jipitec

2 | 2013

Volume 4 (2013)
Issue 2
ISSN 2190-3387

Journal of Intellectual Property, Information Technology, and Electronic Commerce Law

Articles

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 4 Issue 2, August 2013
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

Prof. Dr. Thomas Dreier, M. C. J., Karlsruhe Institute of Technology, Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe

Prof. Dr. Axel Metzger, LL. M., Institute for Legal Informatics, Leibniz Universität Hannover, Königsworther Platz 1, 30167 Hannover

Prof. Dr. Gerald Spindler, Dipl.-Ökonom, Georg-August-Universität Göttingen, Platz der Göttinger Sieben 6, 37073 Göttingen

Karlsruhe Institute of Technology, Leibniz Universität Hannover, and Georg-August-Universität Göttingen are corporations under public law, and represented by their respective presidents.

ISSN 2190-3387

Funded by
DFG Deutsche Forschungsgemeinschaft

Table Of Contents

Articles

Online Sexual Harassment

Issues & Solutions

by Mohamed Chawki, LL.B, BA, LL.M, Ph.D, St. Center for Terrorism Law, St. Mary's University, Texas, USA
Yassin el Shazly, LL.B, LL.M, Ph.D, University of Ain-Shams, Cairo, Egypt

Abstract: This paper addresses and analyses the growing threat of sexual harassment in cyberspace. Digital transactions and communications have, over the past decade, been increasingly transpiring at an increasingly accelerated rate. This non-linear progression has generated a myriad of risks associated with the utilization of information and communication technologies (ICTs) in cyberspace communications, amongst the most important of which is: the threat of sexual harassment. On such account, this paper aims to provide an overview of the issues and risks pertinent to sexual harassment and seeks to offer some solutions based on the necessity of pursuing a tri-fold policy encompassing strategic and regulatory, technical, and cultural approaches.

Keywords: Social Networking Sites (SNS); Bullying; Sexting; Legislation; Regulation

Recommended citation: Mohamed Chawki, Yassin el Shazly, Online Sexual Harassment: Issues & Solutions 4 (2013) JIPITEC 2, para 71.

A. Introduction

> *Sexual harassment is a well-known social problem that affects people at work, school, military installations, and social gatherings. (Barak, 2005)*
>
> *A worldwide phenomenon, it has been thoroughly investigated in recent decades in terms of prevalence, correlates, individual and organiational outcomes, and prevention; the range of studies provides an interdisciplinary perspective covering psychological, sociological, medical, legal, and educational aspe1cts of the phenomenon. (Ibid)*

1 Although men face harassment, women are the most likely victims.[2] In many environments on the Internet, some users find themselves so captivated by their cyberspace lifestyle that they want to spend more and more time there, sometimes to the neglect of their in-person life (Suler, 1999). They may not be entirely sure why they find themselves so engrossed. They can't accurately verbalize an explanation for their 'addiction'. The humorous substitution of words in the Palace Spa suggests that it is an unnameable 'thing' – a compelling, unnameable, hidden force. It's not the chat room or the newsgroup or the e-mail that is eating one's life, but the internal, unconscious dynamic it has ignited (Ibid). Indeed, the Internet has two faces, positive and negative (Barak and King, 2000). Its positive aspect is that it enables the enrichment and improvement of human functioning in many areas, including health, education, commerce and entertainment. On its negative side, the Internet may provide a threatening environment and expose individuals to great risks (Ibid).

2 In the context of women using the Internet, Morahan-Martin (2000) noted the 'promise and perils' facing female Net users. Sexual harassment and offence on the Internet is considered a major obstacle to the free, legitimate, functional and joyful use of the Net, as these acts drive away Net users as well as cause significant emotional harm and actual damage to those who remain users, whether by choice or by duty.

B. Harassment in Cyberspace

3 'Sexual harassment is a prevalent phenomenon in face-to-face, social environments' (Barak, 2005). The harassment of women in the military (Fitzgerld, Magley, Drasgow & Waldo, 1999), at work (Richman et

al., 1999) and schools (Timmerman, 2003) is receiving increased attention from both policymakers and the popular media. 'Sexual harassment is not a local phenomenon, but exists in all countries and cultures, although its perceptions and judgment, and consequently definitions, significantly differ from one culture to another' (Barak, 2005).

I. Classification of Sexual Harassment Behaviours

4 Till (1980) classifies sexual harassment behaviours into five categories: (1) sexist remarks or behaviour, (2) solicitation of sexual activity by promise or rewards, (3) inappropriate and offensive, but sanction-free sexual advances, (4) coercion of sexual activity by threat of punishment and (5) sexual crimes and misdemeanours. Following extensive pilot work, the suggestion was made (by Fitzgerald et al., 1995) to change the classification of types of sexual harassment into three different categories: gender harassment, unwanted sexual attention and sexual coercion. According to this study,

> *[g]ender harassment involves unwelcome verbal and visual comments and remarks that insult individuals because of their gender or that use stimuli known or intended to provoke negative emotions. These include behaviors such as posting pornographic pictures in public or in places where they deliberately insult, telling chauvinistic jokes, and making gender related degrading remarks. (Barak, 2005)*

5 Unwanted sexual attention covers a huge range of behaviours from being touched without permission, causing fear or distress, sexual name calling and harassment to rape and sexual assault.[3] Unwanted sexual attention can happen to both women and men and between people of the same and opposite sex.[4]

6 Sexual coercion exists along a continuum, from forcible rape to nonphysical forms of pressure that compel girls and women to engage in sex against their will. The touchstone of coercion is that a woman lacks choice and faces severe physical or social consequences if she resists sexual advances.[5]

7 All three types of sexual harassment may exist offline or on the Internet. 'However, because of the virtual nature of cyberspace, most expressions of sexual harassment that prevail on the Net appear in the form of gender harassment and unwanted sexual attention' (Barak, 2005).

> *Sexual coercion is distinctly different online than it is offline in that tactile force is not possible; however, the prevalence of verbal uses of threats, rewards, intimidation or some other form of pressure can be perceived as just as forceful as if it were in person. A unique feature of online interactions is that a perpetrator may possess technical skills which allow hacking into the victim's computer and/or 'cyberstalking' to follow a victim from digital place to place, which is often perceived as quite threatening to the victim. (Ibid)*

II. Gender Harassment

8 'Gender harassment in cyberspace is very common. It is portrayed in several typical forms that Internet users encounter very often, whether communicated in verbal or in graphical formats and through either active or passive manners of online delivery' (Barak, 2005). Active verbal sexual harassment mainly appears in the form of offensive sexual messages, actively initiated by a harasser toward a victim. 'These include gender-humiliating comments, sexual remarks, so-called dirty jokes, and the like' (Ibid).

