81].

  This criterion is also adopted by Advocat-General Poiares Maduro in the pending Google Adwords case[82]. The Advocate General argues that the Google Adwords service (which displays

---

[75] i.e., hosting web space to publish a website

[76] For example, e-mail services (temporary storage of e-mails) and newsgroup access (temporary storage of newsgroup "posts")

[77] Three separate cases of the same date, all issued by the Commercial Court of Paris, First Chamber, on 30 June 2008 (Louis Vuitton Malletier / Christian Dior Couture and Parfums Christian Dior, Kenzo, Givenchy et Guerlain v. eBay)

[78] T.G.I. Paris, réf., 22 June 2007, *Lafesse v. Myspace.*

[79] Still, in another famous case regarding a video sharing website less than one month later, the Court of Paris ruled that *"[DailyMotion] cannot be qualified as an editor, as the content is furnished by the users of the service"*, even though the editing facilities and banners offered by DailyMotion and MySpace are very similar from a functional point of view. (T.G.I. Paris, 13 July 2007, Nord-Ouest Production c. s.a. Dailymotion)

[80] Bayard Presse / YouTube LLC, TGI de Paris 3ème chambre, 2ème section, 10 July 2009, available at www.legalis.net/jurisprudence-decision.php3?id_article=2693

[81] P. BALBONI, p. 65-66

[82] Joined Cases C-236/08, C-237/08 and C-238/08 of Google France/Inc. v. Louis Vuitton Malletier e.a.

advertisements next to search results) is not protected by the special liability regime, because – although it stores certain information – the service is not neutral as regards the information it carries, because the display of ads stems from Google's relationship with its advertisers. Consequently, Google can be held liable for trademark infringements occurring through its Adwords service.

- Still other courts **subdivide** a single commercial service into several distinct activities, and only apply the special liability regime to some activities. For example, in France, the court of Troyes[83] considered in June 2008 that, although online auction provider eBay indeed provides hosting activities by storing photos and texts associated with items put up for sale, it also provides various other auction-related activities (rating systems, payment facilities, advertisement tools, etc.), to which article 14 does not apply[84]. The Tribunal de Grande Instance came to a similar decision in May 2009 [85].
- UK courts tend to differentiate between service providers that only *facilitate* infringements by a third party, and service providers that ***authorise* infringements** by a third party[86].
- Some courts do not seem to use a specific criterion, and qualify a service as a hosting service as soon as there is **some storage activity** involved[87].

"Under the control" – Article 14.2 holds that the liability exemption does not apply when the recipient of the service is acting *"under the authority or the control of the provider"*. It is indeed obvious that an employer who hosts illegal information created by an employee at the employer's request, should not benefit from the liability exemption.

Less obvious, however, is to which extent hosting providers can monitor and manipulate the information stored on their website. Community encyclopaedia Wikipedia, for example, is permanently monitored by a team of content managers, to ensure that the information being published is accurate, verifiable, built on solid sources, and excludes personal opinions. As these content managers have the possibility to modify and delete articles uploaded by other users, there is clearly a level of control being exercised. The same is true for many social community websites and blogs.

Another example is discussion forums, where there is already case law that exempts service providers from the special liability protection when the messages are moderated or compiled by a forum administrator[88].

Illegal information – Since the actual knowledge requirement only concerns knowledge of *illegal* activity, providers will need to make an assessment of what does and what does not constitute illegal information, in order to make a decision to block access to certain content. This has led to complaints of

---

[83] T.G.I. Troyes 4 June 2008, Hermès International v. eBay. The case concerned a counterfeited bag being put up for sale by one of eBay's customers.

[84] Identical analysis performed by the Brussels Court of Commerce, decision of July 31, 2008 (A/07/06032), although this court did not conclude that eBay was to be held liable. See E. MONTERO, 33/2008). Contrary to the French Courts, the Brussels Court did apply the liability protection to the hosting-related activities of eBay.

[85] Tribunal de grande instance de Paris, 3ème chambre, 13 May 2009, L'Oréal et autres / eBay France et autres

[86] Bunt v. Tilley, [2006] EWHC 407 (QB) at 22, as mentioned by P. BALBONI et al, *o.c.*, p. 67

[87] For operators of blogging websites, see the Greek case No 44/2008 of Rodopi Court of First Instance (website blogspot.com), published in Armenopoulos 2009/3, p. 406. According to this decision, the company that hosts the blog cannot be considered as the owner, the publisher, the director of editing and/or the editor of the blog posts themselves. The blog operator only provides space for the blogs, and does not initiate the transmission of information, does not choose the receiver of the transmission, does not choose or alter the transmitted information.

[88] Court of Amsterdam, 12 March 2009, regarding messages available at www.internetoplichting.nl

stakeholders[89], who feel incapable of taking up such responsibilities. The issue is aggravated by the fact that the answer to the question as to when content can be deemed manifestly unlawful is answered differently in various Member States. While the illegal nature of some types of information will be obvious to any person (*e.g.,* pirated copies of commercial software or recent Hollywood movies), the legal assessment becomes more difficult for cases of defamation or texts that may be in the public domain. Notice-and-takedown letters may therefore induce service providers to take down material without reason, if they do not want to have the material examined by a legally trained person[90].

> *For example, in Germany, trademark infringements were judged to be a obvious infringement, while an Austrian court found that such infringements could not be qualified as obvious[91]. In France, a judge found that the sale of copyrighted videogames under the counter price constituted a manifest infringement. On the subject of defamation, a Dutch court found that such content was not unmistakably unlawful, while an Austrian court ruled that insulting statements could be qualified as obvious, since anyone is capable of determining the defaming character of such statements[92].*

Required level of knowledge or awareness – Caching providers and hosting providers can only benefit from the limited liability regime when they expeditiously remove or disable access to illegal information as soon as they either *"have actual knowledge"* or *"are aware of facts or circumstances"* regarding this illegal information. While these concepts are crucial to adequately determine the liability of caching and hosting providers, the eCommerce Directive does not define what should be considered as "actual knowledge" or "awareness". Consequently, it is left to the courts to determine which level of knowledge or awareness is required.

This issue was discussed in a number of German court decisions[93]. It was decided that the term actual knowledge implies actual *human* knowledge, as opposed to computer knowledge. Negligence and conditional intent were not considered to constitute actual knowledge. In addition, German courts found that knowledge of *specific* illegal content is required, as opposed to a general awareness of the past presence of illegal material on a server[94]. Under German law, providers can only enjoy liability in the absence of facts or circumstances from which illegal activity or information would be apparent, a condition which is interpreted in German jurisprudence as the absence of gross negligence. A similar condition exists under Dutch law, where providers can not be held liable if they could not reasonable be expected to know of the illegal nature of an activity[95].

---

[89] See, for example, E. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", in *Le commerce électronique européen sur les rails?*, Bruylant, Brussels, 2001, p. 290-291

[90] In a test conducted in the Netherlands, where takedown letters regarding material that was clearly in the public domain, 7 out of 10 ISPs took down the allegedly infringing material (see http://www.bof.nl/docs/researchpaperSANE.pdf). See also section 5.2.3 (particularly footnote 174) below for a comparison with the United States, where this issue is even more relevant, as US hosting providers cannot be held liable by their users for taking down content by mistake.

[91] Study on liability of Internet intermediaries, p. 38

[92] www.internet4jurists.at/entscheidungen/olgi_114_05i.htm

[93] Study on liability of Internet intermediaries, p. 36

[94] BGH, 23/09/2003, VI ZR 335/02, *NJW* 2003, 3764

[95] Study on liability of Internet intermediaries, p. 37

4.5. No harmonised notice-and-takedown procedure

Although the majority of Member States have followed an almost *verbatim* transposition of articles 12, 13 and 14 of the eCommerce Directive[96], some examples can be found of diverging statutory implementations of article 14 and (to a limited extent) article 13. These implementation divergences concern, particularly[97], the notification procedure for hosting providers[98].

Caching providers and hosting providers can only benefit from the limited liability regime when they expeditiously remove or disable access to illegal information as soon as they either *"have actual knowledge"* [99] or *"are aware of facts or circumstances"* [100] regarding this illegal information. Despite the importance of these concepts, the eCommerce Directive does not define them, nor does it establish a procedure to establish the "actual knowledge" or "awareness", or define what should be considered "expeditiously". The eCommerce Directive does, however, allow Member States to *"[establish] specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information"* [101].

As a result, Member States have developed different practices for verifying the presence of the required level of knowledge, and right holders submit notices in a variety of forms[102]:

- Most Member States have not established formal notification procedures, although various criteria may have been developed in **case law** or **legal doctrine**.

  In the Netherlands, for example, the parliamentary preparatory works state explicitly that a "simple" message is not sufficient, whereas a court order will always be sufficient. In a Germany, case law considers that a notice that lacks detail as regards the claimed copyright, is not sufficient.

- Other Member States have not established a formal procedure in their laws, but have nevertheless certain **statutory criteria** that must be met by the notification.

  For example, a hosting provider is not required to remove or block access under Portuguese law *"only because of the fact that a third party is arguing an infringement"*, which restricts private notifications. The United Kingdom, on the other hand, requires courts to take into account all circumstances, in particular whether the notice was received through a specified means of contact, whether the notice included the contact details of the sender, and whether the location and unlawful nature of the information was described.

- Some Member States have established a **formal notification procedure** (commonly referred to as a *"notice-and-takedown procedure"*).

---

[96] Study on the liability of Internet intermediaries, p. 32, 33 and 34

[97] See Study on the liability of Internet intermediaries for other examples of divergences. In summary, for almost every aspect of article 14, there is at least one Member State that uses a different wording or a different approach. For example: the Netherlands, Portugal, Germany and the Czech Republic have slightly varied the words used in article 14 (p. 34); the Czech Republic, Hungary, Latvia, Malta, Poland, Slovak Republic and Spain do not distinguish between actual knowledge (for criminal liability claims) and awareness of facts / circumstances (for civil liability claims); Lithuania, Poland, Finland, the Slovak Republic and Sweden vary with respect to the requirement to remove or disable access to unlawful information; etc. Implementation differences for article 12 and article 13 are less pronounced between Member States.