9 This type of gender harassment is usually practiced in chat rooms and forums; however, it may also appear in private online communication channels, such as the commercial distribution through email (a kind of spamming) of pornographic sites, sex-shop accessories, sex-related medical matters, such as drugs such as Viagra and operations similar to penis enlargement. (Ibid)

10 Some scholars (Biber, Doverspike, Baznik, Cober & Ritter) investigated people's responses to online gender harassment in academic settings compared with traditional face-to-face forms of harassment (Li, 2005). A survey was administered to 270 undergraduate students in the US. The study examined a total of eight potential sexual harassment acts: (1) sexually explicit pictures; (2) content; (3) jokes; (4) misogyny; (5) use of nicknames; (6) requests for company; (7) requests for sexual favours; and (8) comments about dress (Ibid). The results showed that certain behaviour, such as requests for company, misogyny, the use of sexist nicknames, and comments about dress were seen as differentially harassing depending on the discourse medium (Ibid). Participants did not hold more relaxed standards for online behaviour. Rather, they had similar or even more stringent standards for online behaviour. Females perceived online jokes as more harassing than the same behaviour in a face-to-face environment, while males rated jokes as more harassing in the traditional environment (Ibid). Females tended to act rather cautiously (in comparison with a face-to-face setting) in defining the parameters of sexual harassment online. Compared with their male counterparts, they were more stringent in their judgment of behaviour as harassment because they took sexually explicit online pictures, jokes and requests for company more seriously (Ibid).

11 'Passive verbal sexual harassment on the other hand, is less intrusive, as it does not refer to one user communicating messages to another. In this category, the harasser does not target harassing messages directly to a particular person or persons but, rather, to potential receivers' (Barak, 2005). Nicknames and terms or phrases clearly attached to personal details often encompass this form of sexual harassment,

e.g. 'Sweet Tits' as a nickname or 'Want to blow my pole?' as an offensive phrase (Schenk, 2008). This category also includes explicit sexual messages attached to one's personal details in communication software or on a personal web page (Barak, 2005).

12 On a different note (Scott, Semmens, and Willoughby, 2001), illustrated how flaming creates a hostile environment for women.

> *Although flaming is not necessarily aimed at women, it is considered, in many instances, to be a form of gender harassment because flaming is frequently, typically, and almost exclusively initiated by men. The common result of flaming in online communities is that women depart from that environment or depart the Internet in general—what has been termed being 'flamed out'. Flamed out highlights the fact that the use of male violence to victimize women and children, to control women's behaviour, or to exclude women from public spaces entirely, can be extended into the new public spaces of the Internet. (Barak, 2005)*

13 A constructive solution has been the design of women-only sanctuaries that offer communities where flaming is rare and obviously not identified with men.

14 Graphic-based harassment can be active or passive.[6] Active graphic gender harassment refers to the intentional sending of erotic, pornographic, lewd and lascivious images and digital recordings by a harasser to specific or potential victims. Graphic harassment often occurs via email, instant messaging, redirected/automatic linking and pop-ups[7] (Schenk et al., 2008).

III. Cyberstalking

15 Another area of research that has provided insight into cybersexual harassment is cyberstalking. Bocji (2004) defined cyberstalking as a group of behaviours in which the use of information and communications technology is intended to cause emotional distress to another person. Behaviours associated with cyberstalking include making threats, false accusations (false-victimization), abusing the victim, attacks on data and equipment, attempts to gather information about the victim, impersonating the victim, encouraging others to harass the victim, ordering goods and services on behalf of the victim, arranging to meet the victim and physical assault (Schenk, 2008).

16 Imagine a distressed woman discovering the following message on the Internet that was falsely attributed to her:

> *Female International Author, no limits to imagination and fantasies, prefers groups macho/sadistic interaction...stop by my house at [current address]. Will take your calls day or night at [current telephone number]. I promise you everything you've ever dreamt about. Serious responses only.*[8]

17 Or imagine the fear generated by the following email messages sent over and over again from someone who remained anonymous, but seemed to have specific knowledge of the recipient's personal life:[9]

> *I'm you worst nightmare. Your troubles are just beginning.*

18 Some scholars believe that cyberstalking is synonymous with traditional offline stalking because of the similarities in content and intent (Goodno, 2007).

19 Similarities that are pointed to include a desire to exert control over the victim, and, much like offline stalking, cyberstalking involves repeated harassing or threatening behaviour, which is often a prelude to more serious behaviours. While these similarities do exist, cyberstalking differs from offline stalking in the following ways (Ibid):

- Cyberstalkers can use the Internet to instantly harass their victims with wide dissemination. For example, an offline stalker may harass the victim by repeatedly telephoning the victim. However, every telephone call is a single event that requires the stalker's action and time. This behaviour can easily snowball online because, with only one action, the stalker can create a harassing email message that the computer systematically and repeatedly sends to the victim thousands upon thousands of times.

- Cyberstalkers can be physically far removed from their victim. Offline stalking often entails situations where the stalker is physically near the victim. Cyberstalkers, however, can use the Internet to terrify their victims no matter where they are; thus, the victims simply cannot escape. The Internet provides cyberstalkers a cheap and easy way to continue to contact their victim from anywhere in the world. In addition, there is a sinister element to the secrecy of the cyberstalker's location. The uncertainty of the cyberstalker's location can leave the victim in a state of constant panic as she is left wondering whether her stalker is in a neighbouring house or a neighbouring state. Finally, the physical location of the cyberstalker can create several jurisdictional problems, because this act can take place across state lines.

- Cyberstalkers can remain nearly anonymous. The environment of cyberspace allows offenders to overcome personal inhibitions. The ability to send anonymous harassing or threatening communications allows a perpetrator to overcome any hesitation, unwillingness or inabilities he may encounter when confronting a victim in person. Perpetrators may even be encouraged to continue these acts.

- Cyberstalkers can easily impersonate the victim. Unlike offline stalking, the cyberstalker can easily take on the identity of the victim and create havoc online. While pretending to be the victim, the cyberstalker can send lewd emails, post inflammatory messages on multiple bulletin boards and offend hundreds of chat room participants. The victim is then banned from bulletin boards, accused of improper conduct and flooded with threatening messages from those the stalker offended in the victim's name.