[98] Although Member States also differ significantly regarding their interpretation of "illegal information", "actual knowledge" and "awareness", these differences result from court decisions, and are therefore discussed below in section 4.4 above

[99] requirement for caching providers (regardless of the type of claim) and hosting providers (for claims other than claims for damages)

[100] Requirement for hosting providers that are confronted with claims for damages. Hence, the threshold for incurring liability as a hosting provider due to claims for damages, is lower than the threshold for incurring liability due to other claims (such as criminal allegations).

[101] Recital 46

[102] Study on liability of Internet intermediaries, p. 14 and 41 onwards

Such is the case with Spain, where a "competent body" – such as a court or administrative authority – must order the removal or blocking of information, although this strict procedure does not seem to be followed by all Spanish courts[103]. Similarly, Italian law requires a notice from relevant authorities, although it is not clear whether hosting providers should inform their customers/users about the notification. Finish and Hungarian law have established detailed formal procedures, although they are limited to intellectual property infringements. French and Lithuanian law have opted for optional notification procedures.

Subsidiarity – It has been subject to debate whether some kind of subsidiarity principle applies regarding injunctions against providers. Such a principle would entail that right holders have to address the author of illegal content, before directing a claim against the host provider and (possibly after addressing the host provider) the access provider. French courts have used the subsidiarity principle by only ordering injunctions against access providers for cases where hosting providers refrained from acting, a practice later confirmed by the French Court of Appeal[104]. The German Federal Court of Justice, on the other hand, dismissed the principle of subsidiarity in the context of injunctions against host providers[105].

Disclosing information – Online intermediaries have been the target of claims for disclosure of information in a variety of cases, mainly concerning copyright infringement. Such claims have been directed against providers in various Member States with varying success. In Austria, successful claims for information have been made based on national intellectual property law, which explicitly provides for a right for copyright holders to demand information against intermediaries in case of copyright infringement[106]. Similar claims have been known to be granted in the Netherlands[107] and France[108]. In the common law Member States, the "Norwich Pharmacal rule" permits a court to order a third party to disclose documents related to a litigation in its possession. The rule has been applied to online intermediaries in Ireland and the UK, in copyright as well as defamation cases[109].

However, requests for information are sometimes also dismissed on data protection grounds. Italian, Belgian and German courts refused requests for information on the grounds that data protection regulation did not give providers the right to disclose user information[110]. For example, in an Italian copyright infringement case regarding the use of file-sharing networks, a court dismissing a claim for disclosure of information, based its opinion on arguments of the Data Protection Commissioner, who argued that the disclosure of user data and logs represented an invasion of privacy[111]. Under Irish data protection law, intermediaries are not allowed to share user information with anyone, although the Norwich Pharmacal rule provides an exception, if the claimant can obtain a court order[112].

---

[103] some case law pre-assumes "effective knowledge" due to the hosting provider's duty to monitor the content hosted by it (SGAE v. Asociacion de Internautas, case pending before the Supreme Court)

[104] Study on liability of Internet intermediaries, p. 50

[105] BGH, 27/03/2007, VI ZE 101/09, *MMR* 2007, 518

[106] Study on liability of Internet intermediaries, p. 77

[107] Court of The Hague, 05/01/2007, 276747/KG ZA 06-1417, available at www.rechtspraak.nl

[108] www.legalis.net/breves-article.php3?id_article=1648

[109] Study on liability of Internet intermediaries, p. 79

[110] Study on liability of Internet intermediaries, p. 81

[111] Tribunale di Roma, Sezione IX civile (IP specialized section), 09/02/2007, Peppermint Jam Records v. Telecom Italia

[112] Study on liability of Internet intermediaries, p. 82

4.6. Possibility of to issue injunctions

Although the eCommerce Directive protects providers of mere conduit, caching and hosting services against liability, the Directive explicitly mentions that *"[t]he limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it"* [113]. Thus, even when an online service provider would not be held liable for storing or transmitting third party content, it can still be ordered to remove third party content and/or prevent the alleged infringements from re-occurring in the future.

The possibility to issue injunctions against service providers should not be underestimated: while liability claims against mere conduit service providers (and caching service providers) are not important in court practice, injunctions are frequently issued against them. Injunctions therefore constitute important tools for plaintiffs[114].

Legal basis – Which types of injunctions can be requested by a plaintiff, depends on the Member State considered[115]. While a few Member States (Austria, France Italy, Sweden and the United Kingdom) have adopted specific provisions for injunctions against intermediaries, most Member States require plaintiffs to rely upon general procedural rules to request injunctions against online service providers. Such general procedures can have far-reaching effects: according to the German legal doctrine of accessory liability, all parties involved in a wrongdoing activity can become subject to the injunction, without necessarily being wrongdoers or participants.

Links with other Directives – In practice, many injunctions against online intermediaries are (directly or indirectly) based on the Enforcement Directive and Copyright Directive, which require Member States to provide for the possibility of injunctions:

> *Article 8.3 Copyright Directive: 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.*
>
> *Art. 11 Enforcement Directive: 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.*

Both Directives clearly state that they leave the eCommerce Directive untouched:

> *Consideration 16 of the Copyright Directive: This Directive is without prejudice to provisions relating to liability in [the Ecommerce Directive].*

---

[113] See articles 12.3, 13.2 and 14.3, as well as recital 45

[114] Study on liability of internet intermediaries, p. 66-69

[115] Study on liability of internet intermediaries, p. 52-66

> *Article 2.3 Enforcement Directive: This Directive shall not affect: (a) the Community provisions governing the substantive law on intellectual property, Directive 95/46/EC, Directive 1999/93/EC or Directive 2000/31/EC, in general, and Articles 12 to 15 of Directive 2000/31/EC in particular;*

Although the E-commerce, Copyright and Enforcement Directive do not seem to contradict each other, the question arises how the reconciliation between these three Directives should be accomplished in practice, because injunction (on whatever legal basis) must not lead to general obligations in practice.

Types of measures – Courts differ in the range of measures they impose: plaintiffs can ask to block access to certain websites[116], block access to file sharing networks, block infringing users[117], filter unauthorised copyrighted works from a customer's internet traffic[118], filter trademark-infringing auction items, or expose the contact details of the alleged infringers[119].

Diverging case law – Across Member States, courts react differently to requests for injunctions. While some courts seem openly sympathetic towards the plaintiff[120], other courts consider the injunctions to be disproportionate[121]. Still other courts openly admit that the possibility to issue injunctions and the relationship between the eCommerce Directive and the Enforcement Directive is highly unclear:

> *"I conclude that the scope of the obligation placed on Member States by the third sentence of Article 11 [of the Enforcement Diretive], and in particular the scope of the injunction which it requires to be available against intermediaries, is unclear. This is another matter upon which the guidance of the ECJ is required."* [122]

Also, Member States differ in whether or not they apply the principle of subsidiarity, which requires a plaintiff to first seek relief against the content provider, and only claim an injunction against the service provider as a last resort[123].

Preventing future infringements – Injunctions can not only impose the *termination* of an infringement, but also the prevention of future infringements. However, the prevention of future infringements often leads *de facto* to a general monitoring obligation for the hosting provider, and may therefore conflict with article 15 of the eCommerce Directive, which prohibits Member States to impose general monitoring obligations on service providers that fall within the scope of the special liability regime.

---

[116] See, for example the famous Danish "Tele2" case, in which access provider Tele2 was ordered to block access to the Russian webshop allofmp3.com (Court of Copenhagen, 25 October 2006)

[117] Google video case: Zadig Productions v. Google Inc., juris-data num. 2007-344344; RDLI 2007/32 num. 1062 obs. L. Coste

[118] Either by blocking a specific IP-address, or blocking the DNS-translation from a domain name to an IP-address

[119] Study on liability of internet intermediaries, p. 13

[120] For example, the Brussels Court of First Instance in the Sabam v. Tiscali/Scarlet cases (26 November 2004 and 29 June 2007), in which the court ordered internet access provider Tiscali/Scarlet to install filtering software to prevent copyright-infringing songs from being downloaded, even though there were various technical, operational and legal concerns associated with such filtering software; the Court of Copenhagen in the Tele2 case (25 October 2006); the Court of The Hague, which ordered internet access provider KPN to cut off customers' access to the Internet due to copyright infringements (5 January 2007)

[121] UK Queen's Bench Division, 10 March 2006, [2006] EWHC 407 (QB); [2006] 3 All ER 336; [2006] EMLR 523, Bunt v Tilley & Others

[122] nr. 465

[123] For example, French courts follow this principle, contrary to German courts: see Study on liability of internet intermediaries, p. 49-50

Courts across the EU have different opinions on the required conditions and the extent of injunctions to prevent future infringements. In Germany, the Federal Court of Justice decided that a provider should not only remove unlawful content of which it was informed, but should also take all technically feasible and reasonable precautions to prevent future infringements[124]. This decision was confirmed in 2008[125]. The German Court ruled that it was not sufficient to use a manual screening process consisting of six full time-employees, combined with a hashing system to prevent uploads of banned files[126].

In Austria, the Supreme Court decided that an obligation to monitor was legitimate, where the provider had obtained notice of at least one infringement so that the danger of further infringements by individual users was substantiated[127]. In France, the Court ruled in the *Dailymotion* case[128] that a service provider who was aware of the possibility that users upload illegal content, had an obligation to monitor this content before it was published on the website. Similarly, in the Google Video case[129], the Italian Court obliged the service provider to take measures to prevent that videos that had previously been removed due to their illegal nature, would be uploaded again.

Even more interesting is the Belgian Sabam v. Tiscali/Scarlet case (29 June 2007), in which the judge considered that the possibility to issue injunctions against an intermediary was in no way restricted by the eCommerce Directive, because the prohibition on general monitoring obligations is listed in section 4 of the eCommerce Directive (entitled *"Liability of intermediary service providers"*), while injunctions only concern the termination of infringements, and do not deal with *liability* at all.