20 In many ways, the Internet makes many of the frightening characteristics of offline stalking even more intense. It provides cyberstalkers with twenty-four-hour access, instantaneous connection, efficient and repetitious action and anonymity (Goodno, 2007). On top of all this, cyberstalkers can easily pretend that they are different people. The possibilities open to cyberstalkers are as endless as the borders of the ubiquitous Internet.

IV. Online Sexual Harassment on Social Media

21 Online Social Networks or Social Networking Sites (SNS's) are one of the most remarkable technological phenomena of the 21st century, with several SNS's now among the most visited websites globally. SNS's may be seen as informal but all-embracing identity management tools, defining access to user-created content via social relationships.[10]

22 Over the past five years, the popularity of Social Networking Sites (SNS's) has increased spectacularly, attracting an extraordinary number of users, of which a significant proportion are teenagers. An EU Kids Online study showed that in Europe, 77% of 13- to16-year-olds have a profile on a social networking site (Lievens, 2012), even though most social network sites put the minimum age required to create a profile at 13. The study also found that 38% of 9- to 12-year-olds are already active on SNS's (Ibid). According to a US study which examined the social media use of 12- to 17-year-olds, 80% of American teenagers are active on social network sites, of which 93% are present on Facebook (Ibid).

23 Sociologically, the natural human desire to connect with others, combined with the multiplying effects of Social Network (SN) technology, can make users less discriminating in accepting 'friend requests'. Users are often not aware of the size or nature of the audience accessing their profile data, and the sense of intimacy created by being among digital 'friends' often leads to disclosures which are not appropriate to a public forum.

24 As the Council of Europe put it in 2011 in their Recommendation on the protection of human rights with regard to social networking services, SNS's have 'a great potential to promote the exercise and enjoyment of human rights and fundamental freedoms, in particular the freedom to express, to create and to exchange content and ideas, and the freedom of assembly' (Lievens, 2012). However, the fact that SNS's allow users to communicate through status updates, through messages on 'walls' or through instant messaging, to share photo or video fragments, and to connect with old or new 'friends', also entails a number of risks, the most important of which include stalking and bullying.[11]

1. Stalking on Social Media

25 Stalking typically involves threatening behaviour in which the perpetrator repeatedly seeks contact with a victim through physical proximity and/or phone calls (offline stalking), but also by electronic means, such as Instant Messenger and messaging on SNS's. Statistics on cyberstalking suggest that stalking using SNS's is increasing.[12]

26 In a 2005 study of one university's Facebook network, between 15 and 21% of users disclosed both their full current address as well as at least two classes they were attending. Since a student's life is mostly dominated by class attendance, the combination of address and class schedule provides the physical location of the user throughout most of the day (and night).[13] A much larger number of users, 78%, provided instant messaging (IM) contact information suitable for tracking their online status. Emerging mobile-based social network sites such as Twitter tend to emphasise location data even more. It can also be seen from the other threat descriptions that SNS's provide many other more subtle methods for stalkers to track their targets.[14]

27 The impact of cyberstalking via social networks on the victim is well known, and can range from mild intimidation and loss of privacy to serious physical harm and psychological damage. In Seattle two girls aged 11 and 12 were charged in 2011 with first-degree computer trespassing and cyberstalking, for allegedly posting sexually explicit photos and comments on the Facebook page of a 12-year-old classmate.[15] The two girls charged in the case were also accused of using the third girl's computer address to send out instant message solicitations for sex using her name. The children involved are all middle-school classmates and live in the suburban city of Issaquah, east of Seattle. The two accused offenders are believed to be the youngest individuals ever charged with cyberstalking and computer trespassing in King County.[16]

2. Bullying on Social Media

28 On a different note, social networks like Bebo, Facebook, Twitter, Youtube and MySpace are sometimes sites of cyberbullying, because people can post abusive messages and pictures on other people's walls, pages or profiles.

29 In a study of 799 youth ages 12-17, it was found that 90% of youth using social media said that when they witness online meanness, they ignore it (Levy et al., 2012). Eight per cent of youth reported having experienced some form of online bullying, such as through email, a social network site or instant messaging. Eighty per cent said they have defended the victims (Ibid). Seventy-nine per cent said that they have told the other person to stop being mean. About 67% of teens who have witnessed online cruelty have also witnessed others joining in – and 21% said they have also joined in the harassment (Ibid).

30 In addition, a 2006 study found out that 'about one out of ten youngsters have been involved in frequent cyberbullying: 3.3% exclusively as a victim, 5.0% exclusively as a perpetrator, and 2.6% as both a victim and a perpetrator'.[17] 'The majority of youngsters (63.8%) believe cyberbullying is a "big problem". This figure may reflect either a general assessment of the issue in the eyes of the youngsters, or it may indicate that they find it a serious problem for those being bullied'.[18] Whether this is due in whole, in part or in combination to the increased use and development of social networks, increased platform compatibility, increased access to the Internet, ease of multimedia creation and distribution, or indeed to the increasing recognition that there are a group of acts which utilise technology that are identifiable as bullying is not currently known.[19] Social networks tend to offer an array of tools to users – for example, in addition to profile and people search there may also be blogging or micro-blogging facilities, instant messaging, chat rooms, community and collaboration areas etc. which together constitute a very useful 'suite' of tools for the bully. Each of these elements can be used positively or potentially misused.[20] The forms of cyberbullying behavior that can be carried out on social networks include the following:[21]

- Flaming: Online fights using electronic messages with angry and vulgar language.
- Harassment: For example, repeatedly sending hurtful or cruel and insulting messages; gaining access to another's username and password in order to send inappropriate messages to friends' lists.
- Denigration: Setting up accounts pretending to be people in order to humiliate them; sending or posting gossip or rumours about a person to damage his or her reputation or friendships, e.g. the creation of 'Hate' websites, the posting of jokes, cartoons, gossip and rumours, all directed at a specific victim; posting harmful, untrue and/or cruel statements or pictures, and inviting others to do the same, or to comment on them.
- Impersonation: Pretending to be someone else and sending or posting material to get that person in trouble, put them in danger or to damage their reputation or friendships.
- Outing: Sharing someone's secrets or embarrassing information or images online.
- Trickery: Talking someone into revealing secrets or embarrassing information, then sharing it online.
- Exclusion: Intentionally and cruelly excluding someone from an online group, for example, a group of offline friends deciding to ignore a specific individual as a form of punishment.
- Threatening behaviour: Either direct or indirect (interestingly, Willard includes threats to hurt someone or to harm oneself).