> ***Practical example: videos on a social community.*** *In a currently pending case, a leading European video platform is being sued by a rightholders association. According to the plaintiff, the platform operator is an intermediary, who (based on article 8.3 of the Copyright Directive) must take all steps required to remove copyright-infringing videos from its platform.*
>
> *The platform operator, on the other hand, argues that the special liability regime does not allow the court to grant this request, as it would boil down to a general monitoring obligation.*
>
> *While the plaintiff does not hold the platform operator liable for the infringing material, it does ask the court to impose an injunction which – if granted – would immediately render the platform operator bankrupt, due to the sheer volume of videos available on the platform, which must be manually screened to comply with the plaintiff's request.*

Comparison with the US – It is interesting to note that, contrary to the eCommerce Directive, the US Digital Millennium Copyright Act – which also introduces a special liability regime for some service providers – explicitly includes the prevention of future infringements as a condition to fall within the scope

---

[124] BGH, 11/03/2004, ZE 304/01, *MMR* 2004, 668

[125] RapidShare cases: Oberlandesgericht Hamburg, 2 July 2008; District Court of Düsseldorf, 23 January 2008; Regional Court of Hamburg, 12 June 2009 (available at www.gema.de/fileadmin/inhaltsdateien/presse/pressemitteilungen/GEMA_RapidShare_Urteil_LG_Hamburg_vom_12062009.pdf)

[126] See http://arstechnica.com/tech-policy/news/2008/10/german-court-says-rapidshare-must-get-proactive-on-copyrighted-content.ars

[127] Study on liability of Internet intermediaries, p. 752

[128] T.G.I. Paris, 13 July 2007, Nord-Ouest Production c. s.a. Dailymotion

[129] See footnote 117

of the liability exemptions. Under the Digital Millennium Copyright Act, all types of online service providers must implement a policy to terminate repeating infringements[130].

Result: no liability, but similar costs incurred – The uncertainty surrounding the possibility to issue injunctions, also undermines the strength of the liability regime. Even when a service provider would not be held liable for certain infringement committed by its users, the practical consequences of an injunction will often lead to similar results (lawsuits, exposure, legal costs, technical costs, technical measures being imposed, etc.).

Meaning of recital 48 – Recital 48 holds that the eCommerce 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"*. It is not clear to which extent the reference to "duties of care" can allow Member States to introduce some kind of general obligation for hosting providers to monitor their systems, or may even broaden the ways by which a hosting provider may be deemed to obtain "knowledge" under article 14. Accordingly, it is not clear how recital 48 can be reconciled with articles 14 and 15, and most authors consider it a mere glitch[131].

4.7. Gaps in the scope of the special liability regime

Protection of search engines – Despite the importance of search engines for the functioning of the Internet, the eCommerce Directive does not set out a liability regime for these intermediaries, to which it refers as location tool services[132]. However, some Member States, such as Portugal and Spain, have provided for limitations to the liability of search engines by extending the special liability regime of the Directive[133]. Interestingly, the United States have also adopted a similar special liability regime for search engines[134]. While search engines seem to have fared pretty well at the hands of courts in most Member States, their position remains unclear for the time being[135]. Moreover, Advocate-General Poiares Maduro recently acknowledged that – contrary to the Google Adwords service – the Google search engine qualifies as a hosting service[136].

Although the European Commission has encouraged Member States to further develop legal security for internet intermediaries[137], some Member States, such as the United Kingdom, have adopted a minimalist

---

[130] See section 5.2.2 below

[131] R. BARCELO and K. KOELMAN, "Intermediary liability in the E-commerce Directive: so far so good, but it's not enough" in *Computer Law & Security Report*, Vol. 16, no. 4, 2000, p. 232; C. DE PRETER, "Wie heeft nog boodschap aan de boodschap? De aansprakelijkheid van tussenpersonen onder de Wet Elektronische Handel", *Auteurs & Media 2004*, p. 265-266; E. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", in *Le commerce électronique européen sur les rails?*, Bruylant, Brussels, 2001, p. 289

[132] Article 21 Electronic Commerce Directive

[133] COM/2003/0702, p 13

[134] See section 5.2 below

[135] See, for example, the UK case Designtechnica Corporation v. Google, available at www.bailii.org/ew/cases/EWHC/QB/2009/1765.html, in which the court concluded that it was unclear whether the provider of a search engine fell within the scope of articles 12 to 14 of the eCommerce Directive. The court also refers to similar cases where search engines were not held liable: Jensen v Google Netherlands (26 April 2007, court of Amsterdam); SARL Publison System v SARL Google France (Court of Appeal in Paris, 19 March 2009); Palomo v Google Inc (Court of First Instance in Madrid on 13 May 2009)

[136] Joined Cases C-236/08, C-237/08 and C-238/08 of Google France/Inc. v. Louis Vuitton Malletier e.a.

[137] *Ibid.*

approach to the adoption of the Directive and offer no additional protection[138]. The lack of harmonisation in this area seems problematic in view of the important function performed by search engines and their significant impact on the online world.

Protection for hyperlinking – Similar to the issue of search engines, the eCommerce Directive does not set out a specific liability regime for hyperlinks, although hyperlinks are at the very core of the functioning of the Internet, and have already triggered substantial case law. Only some countries, such as Austria, Spain and Portugal[139] (as well as Liechtenstein), have implemented a liability model for hyperlinking, based on article 14 of the Directive. As such, providers of hyperlinks cannot be held liable for changes to linked content of which they are not aware, unless notification has been given[140].

4.8. Result: considerable legal uncertainty

Due to the various ambiguities in the eCommerce Directive and the diverging national implementations of the eCommerce Directive, the manner in which courts and legal practitioners interpret the special liability regime across the EU, varies widely across EU Member States[141]. It seems that courts and legal practitioners find it difficult to apply the special liability regime, and seem inclined to find arguments to put aside the special liability regime and instead revert to more general rules of legal doctrine[142]. This may be linked to the fact that a Member state's approach to the issue of provider's liability is often based upon a general doctrine of contributory liability, which renders the horizontal liability exemptions provided for by the eCommerce Directive difficult to implement[143].

As a result, online service providers, users and third parties face considerable legal uncertainty in the European Community, in particular when it concerns services that do not qualify as the "traditional" internet access, caching or web hosting services envisaged by the eCommerce Directive.

While not all of the uncertainties and ambiguities enumerated above have been tested in court[144], we assume that it is only a matter of time before national case law is triggered in this regard. Other ambiguities – in particular the definition of hosting services – have already been discussed at length, although no convergence can be found across the Member States. Consequently, stakeholders are once again faced with legal uncertainty, as was the case before the introduction of the eCommerce

---

[138] See www.out-law.com/page-7670

[139] COM/2003/0702, p 13.

[140] Study on liability of Internet intermediaries, p. 18

[141] Study on liability of internet intermediaries, p. 30; A. SAINT MARTIN, "Les obligations du fournisseur d'hébergement Web 2.0", *Revue Lamy Droit de l'Immatériel,* 2008/36, p. 26

[142] Spanish legal doctrine even reports that in Spain *"some judgments simply have completely ignored the existence of a legal provision specifically aimed at excluding intermediary liability. (...) Indeed, the very existence of the exemption is not even mentioned, much less considered."* (M. PEGUERA, *"I just know that I (actually) know nothing"*: actual knowledge and other problems in ISP liability case law in Spain", *EIPR*, 2008, issue nr. 7, p. 281). It can be assumed that similar situations arise in other Member States.

A more recent Dutch example is the case LJN BJ1409, Rechtbank Utrecht, 267630 / KG ZA 09-5161, in which the court ruled that the eCommerce Directive does not protect an online service provider against data protection infringements committed by its users.

[143] Study on liability of Internet intermediaries, p. 30

[144] For example, we are not aware of case law regarding the ambiguities surrounding "normally provided for remuneration" (section 4.1.1), "by electronic means" (section 4.1.2) and "select or modify" (section 4.2).

Directive[145]. History therefore seems to repeat itself, despite the protective efforts of the eCommerce Directive[146], for example:

- **Costly involvement** – In 1996, the computer equipment of two French internet access providers was confiscated during a criminal investigation of acts performed by their users. Also in 2008, internet access providers can incur significant costs due to counter actions performed by their users, for example by having to install filters on their networks[147].
- **Criminal charges** – In 1996, the CEO of an internet access provider was personally convicted for having provided access to illegal third party information. In 2009, natural persons can still face criminal charges. For example, Google executives are personally prosecuted in Italy for an illegal video uploaded by a user[148].
- **Publisher's liability** – In 1996, French and Dutch national law reverted to a system of publisher's liability to assess defamation cases. Due to the specific nature of the Internet, the publisher's liability doctrine is often difficult to apply to an online context. However, despite the introduction of the eCommerce Directive, the publisher's liability doctrine is still frequently used by Courts[149].

5. Liability of online intermediaries in the United States

This section 5 discusses how the case law and legislation of the United States deal with the topic of online intermediary liability. Online intermediaries are essentially protected through three different channels in the United States: the case law on secondary liability, the Digital Millennium Copyright Act and the Communications Decency Act. Section 6 below will then compare the EU to the United States.

5.1. Case law secondary liability for copyright infringements

Types of secondary liability – US case law generally recognises two types of secondary liability in the context of copyright infringements: *contributory infringement* and *vicarious liability*. Contributory liability arises when a party with knowledge of another party's infringing conduct has materially contributed to that conduct, while vicarious liability is incurred when a defendant has enjoyed a financial benefit from the infringing conduct of another person, whose infringing conduct the defendant had the "right and ability to supervise"[150].

Sony Betamax case – The milestone case in which secondary liability for copyright infringements was first assessed, is the 1984 Sony Betamax case[151]. The US Supreme Court ruled that VCR manufacturer Sony was not liable for contributory infringement, even when some users would use Sony's VCR for the illegal copying of television shows, because its product was *"capable of substantial non-infringing uses"*.