V. Online Grooming

31 Online grooming can be described as 'an adult actively approaching and seducing children via the Internet (especially through social network sites, profile sites, chat rooms, news groups, etc.), with the ultimate intention of committing sexual abuse or producing child pornographic material depicting the child concerned' (Kool, 2011). Although grooming has always existed, the online version thereof is relatively new. Digital communication has enormously increased in Western societies. Research into young people's Internet behaviour has shown that they spend a considerable part of their free time roaming the Internet, often with insufficient supervision (Ibid). The Internet offers potential abusers ample opportunity to enter into digital contact with children in relative anonymity, which can lead to offline and/or online sexual abuse (Ibid).

32 For grooming to be a criminal offence, as referred to in European regulations, at least one act towards committing the offence is required, aiming to organise a meeting with the child and intending to have sexual contact (Ibid).

33 In the process of grooming, the perpetrator creates the conditions which will allow him/her to abuse the children while remaining undetected by others, and the child is prepared gradually for the time when the offender first engages in sexual molestation (Childnet International, 2009). Offenders may groom children through a variety of means. For example, an of-

fender may take a particular interest in the child and make him or her feel special. He may well treat the child emotionally like an adult friend, sharing intimate details about his sex life and adult relationships (Ibid). Another grooming technique is through the gradual sexualisation of the relationship. Offenders thus test the child's reaction to sex by bringing up sexual matters, having sexual materials around or engaging in sexualised talking (Ibid).

34 In December 2012, Daniel Enright, 21, from Australia was charged with sexually assaulting two teenagers he allegedly groomed online.[22] The offender approached the girls via the social networking website 'Facebook' before sending them text messages where he allegedly posed as a photographer looking for models. The charges included 11 counts of grooming girls under the age of 16 for sexual activity by sending them text messages. [23]

35 Enright was also charged with soliciting child pornography via text messages and sending menacing or harassing text messages.[24]

VI. Sextortion

36 Sextortion is 'a form of sexual exploitation where people are extorted with a nude image of themselves they shared on the Internet' (De la Cerna, 2012). Victims are later coerced into performing sexual acts with the person doing the extorting, and are coerced into performing hard-core pornography (Ibid).

37 Sextortion also refers to a form of sexual blackmail in which sexual information or images are used to extort sexual favours from the victim.[25] Social media and text messages are often the source of the sexual material and the threatened means of sharing it with others.[26]

38 Incidents of sextortion have been prosecuted under various criminal statutes, including extortion, bribery, breach of trust, corruption, sexual coercion, sexual exploitation, sexual assault, child pornography, computer hacking and wiretapping.

39 In April 2010 an offender from Alabama, USA, was sentenced to 18 years in prison after he admitted sending threatening emails on Facebook and MySpace extorting nude photos from more than 50 young women in Alabama, Pennsylvania and Missouri (Wilson, 2010).

40 In Wisconsin, New Berlin, Anthony Stancl, 18, received 15 years in prison in February 2010 after prosecutors said he posed as a girl on Facebook to trick male high school classmates into sending him nude cell phone photos, which he then used to extort them for sex (Ibid).

41 In the same year, a 31-year-old California man was arrested on extortion charges after authorities said he hacked into more than 200 computers and threatened to expose nude photos he found unless their owners posed for more sexually explicit videos. Forty-four of the victims were juveniles. Federal prosecutors said he was even able to remotely activate some victims' webcams without their knowledge and record them undressing or having sex (Ibid).

42 In October 2012, a Canadian teen girl began an online relationship with a boy, during which she sent him intimate photos of herself.[27] The boy then used the photos in an attempt to manipulate and coerce the girl into sending him a video of herself.[28] When she refused, the boy gained access to her email account and sent the photos to several of her email contacts. The boy was charged with making, possession and distribution of child pornography, extortion, and threatening death.[29]

43 In another case, "'In [i]n January 2013 a Glendale man allegedly hacked hundreds of online accounts and extorted some 350 women and teenage girls into showing him their naked bodies'" (Los Angeles News Online, Jan 29, 2013). This incident is further described as such:

> *The offender hacked into the women's Facebook, Skype and email accounts. He then changed the passwords to lock victims out of their own accounts and then searched emails or other files for naked or seminaked photos of the victims (Ibid). He then posed as a friend, persuading them to strip while he watched via Skype, captured images of them, or both. When the women discovered that the offender was posing as a friend, he often blackmailed them with the nude photos he had fraudulently obtained to coerce more stripping. In some cases, he's accused of posting the nude photos to the victims' Facebook pages when they refused his demands. (Ibid)*

VII. Age Play

44 "'Second lLife'" is not even immune from sexual offences. In everyday language, "'Second lLife'" is often referred to, as an online computer game.[30] Avatars are frequently called "'players'" and the conditions set up by "'Linden Lab'" are considered the rules of the game (Hoeren, 2009). The established Second Life practice of so-called "'age play'", in which users request sex with other players who dress up as child avatars, has encouraged a growth in players posing as children in order to make money (Kierkegaard, 2008). Age play is in world sexual activity between a child avatar and an adult avatar. Sex is an important feature in Second lifeLife. Participants can make their avatars look like anything they want and create software renderings of whatever equipment they want to use (Ibid). They even go to the extent of actually purchasing scripts and making the avatars engage in simulated sex.

C. Prevalence of Sexual Harassment in Cyberspace

45 Many authors refer to sexual harassment on the Internet and describe it as prevalent and risky. Leiblum and Döring (2002) argued that the Internet provides a convenient vehicle, commonly used, to force sexuality on women through non-social (logging into web pages) and social (interpersonal communication) uses of the Net.

46 Sexual harassment appears on the Internet in a peculiarly virulent form.[31] This is because there are many more men than women using online services, and each male user seems to spend more time online than female users.[32] Surveys suggest the proportions of people are around 94% male, and that the male presence is dominant in content. Also, the anonymity of the Net gives an atmosphere of seclusion, where the harasser feels that he may behave in an unacceptable manner with impunity.[33]

47 Casey & McGarth consider cyberspace as an ideal environment for sex offenders to commit sexual harassment and imposition because of its characteristics. Firstly, it is difficult to locate the IP address of cybercriminals (Lovet, 2009). Secondly, cybercriminals may use cryptography to encrypt evidence (Ibid). Thirdly, the transnational nature of cybercrime raises an issue because legal and repressive systems in the world are currently based on sovereign jurisdictions with borders. Frequently, in a cybercrime scenario, the attacker sits in country A, and without moving an inch, engages in cybercriminal action targeting a victim in country B. The theoretical problem is therefore: as follows: knowing the crime occurs in country B, while the criminal is in country A, how can the criminal be prosecuted and under which jurisdiction? (Ibid).