---

[145] L. THOUMYRE, "Responsabilité 2.0 ou l'éternel recommencement", *Revue Lamy Droit de l'Immatériel,* 2007/33, n° 1098; E. BARBRY and O. PROUST, "Le Web 2.0 passe la barre des prétoires", *Gazette du Palais*, 18 October 2007, p. 10

[146] See also L. THOUMYRE, "Responsabilité 2.0 ou l'éternel recommencement", *RLDI 2007/33*, 1098; E. BARBRY and O. PROUST, "Le Web 2.0 passe la barre des prétoires", Gaz, Pal., 18 October 2007

[147] See footnotes 116 to 119.

[148] See J. CHENG, "Google execs facing Italian judges over teen beating video (updated)", *Ars Technica*, available at http://arstechnica.com/web/news/2009/02/google-execs-face-criminal-charges-in-italy-over-2006-video.ars. This case is pending before the Court of Milan.

[149] See MySpace case (footnote 78) and eBay case (footnote 77)

[150] M. SCOTT, "Safe harbors under the Digital Millennium Copyright Act", *New York University Journal of Legislation and Public Policy*, 2005, 9: 99, p. 104; P. MENELL and D. NIMMER, "Legal realism in action: indirect copyright liability's continuing tort framework and Sony's de facto demise", in *UC Berkeley Public Law Research Paper,* No. 966380, p. 26

[151] Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984)

This decision constituted an important restriction on secondary liability for copyright infringement, and is therefore often hailed as having spurred innovation[152]. Accordingly, the Sony Betamax decision forms an important protection for producers that can ensure that their service or product is capable of substantial non-infringing use.

Scope of the Sony Betamax protection – Although the Sony Betamax decision constitutes an important protection, several limitations should be pointed out. First, the protection is limited to copyright infringement. Second, some courts limit the Sony Betamax protection to contributory infringement, leaving open the possibility of vicarious liability[153]. Third, subsequent decisions[154] have not always been consistent, and have carved out this protection when an online service provider has actual knowledge and fails to block access to (or remove) the offending copyrighted material.

Refinement in the Grokster case – The Sony Betamax protection was further refined and carved out in the 2005 case against peer-to-peer software manufacturers Kazaa, Morpheus and Grokster[155], in which the Supreme Court held that an actor *"who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."* Consequently, even if a product would be capable of legal uses, a manufacturer would still be liable for intermediary infringement when the manufacturer induces its users to infringe third party rights[156], which requires both an affirmative act and intent on the part of the defendant to foster infringing uses[157].

Result – Despite the limitations in the scope of the Sony Betamax protection and the ambiguity created by inconsistent case law, the Sony Betamax decision is deemed central to any discussion of the secondary liability of online service providers[158]. Although the Sony Betamax defence was not accepted for high-profile cases involving services that were designed to infringe copyright, it seems to clear the way for service providers to experiment with new services that depend on third party content.

5.2. Digital Millennium Copyright Act

5.2.1. Overview

Introduction – The Digital Millennium Copyright Act ("DMCA"), adopted in 1998, was a legal compromise for the strong lobbying work of both content providers and online service providers[159]. On the one hand, it responded to the concern that online service providers would become so fearful of incurring secondary liability that they would be reluctant to invest in technological experimentation, while

---

[152] It is sometimes called the "Magna Carta" of product innovation and technology. See P. MENELL and D. NIMMER, *o.c.*, p. 2, although this author argues that the impact of the Sony Betamax decision should not be exaggerated, as the *"capable of substantial non-infringement use"* criterion has not prevented companies such as Napster, Aimster and Grokster from being held liable for secondary liability.

[153] See F. VON LOHMANN, *What Peer-to-Peer Developers Need to Know about Copyright Law*, January 2006, available on www.eff.org

[154] particularly the Napster, Aimster and Grokster cases, which deal with peer-to-peer technology to exchange (copyrighted) files between users

[155] MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005)

[156] See Z. LOCKE, *o.c.*, p. 19

[157] F. VON LOHMANN, *o.c.*, p. 9

[158] M. SCOTT, *o.c.*, p. 106

[159] P. SAMUELSON, "The Copyright Grab", *Wired News*, Jan. 1996, available at www.wired.com/wired/archive/4.01/white.paper_pr.html; URBAN and QUILTER, p. 621

on the other hand it also responded to the concern that copyright holders would refuse to make works available online unless they were assured that their works would be adequately protected. The DMCA made US law compliant with the 1996 WIPO copyright treaties[160], heightened the penalties for online copyright infringement and addressed issues such as anti-circumvention of protection measures and access restrictions.

Most importantly from a liability point of view, section 512 of the DMCA (entitled the Online Copyright Infringement Liability Limitation Act / "OCILLA") introduces a safe harbour to online service providers for copyright claims resulting from the conduct of their customers, in light of the emerging case law regarding contributory and vicarious liability of online service providers[161]. The safe harbour was conceived as to ensure that online service providers would have incentives to remove infringing material, while online service providers would also be protected from lawsuits and judgments based on secondary liability for their copyright infringements[162].

OCILLA – Similar to the eCommerce Directive, the DMCA reflects the state of the technology at the time the Act was adopted, and distinguishes between several types of functions that are protected from liability: mere conduit services, caching services and hosting services. Unlike the eCommerce Directive, however, the DMCA also recognises information location tools (search engines) as a fourth category of protected services. These four categories of services are subjected to various conditions that are broadly similar to the conditions imposed by Section 4 of the eCommerce Directive. For example, mere conduit service providers must not initiate the transmission, select the recipient or modify the content, while caching services must comply with information updating rules, and hosting providers (as well as search engine) must comply with notice-and-takedown requests. As is the case in the eCommerce Directive, online service providers are not required to actively monitor their systems for infringing activities[163].

Additional layer of protection – Similar to the eCommerce Directive[164], OCILLA only provides another layer of protection ("shield") for online service providers. When an online service provider does not meet the requirements of OCILLA, the additional layer of protection provided by OCILLA will not apply, so that the liability of the service provider will be assessed under traditional liability rules. Hence, OCILLA has merely added a second step to assessing infringement liability of service providers[165].

5.2.2. *Differences between OCILLA and the eCommerce Directive*

Despite their striking similarities, two interesting differences between OCILLA and the eCommerce Directive merit a further discussion.

Scope – While the eCommerce Directive protects the online service provider against liability for any type of infringement, OCILLA is strictly limited to copyright infringements.

---

[160] WIPO Copyright Treaty art. 11, Dec. 20, 1996 and the WIPO Performances and Phonograms Treaty

[161] M.P. GOLDSTEIN, "Service Provider Liability for Acts Committed By Users: What You Don't Know Can Hurt You", 18 *J. Marshall J. Computer & Info. L.* 591, 613 (2000)

[162] J.M. URBAN and L. QUILTER, "Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act", 22 *Santa Clara Comp. & High Tech. L.J.* 621 (2006), p. 622

[163] §512(m)

[164] See section 3.2 above

[165] CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 555 (4th Cir. 2004)

Termination policy – Unlike the eCommerce Directive, all types of online service providers (including mere conduit service providers) must implement a policy for termination of account holders who are repeat offenders, in order to benefit from the liability exemptions[166] [167].

Notice-and-takedown provisions – The E-Commerce Directive only states[168] that the service provider must expeditiously remove or disable access to illegal information, and leaves it up to the Member States to establish procedures to implement this requirement. Conversely, OCILLA sets forth a detailed notice-and-takedown procedure. When an online service provider receives a compliant takedown notice[169], the material must be taken down expeditiously, and reasonable steps must be undertaken by the service provider to notify the alleged infringer that the material has been removed[170]. The alleged infringer then has the possibility to file a counter-notice, which must be forwarded to the complainant by the service provider. In case such counter-notice has been submitted by the alleged infringer, the service provider must reinstate the allegedly infringing material if the complainant has not filed a lawsuit against the alleged infringer within 10-14 days.

5.2.3. *Evaluation*

The DMCA has been heavily debated, and its interpretation is far from settled[171]. The criticism can be summarized around three issues: incentives to take down, incentives to send, monitoring obligations, privacy concerns and notice requirements.

Incentives to take down – The DMCA is criticized for making it too easy for copyright owners to encourage website owners to take down allegedly infringing content and links which may in fact not be infringing. When online service providers receive a takedown notice, it is almost always in their interest to take down the material, even if it is not clear if infringement is taking place, because they will never be liable to take down the allegedly infringing material[172], also when it would turn out that the material is not infringing. In practice, online service providers are therefore strongly encouraged to take down the infringing material *"since no subscriber is worth even the price of a phone call to a lawyer to figure out*

---

[166] Section 512 (i): *"[adopt] and reasonably [implement] ... a policy that provides for the termination in appropriate circumstances of [users] ... who are repeat infringers"*

[167] Furthermore, §512(i) requires the systems of online service providers to accommodate standard technical measures broadly used in industry by copyright owners to identify or protected their copyrighted works

[168] Article 14.1.(b) and 14.3 of the eCommerce Directive

[169] The requirements for the takedown notice are set forth in §512(c)(3). The notice must be a written and signed communication sent to the "designated agent" of the service provider, which identifies the copyrighted work, the material that is claimed to be infringing, information on how to contact the complaining party, a statement that the complaining party has a good faith belief that the use of the material is unauthorised, as well as a statement that the information is accurate and the that the complaining party is authorised to act on behalf of the owner of the material. Interestingly, the complaining party is not required to give a description of the nature of the alleged infringement (see 17 U.S.C. § 512(c) (2000))

[170] Such notification must not be undertaken by search engines, as they rarely have the contact details of the alleged infringer.

[171] O. MEDENICA and K. WAHAB, "Does liability enhance credibility? Lessons from the DMCA applied to online defamation", *Cardozo Arts & Entertainment Law Journal*, Vol. 25:237, 2007, p. 258

[172] §512(g)(1) holds that *"a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing."*

what to do, it is easier just to cancel them" [173]. Anecdotal evidence indeed indicates that online service providers indeed take down content, even when the material is clearly not infringing[174].