48 Cunneen and Stubbs (2000) reported an incident in which an Australian citizen solicited sex among Filipino women through the internetInternet in return for economic privileges. Cooper et al., (2002) mentioned the case of an internetInternet user with a paraphilia-related disorder who obsessively used chat rooms to communicate his sexual thoughts to women.

49 According to "Journal of Adolescent Health (47, 2010"), only 18% of youth use chat rooms, ; however, the majority of Internet-initiated sex crimes against children are initiated in chat rooms.[34] In 82% of online sex crimes against minors, the offender used the victim's social networking site to gain information about the victim's likes and dislikes.[35] 65% of online sex offenders used the victim's social networking site to gain home and school information about the victim.[36] 26% of online sex offenders used the victim's social networking site to gain information about the victim's whereabouts at a specific time.[37]

50 In 2006 one in seven kids received a sexual solicitation online. Over half (56%) of kids sexually solicited online were asked to send a picture; 27% of the pictures were sexually- oriented in nature. 44% per cent of sexual solicitors were under the age of 18.[38] 4 % of all youth Internet users received aggressive sexual solicitations, which threatened to spill over into "'real life"'. These solicitors asked to meet the youth in person, called them on the telephone or sent offline mail, money or gifts. Also, four per cent of youth had distressing sexual solicitations that left them feeling upset of extremely afraid.[39]

51 Of aggressive sexual solicitations of youth (when the solicitor attempted to establish an offline contact via in-person meeting or phone call), 73% of youth met the solicitor online. 80% of online offenders against youth were eventually explicit with youth about their intentions, and only 5% concealed the fact that they were adults from their victims. The majority of victims of Internet-initiated sex crimes were between 13 to 15 years old; 75% were girls and 25% were boys.[40]

52 In 2008, 14 % of students in 10th- to 12th grade have accepted an invitation to meet an online stranger in-person and 14 % of students, who are usually the same individuals, have invited an online stranger to meet them in-person.[41] 14 % of 7th- through 9th grade students reported that they had communicated with someone online about sexual things; 11 % of students reported that they had been asked to talk about sexual things online; 8 % have been exposed to nude pictures and 7 % were also asked for nude pictures of themselves online.[42] 59 % of 7th- through 9th grade victims said their perpetrators were a friend they know knew in-person; 36 % said it was someone else they know; 21 % said the cyber offender was a classmate; 19 % indicated the abuser was an online friend; and 16 % said it was an online stranger.[43] 9 % of children in 7th- through 9th grade have accepted an online invitation to meet someone in-person and 10 % have asked someone online to meet them in-person. 13 % of 2nd- through 3rd grade students report that they used the Internet to talk to people they do not know, 11 % report having been asked to describe private things about their body and 10 % have been exposed to private things about someone else's body.[44]

D. Legal Regulation

53 There have been calls in the United States for specific cyberstalking legislation (Elison et al., 1998). It is argued that victims of cyberstalking are inadequately protected as existing laws are too inflexible to cover online harassment (Ibid). Under this section,

we shall focus on the legal regulation of online sexual harassment in the USA, the United Kingdom and according to the Council of Europe & the European Union.

I. United States

54 Under 18 U.S.C. 875(c), it is a federal crime, punishable by up to five years in prison and a fine of up to $250,000, to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another. Section 875(c) applies to any communication actually transmitted in interstate or foreign commerce – thus it includes threats transmitted in interstate or foreign commerce via the telephone, email, beepers or the Internet.[45]

55 Although 18 U.S.C. 875 is an important tool, it is not an all-purpose anti-cyberstalking statute. First, it applies only to communications of actual threats. Thus, it would not apply in a situation where a cyberstalker engaged in a pattern of conduct intended to harass or annoy another (absent some threat). Also, it is not clear that it would apply to situations where a person harasses or terrorizes another by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person.[46]

56 Certain forms of cyberstalking also may be prosecuted under 47 U.S.C. 223. One provision of this statute makes it a federal crime, punishable by up to two years in prison, to use a telephone or telecommunications device to annoy abuse, harass, or threaten any person at the called number. The statute also requires that the perpetrator not reveal his or her name. (Ssee 47 U.S.C. 223(a)(1)(C)). Although this statute is broader than 18 U.S.C. 875 – in that it covers both threats and harassment – Section 223 applies only to direct communications between the perpetrator and the victim. Thus, it would not reach a cyberstalking situation where a person harasses or terrorizes another person by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person. Moreover, Section 223 is only a misdemeanormisdemeanour, punishable by not more than two years in prison.

57 In addition, Title VII of the Civil Rights Act of 1964, a federal law, prohibits sex harassment in employment, including harassment based on sex, pregnancy, childbirth, and related medical conditions. The Equal Employment Opportunity Commission (EEOC) is the federal agency charged with enforcing these provisions. Under Title VII, online content can be considered illegal sexual harassment if it is unwelcome, of a sexual nature, and is severe or pervasive enough to create a hostile work environment.[47]

58 President Clinton signed a bill into law in October 1998 that protects children against online stalking. The statute, 18 U.S.C. 2425, makes it a federal crime to use any means of interstate or foreign commerce (such as a telephone line or the Internet) to knowingly communicate with any person with intent to solicit or entice a child into unlawful sexual activity.[48] While this new statute provides important protections for children, it does not reach harassing phone calls to minors absent a showing of intent to entice or solicit the child for illicit sexual purposes.

59 California was the first state to pass a stalking law in 1990, and all the other states have since followed. The first US State state to include online communications in its statutes against stalking was Michigan in 1993. Under the Michigan Criminal Code, "'harassment'" is defined as conduct directed toward a victim that includes repeated or continuing unconsented contact, that would cause a reasonable individual to suffer emotional distress, and that actually causes the victim to suffer emotional distress. Unconsented contact under the Michigan Code specifically includes sending mail or electronic communications to that individual. A number of other US States states besides Michigan have anti-stalking laws that include electronic harassment. These states include: Arizona,[49] Alaska,[50] Connecticut,[51] New York,[52] Oklahoma,[53] and Wyoming.[54]

60 In the US, Michigan was the first state to charge someone with online stalking (Ellison, 1998). Andrew Archambeau refused to stop sending email messages to a woman he met through a computer dating agency and was charged under Michigan stalking laws in May 1994. Archambeau's lawyers sought to challenge the constitutionality of these anti-stalking laws. In January 1996, however, Archambeau however pleaded no contest to the stalking charge (Ibid).