> *Such anecdotal evidence also exists for the EU. For example, in a recent Dutch study (2009), a first researcher uploaded material to seven different high-profile social network sites. Next, a second researcher submitted a complained to each high-profile social network site, asking to take down the alleged copyrighted material uploaded by the first researcher. In reality, however, the uploaded material was not copyrighted, as the copyright protection had recently expired. However, among the seven social network sites, five sites (erroneously) removed the uploaded material.*[175]

Incentives to send takedown notices – Copyright holders are incentivised to send takedown notices. They are not required to describe which rights are infringed. Furthermore, only *"knowingly materially misrepresented"* takedown notices[176] can lead to liability of the copyright holder, so that non-compliant, vague or unfounded takedown notices will generally[177] not raise any liability for the copyright holder. As demonstrated by an ongoing study[178], the incentivation of copyright holders to send non-compliant takedown notices is not merely theoretical: out of a set of 876 takedown notices, almost one third contained at least one major non-compliance flaw[179], such as an issue with the underlying copyright claim[180], formal non-compliance[181] or non-applicability of the takedown procedure[182]. In practice, the DMCA shields copyright owners from liability for shutting down non-infringing content by mistake, *"even if the copyright owner acted unreasonably in making the mistake"*[183]. Only recently has some case law criticized evident notice-and-takedown abuses by copyright holders[184].

No incentive to counter-notify – Contrary to the incentives given to copyright holders to file a takedown notice, the DMCA is much more demanding with respect to the counter notice[185]. First, the content owner must wait until the allegedly infringing material is effectively removed, before he can take any action at

---

[173] M. SCOTT, *o.c.*, p. 129

[174] See (1) C. AHLERT, C. MARSDEN and C. YUNG, *How Liberty Disappeared From Cyberspace*, May 2003, available at http://pcmlp.socleg.ox.ac.uk/text/liberty.pdf. The authors posted texts that were clearly in the public domain on a free website hosted by a UK and a US ISP. The UK-based ISP promptly took down the site with minimal investigation, while the US-based ISP first requested compliance with the DMCA requirements; (2) In a similar follow-up test conducted in the Netherlands, 7 out of 10 ISPs took down the allegedly infringing material (see www.bof.nl/docs/researchpaperSANE.pdf)

[175] See http://ictrecht.nl/notice-takedown-rapport-communitysites-ictrecht-20090306.pdf

[176] §512(f)

[177] Contra: Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004), in which the Court ruled that the complainant (Diebold) should have known that internal corporate e-mails are not protected by copyright, and could therefore not be used to request a takedown. Despite this high-profile case, supported by pro bono legal support, the threshold for invoking §512(f) is very high, as the mere subjective belief that materials were infringing (even if that belief was incorrect) does not qualify as a *"knowing misrepresentation"*: J.M. URBAN and L. QUILTER, *o.c.*, p. 630

Rossi v. Motion Picture Ass'n of America, 391 F.3d 1000, 1004-05 (9th Cir. 2004).

[178] "Chilling Effects Project" (www.chillingeffects.org), a joint project of the Electronic Frontier Foundation and a consortium of law faculties, as reported by J.M. URBAN and L. QUILTER, *o.c.* One of the reasons to create this project, is to monitor the use of the notice-and-takedown procedures. In light of the fact that these procedures are handled by private parties, few cases actually reach a court, which renders it difficult to track such procedures.

[179] J.M. URBAN and L. QUILTER, *o.c.*, p. 666

[180] For example, takedown claims regarding information that is not copyrightable, takedown notices where a fair use defence clearly applied, or takedown notices relating to other areas than copyright (such as trademarks or unfair competition).

[181] such as a failure to identify the allegedly infringing material, or a failure to provide the complainant's contact information

[182] such as a takedown notice being sent to a mere conduit service provider

[183] M. SCOTT, *o.c.,* p. 101-102

[184] Lenz v. Universal Music Corp. (572 F. Supp. 2d 1150 (N.D.Ca. 2008))

[185] M. SCOTT, *o.c.*, p. 132

all. Secondly, the content owner must be willing to swear, under the penalty of perjury, that the material was removed as the result of "mistake or misidentification". Third, it is not clear whether this "mistake or misidentification" also covers an erroneous legal analysis. As a result, there is growing evidence that the counter-notification possibility is rarely used[186].

Privacy concerns – Regardless of whether the online service provider effectively takes down the material, copyright holders can issue a subpoena to the service provider, who is then legally obliged to disclose the identity of the alleged infringer to the copyright holder (assuming such information is in its possession)[187].

Effectiveness – Despite the various concerns, most legal commentators accept that the DMCA has spurred the development of new online services, in particular Web 2.0 services that deal with large amounts of third party content[188].

5.3. Communications Decency Act

5.3.1. Overview

First purpose – The Communications Decency Act[189] (*"CDA"*) was adopted in 1996 as a response to the rising concern over the impact of Internet pornography on children. It criminalises anyone who exposes minors to offensive, obscene or indecent material online.

Second purposes – At the same time, the CDA was a response to prior case law that penalised online service providers that had made efforts to police such material[190]. According to this prior case law – particularly the notorious *Stratton v. Prodigy* case[191] – online service providers that would monitor or edit the content hosted by them, were opened up to a greater liability than service providers that do not make such choice. Consequently, this case law induced service providers to refrain from monitoring any content hosted by them, as the less engaged they were with the content, the less likely they could be held liable[192].

---

[186] According to the data set gathered by Chilling Effects, only 7 counter-notifications were filed on a total of 2000 takedown notices

[187] §512(h)

[188] D. KRAVETS, *"10 Years Later, Misunderstood DMCA is the Law That Saved the Web"*, available at blog.wired.com/27bstroke6/2008/10/ten-years-later.html, 27 October 2008: *"If you're wondering whom to thank for the Web 2.0 explosion in interactive websites, consider sending a bouquet to Congress. Today's internet is largely an outgrowth of the much-reviled Digital Millennium Copyright Act"*

[189] The CDA constitutes Title V of the Telecom Act: see Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, 133–43

[190] O. MEDENICA and K. WAHAB, *o.c.*, p. 247

[191] In this case, the plaintiff (Stratton) sought to hold a network provider (Prodigy) liable for libellous comments posted on one of its bulletin boards. Although prior case law (*Cubby, Inc. v. CompuServe, Inc*, 1991) had considered a network operator to be a *distributor* (who is only liable for defamatory comments if he knew their libellous nature), the Court ruled that Prodigy was to be considered as a *publisher*, as it positioned itself as a family-oriented computer network and had advertised to exercise control over the content on its bulletin boards. As publishers are subject to a strict liability regime for defamatory content, the Court held Prodigy liable. See H. HOLLAND, "In defense of online intermediary immunity: facilitating communities of modified exceptionalism", *Kansas Law Review*, Vol. 56, 2007, p. 103-104

[192] O. MEDENICA and K. WAHAB, p. 248; L.P. MACHADO, "Immunity under §230 of the Communications Decency Act of 1996: a short primer", in *Journal of Internet law*, September 2006, p. 3

Content – As a direct response to this case law[193], the CDA also introduced a liability exemption against publisher's liability in its section 230: *"no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider"*. Furthermore, the CDA tries to encourage service providers to self-regulate content, as *"no provider or user of an interactive computer service shall be held liable on account of (...) any action voluntarily taken in good faith to restrict access to or availability of* [obscene material]*"*. Note that, contrary to the eCommerce Directive and the DMCA, the CDA does not require the service providers to comply with a notice-and-takedown procedure in order to benefit from the liability protection.

Although most of the CDA's anti-indecency provisions (§223) were held to be unconstitutional by the Supreme Court in 1997 due to a violation of the freedom of speech provisions of the First Amendment[194], the CDA's liability exemption (§230) still applies.

5.3.2. *Interpretation*

Service providers covered – Starting with the *Zeran v. America Online, Inc.* case[195], courts consistently extended the application of the CDA by using a broad definition of "interactive computer services", which is found to encompass hosting services, e-mail service providers, auction websites, general web shops, personal home pages, company websites, dating websites, chat rooms and internet access points. These parties are also allowed to make (minor) alterations to the information, while still benefiting from the liability protection[196].

Users covered – The courts have also made clear that not only providers, but also users of such services are within the scope of the protection: *"Congress did not intend for an internet user to be treated differently than an internet provider"* [197]. As a result, a user of a newsgroup cannot be held liable for reposting libellous comments made by another use [198], and a service provider cannot be held liable for the content published on its request[199].

Types of liability covered – Furthermore, although the text of the CDA only refers to *publisher's* and *speaker's* liability, the courts have considered that *distributor's* liability was covered by the CDA. Finally, the courts have expanded the types of claims against which protection is provided[200]: these not only include claims regarding defamation, but also sale/distribution of (child) pornography, sexual assault[201], distribution of incorrect information and privacy infringements. The only types of claims that are not covered by the CDA, relate to intellectual property infringements (including trademarks).

---

[193] Conference report on the CDA (H.R. Conf. Rep. No. 104-458 at 194 (1996)): *"One of the specific purposes of [Section 230] is to overrule Stratton-Oakmont v. Prodigy and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material."*

[194] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997)

[195] 129 F.3d 327 (4th Cir. 1997)

[196] See H. HOLLAND, *o.c.,* p. 105-107

[197] Barrett v. Rosenthal, 146 P.3d 510, 527 (Cal. 2006)

[198] *Ibid.*

[199] Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998), in which internet service provider AOL was not held liable for the defamatory statements made by columnist Matt Drudge, even though these defamatory statements were part of a set of rumour & gossip columns written by Drudge at the request of AOL.

[200] H. HOLLAND, *o.c.*, p. 106

[201] See Jane Doe v MySpace (available at http://en.wikisource.org/wiki/Doe_v._MySpace,_Inc.), in which a US District Court agreed that social community site MySpace is protected by the CDA from liability for the sexual assault and subsequent suicide of a 14-year-old girl who met her attacker on the website.

Minority view – It should be noted that the analysis below reflects the majority view on the CDA. There is some case law that adheres to a more narrow view on the protection offered by the CDA[202].

5.3.3. *Evaluation*

Very wide scope – The CDA shields online service providers from nearly all forms of tort liability for defamatory speech[203] and other types of content created by a third party[204], effectively becoming an absolute shield for service providers[205]. For example, in a delicate case of child pornography, the chat room owner was informed that photographs and videotapes were being exchanged. Even though the terms & conditions of the chat room allowed to terminate the membership of any member infringing the T&C, the chat room owner neither warned the member to stop, nor suspended access to the chat room. The Florida Supreme Court found the chat room owner to be immune under the CDA[206]. In another case, auction website eBay was found to be protected by the CDA for the sale of fraudulent autographed sports memorabilia, even though Bay was extensively informed about the fraud and did not undertake action[207]. The very wide scope of and effects of the CDA is criticised by US legal authors, who question whether the distinction between online service providers (who are almost absolutely shielded from liability claims) and offline players, such as printed newspapers (which are subject to a strict liability regime), is still valid in today's internet society.

Discouraging monitoring and self-regulation – Although the CDA was initially conceived to encourage online service providers to self-regulate, US case law relating to the CDA does not encourage service providers to self-regulate. Neither does the CDA incentivise online service providers to monitor the third party content hosted by them. On the contrary: due to the absence of a notice-and-takedown procedure in the CDA and the absolute shield accorded, online service providers are encouraged to take no action at all under the CDA. As from the *Zeran* case, US courts have clearly wanted to shield online service providers from the chilling effects of tort liability: *"[I]t would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted."* [208]

6. Comparison with the United States

This section 6 provides a high-level comparison of how the United States and the EU deal with the legal treatment of online intermediaries. These differences are then applied to various types of online service providers.

---

[202] See Doe v. GTE (347 F.3d 655 (7th Circ. 2003)) and Barnett v. Rosenthal (later on reversed by the Supreme Court of California). Some influential US authors also argue against broad protection for online intermediaries, because broad protection discourages intermediaries to take preventive measures, although they are closest to the source of the harm, so that it would be cheapest for society if these intermediaries are held liable for illegal material.

[203] O. MEDENICA and K. WAHAB, *o.c.*, p. 239-240

[204] L.P. MACADO, *o.c.*, p. 4

[205] O. MEDENICA and K. WAHAB, *o.c.,* p. 252

[206] Doe v. Am. Online, Inc., 783 So. 2d 1010 (Fla. 2001)

[207] Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 717 (Ct. App. 2002).

[208] Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997), at 331

6.1. Less protection and more uncertainty for online service providers

In the United States, online service providers seem well protected – perhaps even overly protected – against third party liability, due to the combination of a clear takedown procedure for copyright infringements, an extensive court interpretation of the exemption for defamatory content and an interesting "Sony Betamax" defence for services that are capable of substantial non-infringing use.

Although the information available to us indicates that the eCommerce Directive sufficiently protects "traditional" services that entirely correspond to the technologies available at the time the E-commerce Act was drafted (*i.e.,* internet access, caching and web hosting), the protection accorded to other types of online services is not clear. Accordingly, providers of new business models – particularly Web 2.0 models[209] – are less protected in Europe than in the United States against liability claims caused by third party content.

6.2. More uncertainty for rightholders and users

Although primarily online service providers are impacted by this legal uncertainty, it should be pointed out that other parties are also affected. For example, discussions between internet service providers and rightholders will often break down due to the varying case law and the divergent national laws, resulting in increased litigation. Furthermore, due to the lack of a harmonised, clear and detailed notice-and-takedown procedure, rightholders face greater legal costs and/or more uncertainty when trying to take down illegal information across the EU.

Users of online services may also be affected, as service providers may be become more cautious in their online offerings, or implement monitoring systems, in order to reduce the likelihood of liability claims. It is also interesting to note that, contrary to the wide protection granted by the CDA, users in the EU are not protected by liability exemptions when distributing content posted by other users.

6.3. Examples

In order to illustrate the concerns, it is useful to investigate several examples:

Traditional web space hosting – Traditional web space hosting – *i.e.,* providing space to upload files, which are subsequently published on a website – is clearly targeted by article 14, as evidenced by the term "hosting" in the heading of article 14, as well as legal doctrine[210]. However, web space hosting services offered by public authorities (universities, municipalities, ...) may not fall within the scope of article 14, contrary to the situation in the United States.

Internet access provision – Traditional internet access (by dial-up, ADSL, cable, satellite, ...) offered by commercial companies is said to fall within the scope of article 12[211]. However, internet access provision offered by public authorities may not fall within the scope of article 12. Furthermore, internet access provided by free wireless networks, citizen networks or distributed network anonymisation services, may not fall within the scope of article 12 either. Conversely, the US DMCA does not require remuneration, so that all examples enumerated will benefit from its protection regime.

File storage services – File storage services – *e.g.,* online backup services – qualify for protection as hosting providers under the eCommerce Directive (on the condition that service providers comply with

---

[209] French Commission Report, *o.c.*, p. 7

[210] R. BARCELO, "The European Directive on Electronic Commerce: an overview", in P. VAN EECKE and J. DUMORTIER, *Elektronische handel - commentaar bij de wetten van 11 maart 2003,* die keure, 2003, p. 291

[211] Although we refer to the ambiguity created by the definition of information society services: see section 4.1.2 above

the takedown provisions). Even so, service providers may be required to actively monitor files that are being uploaded by their users[212]. Conversely, in the United States, file storage services will likely be protected by the CDA and the DMCA.

Online auctions – As already pointed out in the introduction, French and Belgian courts do not qualify online auction providers (such as eBay) as hosting providers, as their services are not limited to the storage of information regarding auctioned items. In the United States, online auctions are protected by the CDA, although it should be pointed out that the scope of the CDA does not extend to copyright or trademark infringements.

Blogs – It is questionable whether writers of blogs[213] fall within the scope of the special liability regime of the eCommerce Directive when they would face liability questions due to comments being posted by their readers. First, it should be recognised that blogs are typically provided for free[214], so that the activity of writing a blog will often not qualify as an information society service. Second, the storage of reader comments is only a small part of the blog writing activity, so that courts are not likely to qualify blog writers as hosting providers. Conversely, US case law has accorded CDA protection to comments provided by third parties.

Discussion forums – The analysis of the liability of discussion forum operators is analogous to blog writers: the *"normally provided for remuneration"* requirement may not be met, and the act of storing discussions may not qualify as "hosting", as discussion forum operators may be involved in some of the discussions and discussion forums may also offer editing facilities. Conversely, US case law has accorded CDA protection to comments provided by third parties.

Wiki's – Similar to blogs and discussion forums, wiki's – which are often accessible for free – may not qualify for the special liability regime, as they may not meet the "normally provided for remuneration" criterion, they may provide facilities beyond mere storage (such as publishing tools, editing tools, revision history, ...) and they may exercise control over the content[215]. Some courts may, however, sub-divide the services offered by wiki's into various sub-services, and qualify only selected sub-services as hosting services. Again, US case law offers a better protection for such wiki's.

Chat networks – Operators of chat networks do not qualify as hosting or caching providers, but may qualify as mere conduit service providers, as they provide access to communication networks[216]. In order to benefit from the special liability regime, however, chat operators must refrain from filtering or modifying the chat conversations. Conversely, case law has applied the CDA protection to chat networks.

Virtual worlds – A considerable amount of courts will not consider operators of virtual worlds (such as Second Life) and multiplayer online games (such as World of Warcraft) to meet the conditions of the special liability regime, as storage-related facilities only constitute a small part of the service offering[217]. Some courts may, however, sub-divide the service into various sub-services.

---

[212] See footnote 125

[213] A different analysis applies to operators of blog tools, who are more likely to qualify as hosting providers vis-à-vis the blogs written by their users and the comments posted by blog readers.

[214] Some blog writers may be sponsored by advertising revenue.

[215] As an example, encyclopaedia Wikipedia is permanently monitored by a team of content managers, to ensure that the information being published is accurate, verifiable, built on solid sources, and excludes personal opinions.

[216] See section 4.2 above

[217] which also includes software to build characters and environments, chat facilities, programming tools, currency exchange, etc.

Social websites – Social community websites (such as MySpace, Netlog, Facebook and Twitter) offer tools to their users to build a personal profile online, publish photos, host music, post blog messages, communicate with friends, etc. Similar to virtual worlds, there is a risk that courts across the EU will not qualify social community websites as hosting providers, considering that storage is merely one of the various aspects of their services. Again, some courts may sub-divide the service into various sub-services.

Photo sharing websites – Even photo sharing websites (such as Flickr and PhotoBucket) may not qualify for the special liability regime, as they offer various tools to edit photos, order prints and communicate with other users.

Web services and "mash-ups" – The provision of software is shifting from a traditional licensing model towards a service-oriented architecture ("software as a service" model), where software and computing facilities are rented on an as-needed basis, and so-called "web services" from various vendors are concatenated. The integration of web services may result in a mash-up, *i.e.* a web application that integrates data from various sources and webservices.

While some of these web services involved may *store* information (and may thus qualify as "hosting services"), other web services merely *process* information, whereby storage would at most be a mere ephemeral phenomenon. On a conceptual level, the question arises why only the storage-related web services would qualify for protection under the eCommerce Directive (excluding other web services), while the amount of data being processed would call for protection of the online intermediary.

Cloud computing – Cloud computing refers to the internet-based ("cloud") development and use of computer technology, whereby dynamically scalable virtualised resources are provided "as a service over the Internet[218]. Cloud computing services are the latest trend in information processing technology, and encompass a variety of services, which may also relate to data storage. However, considering that cloud computing services are usually not limited to storage, it is questionable whether cloud computing service providers qualify as "hosting providers" under article 14 of the eCommerce Directive.

6.4. Dual protection regime

While the protection regime afforded to online intermediaries is stronger in the United States, this regime is not without issues either.