61 McGraw highlights further difficulties in using anti-stalking legislation to combat online harassment (Ellison et al., 1998). In a number of states, McGraw explains, the language of the statute requires physical activity, thus exempting email harassment (Ibid). Some state statutes also require a "'credible threat'" of serious physical injury or death. In such states, email harassment is unlikely to meet this standard (Ibid). This was true in the Jake Baker case.[55] Using the pseudonym "'Jake Baker'", Abraham Jacob Alkhabaz, a student at the University of Michigan, posted stories to a newsgroup called "'alt.sex.stories'". One of Baker's stories described the rape, torture and murder of a woman. Baker used the real name of a fellow student from the University of Michigan for the victim. Baker also corresponded with a reader of the story via email who used a pseudonym of "'Arthur Gonda'" in Canada. In over 40 emails both men discussed their desire to abduct and physically injure women in their local area. Baker was arrested and held without bail and was charged with the interstate transmission of a threat to kidnap or injure another. Though most described Baker as a quiet

"'computer geek'" with no history of violence, the stories he posted on the Internet were horrific and disturbing. Nevertheless, a US District Court Judge dismissed the case against Baker, ruling that the threats lacked a specific intent to act or a specific target required under the Michigan stalking law.

62 Finally, federal legislation is needed to fill the gaps in current law. While most cyberstalking cases will fall within the jurisdiction of state and local authorities, there are instances – such as serious cyberharassment directed at a victim in another state or involving communications intended to encourage third parties to engage in harassment or threats – where state law is inadequate or where state or local agencies do not have the expertise or the resources to investigate and/or prosecute a sophisticated cyberstalking case. Therefore, federal law should be amended to prohibit the transmission of any communication in interstate or foreign commerce with intent to threaten or harass another person, where such communication places another person in fear of death or bodily injury to themselves or another person. Because of the increased vulnerability of children, the statute should provide for enhanced penalties where the victim is a minor. Such targeted, technology-neutral legislation would fill existing gaps in current federal law, without displacing the primary law enforcement role of state and local authorities and without infringing on First Amendment-protected speech.

II. United Kingdom

63 Existing UK laws are sufficiently flexible to encompass online stalking, email harassment, child pornography offences and online grooming.[56] The Telecommunications Act 1984, Section 43, for example, makes it an offence to send by means of a public telecommunications system a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. For the purposes of the Act, a public telecommunication system is any telecommunications system[57] so designated by the Secretary of State and is not confined to British Telecom's telephone system. The Act therefore potentially covers the sending of offensive email messages in some instances.[58] The Act will not apply, however, in cases where the data is transmitted by using a local area network unless part of the transmission is routed through a public telecommunications system.[59] So, whether the Act applies to email harassment will depend upon the telecommunications network used, but the Act is not limited to voice communications.

64 The Protection from Harassment Act 1997 may also be invoked in cases of online harassment. This Act provides a combination of civil and criminal measures to deal with stalking. It creates two criminal offences, the summary offence of criminal harassment[60] and an indictable offence involving fear of violence.[61] Under Section 2 it is an offence to pursue a course of conduct which amounts to the harassment of another where the accused knew or ought to have known that the course of conduct amounts to harassment. A person commits an offence under Section 4 if he pursues a course of conduct which causes another to fear, on at least two occasions, that violence will be used against him. It is sufficient that the accused ought to have known that his course of conduct would cause the other to so fear on each of those occasions.

65 The Act also gives courts the power to impose restraining orders on convicted defendants, prohibiting them from further conduct which may be injurious to the victim. Breach of such an order carries a potential sentence of five years' imprisonment. Harassment includes both alarm and distress, though harassment, alarm and distress are not specifically defined in the Act and so these terms are to be given their ordinary meaning. The range of behaviour covered by the Act is thus potentially extremely wide. The sending of abusive, threatening emails or the posting of offensive material would constitute an offence under Section 2 of the Act, as long as it amounts to a course of conduct (for example, more than one e-mail must be sent) and the offender knew or ought to have known that his conduct amounted to harassment.

66 On a different note, sections 14 & 15 of the Sexual Offences Act 2003 make it an offense to arrange a meeting with a child, for oneself or someone else, with the intent of sexually abusing the child. The meeting itself is also criminalized. The Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005 introduced a similar provision for Scotland.

67 Thus, a crime may be committed even without the actual meeting taking place and without the child being involved in the meeting (for example, if a police officer has taken over the contact and pretends to be that child).

68 In January 2012, Scotland Yard investigated what was believed to be one of the first cases of cyber-stalking involving Twitter in the United Kingdom.[62] The Metropolitan Police confirmed it examined claims that a 37-year-old man has had allegedly been targeting two women who claim to have received offensive, racist and sexually demeaning tweets and emails. It is believed the alleged harassment has had gone on since the beginning of November 2011 and involved as many as five victims.[63] The pair are were thought to have been targeted because of their views on Israel and the Iraq war. According to those familiar with the case, the man has had allegedly sent more than 16,000 tweets to the victims and tried to contact one of them at work. Although they blocked

the tweets, the sender has varied his Twitter address as his messages have becoame more threatening. His alleged tweets included the warnings: "'I am in a war to the death. Stay well clear for your own safety. Don't ever tweet me again'"; "'Remember watch your back 24 hours a day 7 days a week for life'"; and "'Want me to tweet you your death place?'" Twitter has consequently taken down all of the offensive tweets.[64]

III. The Council of Europe

69 The Council of Europe has pointed to the importance of addressing cyberbullying in several documents, such as the Recommendation on empowering children in the new information and communications environment (Council of Europe, 2006), the Declaration on protecting the dignity, security and privacy of children on the Internet (Council of Europe, 2008), the Recommendation on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment (Council of Europe, 2009) and the Recommendation on the protection of human rights in social networks (Council of Europe, 2012).