Contrary to the European Union, the United States uses a dual protection regime (the DMCA and the CDA, each with their own scope and purpose). It is only through the combination of both Acts that the United States offers a better protection than the European Union for online intermediaries. This dual protection regime results in a more fragmented regime than the approach taken by the European Union, because the DMCA and the CDA have a very different scope, and use different procedures (only the DMCA imposes a notice-and-takedown procedure).

The question arises whether this fragmentation is desirable from a policy point of view. For example, a right of an injured party of defamation is not protected at all under the CDA. On the other hand, the right of the intellectual property right holder is much more protected by the DMCA, because the right holder is likely to be successful in having the allegedly infringed material taken down. The question arises whether it is desirable to treat rights other than intellectual property rights in a subordinate way.

[218] See the Wikipedia-entry for cloud computing (*en.wikipedia.org/wiki/Cloud_computing*)

7. Conclusions

1. The special liability regime introduced by the eCommerce Directive has contributed to the further development of online services, particularly in the first years following the introduction of the Directive. Despite some court decisions to the contrary, the three traditional types of services targeted by the special liability regime (internet access, caching and web hosting) seem to have received adequate protection to further develop their services. The Directive has therefore **reached its goal of protecting traditional internet access providers, caching providers and web hosting companies** against liability caused by content provided by their users.
2. However, over the years, various weaknesses of this liability regime have emerged. One such weakness is formed by the **legal gaps** in the scope of the special liability regime: no uniform notice-and-takedown procedure, no uniform conditions regarding injunctions, no mandatory protection for search engines, and no mandatory protection for hyperlinking. These gaps, in particular the lack of a uniform notice-and-takedown procedure and the lack of uniform conditions regarding injunctions, have led to considerable divergences across Member States, which is likely resulting in increased costs and risks for cross-border transactions. These legal gaps no longer seem justified, in particular when compared to the United States.
3. The special liability regime is **too focused on (only) three types of services**. While the focus on these services was arguably relevant at the time when the Directive was drafted – because these were the services that needed protection at that time – a staggering amount of new types of services and service delivery models have developed, which are increasingly exposed to liability issues, due to the fact that the scope of the special liability regime is **too specific**, **too dependent on particular technologies**. As a result, an entire list of, particularly new, service models — including Web 2.0 services, cloud computing services and web services — are not protected, contrary to a highly specific service such as caching. It is difficult to find a justification for this discrepancy.
4. The **scope of "hosting services"** is ambiguous, and has triggered diametrically opposing decisions from courts across the EU. The most important cause of confusion is the requirement that a hosting service must *"consist of"* the storage of information. When intermediary immunity was first introduced, there was a clear economic separation between the intermediary and the content originators. However, modern intermediary business models are moving away from this clear separation. This leads to the question of to which extent heterogeneous/hybrid services (such as auction services, content sharing services, wiki's, cloud computing services, web services, etc.) can be considered hosting services. Accordingly, if the overarching aspects of a service do not relate to storage, there is a considerable risk that the service no longer qualifies for protection under the special liability regime.

   Another ambiguity in this regard is the assumption of article 14 that hosting providers have no interest in the relationship between the communicating parties. This divide is increasingly blurred. Service providers sometimes do exercise some level of editorial control (for example, when moderating or compiling user contributions), although the bulk of the content remains user-contributed. Similarly, online auction providers do not merely provide a sales platform to sellers, but also advise their users on effective selling techniques and shares in their success[219].
5. The special liability regime allows courts to **issue injunctions**: even when online service providers would not be liable for storing or transmitting third party content, they can still be ordered to remove third party content and/or prevent the alleged infringements from re-occurring in the future. Member States vary to a significant degree as to the conditions for an injunction to be issued, as well as the

[219] C. REED, "Policies for Intermediary Immunity", *Computers & Law*, February & March 2009, p. 20-23

different types of measures that can be imposed on service providers. The uncertainty surrounding the possibility to issue injunctions should not be underestimated, as injunctions can lead to costly lawsuits, public exposure and technical implementation costs for service providers.

6. **Various ambiguities** in the special liability regime undermine its strength, triggering uncertainty among stakeholders and courts. History therefore also repeats itself with respect to the divergences in national case law. The most detrimental ambiguities can be summarised as follows:

   - The fundamental definition of "information society services" excludes services that are not *"normally provided for remuneration"*. Depending on the interpretation, this may create uncertainty for online activities that are provided for free, depend on indirect revenue models or are provided by public authorities. This criterion particularly risks to expose "freemium" web services to liability.
   - It may be the case that various decentralised content distribution systems, including popular peer-to-peer networks, can be qualified as "caching services", so that their users would enjoy considerable protection under the special liability regime.
   - It is not clear for online service providers which information qualifies as "illegal information", which must be removed or blocked by online service providers.

7. The legal gaps of the eCommerce Directive, its dependence on specific services, its various ambiguities and its restricted scope lead to **diverging case law**, across (but sometimes also within) Member States, and thus considerable legal uncertainty for online service providers. There is abundance evidence that courts and legal practitioners encounter difficulties to apply the special liability regime, and seem inclined to find arguments to put aside the special liability regime and instead revert to more general rules of legal doctrine. This results in **considerable legal uncertainty for online service providers**, in particular for new service models.

8. Meanwhile, **in the United States**, online service providers benefit from an **almost absolute protection** under the Communications Decency Act for a variety of liability claims caused by third party content, including defamation, distribution of unlawful content and incorrect information, as well as privacy infringements. Although this almost absolute shield does not protect online service providers against intellectual property claims in the US, they are also better protected against these claims due to the Digital Millennium Copyright Act's **straightforward and harmonised notice-and-takedown procedure**. There are clear indications, however, that the US notice-and-takedown procedure gives too much incentives to service providers to always block / remove third party content when receiving a claim (which may chill free speech and foster censorship by copyright holders). Finally, also **US case law relating to secondary liability** incentivizes service providers to experiment with services that depend on third party content, as they are deemed exempted from liability when their services are capable of substantial non-infringing use.

9. **Japan** has also adopted a legal framework which protects online intermediaries against third party liability. Contrary to the European and American approaches, the Japanese special liability regime does not divide service providers into three / four subcategories[220]. Instead, the liability protection applies to *any* online service provider whose purpose is to communicate third party information to other parties, whether or not such service is offered for remuneration. Similar to the eCommerce Directive, the Japanese legal framework protects against any type of liability, but does not protect against injunctions. Interestingly, the Japanese legal framework also protects the intermediary against claims from its users for having wrongfully taken down illegal material.

[220] See www.soumu.go.jp/main_sosiki/joho_tsusin/chikujyokaisetu.pdf

Hence, the United States and Japan offer a significantly better level of liability protection to "new" types of online services, such as Web 2.0 and cloud computing services.

8. Recommendations

In this section, we provide a list of recommendations to solve various issues identified in this chapter. A distinction is made between recommendations that can be implemented on the short term (2010-2015), the mid-term (2015-2020) and the long term (2020 and beyond). These time frames align with the relative political and legal difficulty to implement these recommendations, as well as the urgency involved. Hence, the threshold for implementing recommendations for the short term is relatively low, or the urgency involved is rather high. Conversely, recommendations for the mid-term require important legal modifications, or may receive more political resistance. Recommendations for the long term are of a more visionary nature.

8.1. Overview of recommendations

8.1.1. Scope of "information society services"

Taking into account the ambiguities relating to the criterion of "normally provided for remuneration", the risk exists that case law may arise that would consider that some types of mere conduit / caching / hosting activities do not qualify as "information society services" because they are provided for free, or are remunerated only very remotely. Accordingly, such activities would not be protected by the special liability regime, and would not benefit from the freedom of establishment and the freedom of online service delivery (even when they would meet all other criteria set forth in articles 12 to 14).

When this ambiguity would not be resolved by case law, we recommend to consider adopting a different criterion.

> *It could, for example, be envisaged to abolish the requirement that activities must constitute economic activities, as it is difficult to justify why economic activities merit a better protection level than non-economic activities.*

In the short or medium term, this different criterion could be used to define the scope of the special liability regime[221]. However, in order to also use this different criterion for the freedom of establishment and the freedom of service delivery, a change of the EC Treaty will be necessary. Such will, obviously, only be possible in the long term.

8.1.2. Optimised wording

In the short term, several flaws in the wording of the eCommerce Directive should be fixed, in order to render the definition of "information society services" and the concepts used in articles 12 to 14 more suitable for new technologies and new business models, and to improve legal certainty.

Selection or modification – The "selection or modification of information" criterion for mere conduit providers should be changed to avoid that minor selections or modifications to the information transmitted, undermine the applicability of the special liability regime.

[221] because the scope of the special liability regime is not necessarily restricted by the scope of article 50 of the EC Treaty (which deals with the essential freedoms)

Mere conduit – In order to resolve the issue described in section 4.1.2 – *i.e.,* "mere conduit" services cannot deal with physical signal transmission – we recommend to clarify the scope of "mere conduit" services, by removing the *"normally provided for remuneration"* requirement (e.g., by the decoupling described above) and clarifying that mere conduit services also encompass *"electronic communication services"*, as defined in Directive 2002/21/EC[222].

Caching – Although several ambiguities can be found in the definition of caching, we do not consider it a priority to clarify this definition in the short term[223]. In the medium term, however, we recommend to merge the caching exemption in a broader field of protected services.

8.1.3. Hosting

The definition of hosting services has arguably triggered most of the case law concerning the special liability regime. We therefore recommend to at least clarify this definition, and also to resolve – if possible – the discrimination between storage-focused services and information-processing services.

Short term – In the short term, the definition of hosting service could – for example – be redefined as an information society service that consists, in at least one aspect, in the storage of information provided by a recipient of the service. It should then also be clarified that related information society services together constitute one information society service.

Mid-term – In the medium to long term[224], we would consider it appropriate to replace the current three-fold structure of the special liability regime by a two-fold structure, consisting of:

- mere conduit service providers; and
- third party information processors, *i.e.* anyone who provides a services for which at least one non-trivial aspect consists of the *processing* of information provided by a recipient of the service (whereby processes is to be construed as including activities such as collecting, indexing, hyperlinking, storing, recording, organising, publishing, altering, consulting, using, etc.) [225]

The protection of caching services – which is too technology-specific and does not seem to be frequently invoked anyway – would then be distributed over both categories: the transmission aspects would be covered by the protection of mere conduit service providers, while the storage aspects would be covered by the protection of third party information processors. Conversely, search engines and hyperlinking activities would be subsumed entirely by the second category.

In our opinion, such larger protection of information society providers, would foster the further uptake of online services. However, this enlargement should always be balanced by an appropriate notice-and-takedown procedure (for example the procedure outlined above in section 8.1.4), as well as a *"Grokster-like"* provision[226] to counter online piracy and alleviate concerns of copyright holders. Such provision

---

[222] Provided, of course, that the "normally provided for remuneration" requirement is also removed from the definition of "electronic communication service"

[223] Should clarification nevertheless be considered (and the caching exemption would not be merged into a broader exemption), we would recommend to clarify to which extent hierarchically distributed systems fall within the scope of the caching exemption.

[224] Assuming that the recommendations for the short term have been implemented

[225] Our proposal is similar to the proposals of C. REED, "Policies for Intermediary Immunity", *Computers & Law*, February & March 2009, p. 20-23. He claims that *"immunity should be granted to those whose primary function in respect of content is communicating it on behalf of others. Secondary activities would not normally affect immunity"*.

[226] In the famous 1984 case against Sony, the US Supreme Court held that Sony had no liability for manufacturing VCRs, even though some users would use Sony's VCR for the illegal copying of television shows. According to this decision, a

would exclude companies that offer services that *induce users to infringe third party rights*. According to this test, companies do not incur liability when their products or services do not induce infringements by users, even though some users would use the services in a clearly infringing manner.

Good faith control – Online service providers that exercise good-faith control over third party content hosted by them (*e.g.,* cleaning up offending user comments on a blog; removing spam messages from a forum; monitoring offensive language in a chat room; etc.) must not loose the protection afforded by the special liability regime.

8.1.4. Notice-and-takedown

A harmonised, detailed and clear notice-and-takedown procedure should be introduced[227], which balances the rights of the online service providers, the service users, as well as the plaintiffs.

DMCA-like model – As a starting point, we are of the opinion that it could be interesting to investigate the procedural model used by the DMCA. However, considering that the DMCA clearly favours plaintiffs (and, secondarily, the service providers) to the detriment of the service users, we propose to alter the DMCA takedown procedure, so that the infringing material would not be taken down immediately. This is also the approach taken by the Japanese legal framework on the liability of online intermediaries[228].

Similar to the Japanese approach, we propose that the service provider must forward the claim to the user. Provided the user has not responded, or does not contest the plaintiff's claim within a reasonably short period of time (*e.g.,* five business days), the service provider must then take down the material. The service provider should, however, immediately take down certain types of material, for which the infringement is highly obvious to any person (*e.g.*, child pornography, obvious racist material, or piracy of (recent) audiovisual material).

---

manufacturer would escape intermediary liability when its product is *"capable of substantial non-infringing uses"* (Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984)). This doctrine was further refined in the 2005 case against peer-to-peer software manufacturer Grokster (Grokster, 545 U.S. 931), in which the Court added that – even if a product would be capable of legal uses – a manufacturer would still be liable for intermediary infringement when the manufacturer *induces its users to infringe third party rights*. See Z. LOCKE, *o.c.*, p. 19

[227] The question arises, however, whether the European Community is competent to harmonise procedural law (such as a notice-and-takedown procedure) in light of article 65 of the EC Treaty, and the principles of subsidiarity and proportionality. Article 65 empowers the European Community to adopt measures in the field of judicial cooperation, and has generally been used to adopt "classical" private international law regulations. During the legislative procedure to adopt the regulation on a European order for payment procedures (1986/2006) and the regulation regarding a European small claims procedure (861/2007), the competence of the European Community to regulate procedural law, was discussed. Although the Commission and the Economic and Social Committee maintained the view that the scope of such procedures should not be limited to cross-border disputes, this view was not supported by the Parliament and the Council, so that both procedures were eventually limited to cross-border disputes. Hence, there are concerns with respect to the possibility to adopt a harmonised notice-and-takedown procedure, which should be further investigated. It should be noted, however, that voices are raised to further debate the scope of article 65 EC Treaty (See X.E. KRAMER, "A Major Step in the Harmonization of Procedural Law in Europe: the European Small Claims Procedure", in *A.W. JONGBLOED (ed.), The XIIIth World Congress of Procedural Law: the Belgian and Dutch Reports, 2008*, Antwerp, Intersentia, p. 15)

[228] The intermediary must first convey the takedown claim to its user. If the user consents to the blocking or fails to reply within seven days thereafter, the intermediary may block the right-infringing material without being liable to its user. According to the official comments on the legal framework, this procedure balances the interests of both the claimant and user: in order not to overly restrict the user's speech right, he/she is given an opportunity to reply before his/her material being blocked.

Dedicated agents – Considering that notice-and-takedown procedures are more likely for specific services – such as auction websites – and taking into account that it can be difficult and costly for service providers to assess whether material is effectively infringing, it could be interesting to introduce sector-specific, dedicated (yet independent) third party agents who would be involved in the takedown procedure.

> *For example, in case a manufacturer would determine that a counterfeited product is offered for sale on an auction website, the manufacturer can contact the service provider's dedicated takedown agent (when no such agent would be known for a particular service provider, the country-level or sector-level agent can be contacted). This agent will then investigate the claim, and inform the service provider whether or not the claim is justified. If the claim is justified, the infringing material would be taken down immediately after the agent's decision, and the user would be informed. If either the user or the manufacturer would object against the decision of the agent, a court procedure can be initiated.*
>
> *Both the user and the manufacturer should, however, be incentivised to not initiate legal procedures in vain. This could be achieved, for example, by requiring that the party which loses the lawsuit, has to pay the costs of the lawsuit and [three] times the cost of the agent (whereby the agent, the service provider and the winning party would be entitled to one third).*
>
> *Finally, a scheme may be envisaged whereby the general cost of the agent would be borne by a sector-level cost distribution mechanism.*

Standards and self-regulation – In addition to (or as an alternative to) dedicated agents, the European Commission should foster the creation of standards on how rightholders can cooperate with online intermediaries to make the notice-and-takedown procedure as efficient as possible for all parties involved. On large online platforms (such as video sharing platforms or online auctions), it can be burdensome for a rightholder to manually check whether the available content infringes its rights.

Technical standards should specify how selected rightholders (or rightholders associations or the dedicated agents described above) get privileged access to the platform and dedicated tools to search for infringements, while respecting the privacy of users and confidentiality of transactions/material. These standards should also specify how the rightholder can suspend a transaction/material, and how the platform user can protest against the takedown.

> *A well-known example is the Verified Rights Owner (VeRO) program of eBay, which provides right owners with additional possibilities to help reporting listings that infringe their rights. VeRO offers dedicated communication channels, with priority e-mail queues for reporting alleged infringements and offers rapid responses by eBay in ending listings reported as infringing. In addition, right owners subscribed to the VeRO program have the ability to obtain identifying information about eBay users (including name, address, phone number and e-mail address)[229] in case of infringements[230].*

While adoption of the standards would be optional (but recommended) for most online service providers, the standards should be mandatory for online platforms that are both sufficiently large and (by their nature or implementation) attract a non-trivial amount of infringing material. It is important to find such a threshold towards mandatory adoption that protects the interests of rightholders, yet does not discourage the creation of new platforms.

---

[229] eBay VeRO Programme, available at http://pages.ebay.co.uk/vero/about.html

[230] eBay Privacy Policy, available at http://pages.ebay.co.uk/help/policies/privacy-policy.html#disclosure_new

8.1.5. Injunctions

Mere conduit – In today's connected society, providers of central connectivity services (such as internet access and internet backbone operations, but also central DNS systems) are becoming increasingly important. As these service providers are technically involved in various steps of the information delivery workflow, they are increasingly facing injunctions to solve issues that arise between private parties with whom the service provider may even not have any (contractual) relationship.

We are of the opinion that such injunctions must be limited to the fullest extent possible. In other words, the special liability regime must be enlarged to not only protect these parties against liability, but also against costly and burdensome procedures initiated against them. We recommend to only allow injunctions when both the legal and technical costs associated with the injunction would be borne by the plaintiff[231], and all other legal (or technical) actions have been exhausted so that the injunction against the mere conduit service provider is a last resort. Injunctions against central connectivity service providers should also remain possible in urgent and seriously threatening cases.

Other online service providers – Injunctions against online intermediaries other than mere conduit service providers, are reported to be fairly limited in court practice[232]. When it is also taking into consideration that the link between such intermediaries and their users is often more direct, and that their role is less central than the role of central connectivity providers, we do not consider it necessary at this moment to limit or harmonise injunctions against them.

8.1.6. Long term

Taking into account today's continuing trend of contradicting court decisions, we are convinced that the extra protection accorded to some online service providers is necessary in the short and medium term (if only to "educate" courts and legal practitioners on the business models and technical aspects of online services), particularly due to the fact that many online service providers inherently operate cross-border.

However, in the long run, we think that this distinction between online and offline service providers (the so-called *"dualism"* or *"internet exceptionalism"* [233]) should no longer be made, as we assume that the specific characteristics of internet services will become familiar to all legal practitioners, so that the "training wheels" accorded by the eCommerce Directive can be left out.

---

[231] This will, in most cases, avoid that the scope of the requested injunction would be too large. For example, a rights holder will not request a service provider to screen each and every file uploaded by its users, because this would easily become prohibitively expensive.

[232] See *Study on liability of internet intermediaries*, p. 32

[233] See H. HOLLAND, *o.c.*; J. HUGHES, "The Internet and the Persistence of law", *Boston Col. L. Rev*, 2003