70 Aside from these recommendations and declarations, the European Convention on Human Rights (ECHR), one of the cornerstones of human rights protection in Europe, provides guarantees with regard to the freedom of expression (article Article 10 ECHR) and the right to privacy (article Article 8 ECHR).

71 The right to freedom of expression protects a broad range of speech. Already in 1976, the European Court of Human Rights (ECHR) argued in the case Handyside v. UK that article Article 10 is applicable not only "'to information or ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb'" (Lievens, 2012). Whether an act which can be classified as cyberbullying (for instance, a series of negative comments on someone's Facebook wall which may be hurtful to the person who is targeted) may be considered a protected 'expression' or not will need to be judged on a case-by-case basis, taking all circumstances into account (Ibid). An important element in this delicate consideration might be the motivation or intent of the offender. However, it is important to note that article Article 10 is not an absolute right. According to paragraph 2, restrictions on the freedom of expression may be imposed if they are (1) prescribed by law, (2) introduced with a view to specified interests such as the protection of health or morals or the protection of the reputation or the rights of others, and (3) necessary in a democratic society (Ibid).

72 Acts of cyberbullying may also infringe on the right to privacy of an individual, guaranteed by article Article 8 ECHR. An interesting case in this context is K.U. v. Finland (Lievens, 2012). The case dealt with an advertisement on a dating site, placed by unknown persons, in the name of a 12-year-old boy without his knowledge. This advertisement included the age of the boy, a description of his physical characteristics, a link to his website which contained a picture and a telephone number, and a statement that he was seeking an intimate relationship with a boy. At the time of the facts it was not possible according to Finnish legislation to obtain the identity of the person who placed the advertisement from the Internet provider (Ibid). The Court considered the applicability of article Article 8 ECHR indisputable and emphasised that "'[c]hildren and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives'". The fact that no effective steps could be taken to identify and prosecute the person who placed the advertisement, and thus the failure by the Finnish government to fulfillfulfil its positive obligation to provide a framework of protection, led the Court to decide that article Article 8 ECHR had been violated (Ibid).

IV. The European Union

73 In December 2011, the European Union adopted the Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child pornography.[65] The approach of this Directive to offences concerning child pornography is similar to the approach of the Lanzarote Convention.[66] Article 5 contains the (range of) punishments that should be applied to the acquisition, possession, knowingly obtaining access to, distribution, dissemination, transmission, offering, supplying or making available of child pornography. In addition, article Article 8 specifically allows Member States to decide whether article Article 5(2) and (6) apply to the production, acquisition or possession of material involving children who have reached the age of sexual consent where that material is produced and possessed with the consent of those children and only for the private use of the persons involved, in so far as the acts did not involve any abuse. As recital 20 put it:

> *This Directive does not govern Member States' policies with regard to consensual sexual activities in which children may be involved and which can be regarded as the normal discovery of sexuality in the course of human development, taking account of the different cultural and legal traditions and of new forms of establishing and maintaining relations among children and adolescents, including through information and communication technologies. These issues fall outside of the scope of this Directive. Member States which avail themselves of the possibilities referred to in this Directive do so in the exercise of their competences.*

74 The European Union has also repeatedly pointed out that cyberbullying is an important issue that needs to be tackled, for instance in the framework of the Safer Internet Programme, or in the European Strategy for a better internetInternet for children (European Commission, 2012). With regard to legislation, the most relevant and applicable provisions are included in the Data Protection Directive. As the European Data Protection Supervisor has stated:

75 *"When individuals put information about third parties, for example, comments on their appearances or behaviors, independently of whether this constitutes legally cyber-harassment, they disclose personal information of their victims. For example, their real name, their address, school, etc. The principles and obligations embodied in the EU data protection legislation are fully applicable to the disclosure of this information, which under EU legislation qualifies as personal data, in forums or social networks. For example, data protection legislation requires informing and in many cases obtaining the consent of individuals before publishing information that relates to them. Obviously, those engaged in cyber harassment do not inform, much less ask for the consent of their victims to publish their personal data, thus, automatically breaching data protection legislation". (Lievens, 2012).*

76 It is possible to file a complaint with the national Data Protection Authority or go to court in case of a violation of the Data Protection Directive.

E. Tackling Online Sexual Harassment

77 From logical, theoretical, and pragmatic perspectives, knowing the associated problem, and risks associated therewith, and the ills resulting therefrom them is an indispensable step towards a possible solution. Furthermore, such a determination constitutes an integral part of devising effective vaccines and serums to eradicate and prevent this evil. Having discussed the diverse aspects of the vexing problem of online sexual harassment, we shall now address some of the its potential solutions thereto. Thus, we shall analyzeanalyse in this section the importance of establishing multinational public – -private collaboration, educating internetInternet users, perpetrators and victims and regulating the liability of internetInternet service providers.

I. Establishing Multidimensional Public-private Private Collaboration

78 To tackle online sexual harassment effectively, it is essential to establish multidimensional public-private collaboration between law enforcement agencies, the information technology industry and ISPs. Without efficient private –- public cooperation, online sexual harassment will never be tackled effectively.

79 The private sector needs to be assured of a confidential relationship in which information can be exchanged for investigative and intelligence purposes. Furthermore, law enforcement, prosecutors and judges often do not have the necessary technical means and knowledge to investigate and prosecute these types of crimes. Law enforcement agencies must work in partnership with those who will influence the operating environment so that all concerned can better anticipate changes in criminal behaviorbehaviour and technological misuse.

II. Using Innovative Software

80 New and innovative software programs which enable users to control the information they receive are constantly being developed. There are, for example, technical means by which internetInternet users may block unwanted communications. Tools available include "'kill"' files and "'bozo"' files which delete incoming email messages from individuals specified by the user. Such tools are included with most available email software packages. In addition, programs such as Eudora and Microsoft Outlook have filter features which that can automatically delete emails from a particular email address or those which contain offensive words. Chat- –room contact can be blocked as well.

81 There is also specially designed software to filter or block unwanted email messages. These tools, such as CyberSitter[67] and Netnanny,[68] are designed mainly to block the access of children to sexually explicit websites and newsgroups, but can also be used to filter out and block email communications. Some of this software can additionally filter words through the incoming and outgoing email messages. The mandatory use of such software, especially at access level, by libraries and ISPs is criticized within the US, because the decisions taken to block certain websites are arbitrary and within the discretion of the private companies that develop these systems (Ellison et al., 1998). They are also defective, since most of them block such websites as the Middlesex County Club or Mars Explorer, while trying to block the word "'sex"'; or block websites by looking at the keywords in the meta-tags offered by the individual html files (Ibid). These tools may be of some use to victims of cyber-stalkers to filter out unwanted messages, nonetheless.

82 These approaches may be useful in situations where the communications are merely annoying but may be useless in situations in which threatening communications are not received by the intended victim. A victim who never "'receives"' the threat may not know he or she is being stalked, and may be alerte-

red, for the first time, when the stalker shows up to act on his or her threats.

III. Educating Internet Users, Perpetrators and Victims

83 The education of potential perpetrators on how to behave online is one of the important steps to in tackle tackling internetInternet sexual harassment. In addition, the education of internetInternet users and victims is the first step towards self-protection.

84 The reason educational approaches are so vital is because they can help teach perpetrators how to behave in and victims how to respond to a wide variety of situations (Szoka et al., 2009). Education teaches lessons and builds resiliency, providing skills and strength that can last a lifetime. That was the central finding of a blue-ribbon panel of experts convened in 2002 by the National Research Council of the National Academy of Sciences to study how best to protect children in the new, interactive, "'always-on"' multimedia world (Ibid). Under the leadership of former U.S. Attorney Attorney-General Richard Thornburgh, the group produced a massive report that outlined a sweeping array of methods and technological controls for dealing with potentially objectionable media content or online dangers (Ibid). Ultimately, however, the experts used a compelling metaphor to explain why education was the most important strategy on which parents and policymakers should rely (Ibid):

> *"Technology—in the form of fences around pools, pool alarms, and locks—can help protect children from drowning in swimming pools. However, teaching a child to swim—and when to avoid pools—is a far safer approach than relying on locks, fences, and alarms to prevent him or her from drowning. Does this mean that parents should not buy fences, alarms, or locks? Of course not—because they do provide some benefit. But parents cannot rely exclusively on those devices to keep their children safe from drowning, and most parents recognize that a child who knows how to swim is less likely to be harmed than one who does not. Furthermore, teaching a child to swim and to exercise good judgment about bodies of water to avoid has applicability and relevance far beyond swimming pools—as any parent who takes a child to the beach can testify".*

85 In addition, there are many websites and books which provide information for self-protection from cyber-stalkers for online users. Women are also advised, where possible, to adopt either a male or gender neutral user name. Internet users should regularly check their online profile (finger files) or biography to see what information is available to a potential stalker. They are also advised to understand how the privacy settings of their social network sites work and customize these privacy settings to block strangers from obtaining personal information.

IV. Regulating the Liability of Internet Service Providers

86 Although the status of ISPs in some European countries is very much debatable , – for instance, whether they are publishers, distributors or common carriers – , the Internet industry should also have a similar responsibility (Chawki, 2009). The tricky question remains: how to achieve this? While it may be difficult to control the content of the Internet, its provision by the ISPs may be controlled. In France, for example, La Loi pour la Confiance dans l'Economie Numérique LEN defines the liability and clarifies the role and responsibility of ISPs.[69] The objective of this law is to provide impetus to the digital economy in France in order to reinforce confidence in the use of such new technology and thereby ensure its growth.[70] This law has transposed the E-commerce Directive 2000/31/CE into French law together with part of the Directive on Privacy and Electronic Communications 2002/58/EC. The (LEN) has been heavily modified during its passage through the pipeline of parliamentary procedure,[71] and has been the subject of criticism and has met with vociferous opposition from a number of quarters, in particular ISPs and user groups, claiming the draft (LEN) threatened free expression on the Internet and placed a significant and unfair burden on ISPs to censor online content (Taylor, 2004). Many actions have also been undertaken by EDRI[72] member IRIS, which launched a petition against this provision in the draft law, together with the French Human Rights League, the G10-solidaires association of trade- unions, and two non-commercial providers.[73] The petition has been signed by more than 8,000 individuals and 170 organisations.

87 Other actions have been undertaken by ODEBI, an association of Internet users, and by Reporters without Borders (RSF).[74] Considerable lobbying continued prior to the second reading of the Bill by the Senate, which took place on 8th April, 2004. At the second reading, the Senate voted to adopt the (LEN), but with certain crucial modifications. Actually, article Article 6 provides that ISPs are not liable for information transmitted or hosted unless they have actual knowledge of illegal activity or information of facts or circumstances from which the illegal activity or information is apparent; or if upon obtaining such knowledge or awareness they act expeditiously to remove or to disable access to the information. With respect to contractual provisions on an ISP's liability, it should be noted that these provisions are not enforceable against third parties in France. As a result, a contractual exemption of liability cannot be used with regard to a third party (not subscribing with an ISP) who has suffered harm as a result of unlawful content broadcast on the networks, for example, or an act of infringement. person habitually engaged in prostitution.[75]

88 On a different note, The Association des Fournisseurs d'Accès et des Services Internet (AFA)[76] requires its members to offer their customers tools for (i) the filtering of illegal or harmful content; (ii) the regulation of unwanted bulk mail; and (iii) a point of contact for the reporting of illegal or harmful content. In this way the responsibility for receiving or sending content is passed back to the customers – the customers are given the tools to determine themselves what information (illegal, harmful, necessary, etc.) they would like to receive or send.[77] The AFA makes a specific reference to the workings of the Internet Content Rating Association (ICRA) in offering systems capable of filtering content (both against illegal and harmful content and for the protection of minors) and members are expected to abide with by ICRA's procedures. The implication of the rules relating to illegal and harmful content is as follows: [78]

- An ISP has no responsibility to monitor and remove material on its own initiative;
- If the ISP removes information at the request of law enforcement agencies or private organisations acting as monitors of Internet content it should not be held responsible for the removal;
- If on the other hand an ISP does not follow the requests of law enforcement agencies and private organisations then it is in breach of these rules and may be liable for the consequences.

89 AFA does not have a formal complaints mechanism. When complaints are received they are passed onto the member and it is up to the member to handle the complaint.[79] The Statute founding AFA as an association, however, allows for a member to be expelled from the association, amongst other reasons, if the member acts against rules set by the AFA. In both cases, member ISPs apparently follow the rules of their association.[80] It can be argued that in certain circumstances, it is in the ISP's own interest to do so for this guarantees a certain amount of protection against liability. An ISP that does not follow the rule of its own association exposes itself to legal liability. Furthermore, AFA is represents strong lobby groups with government and with policy groups. It thus benefits an ISP to be a member of the association and not risk expulsion.[81]

F. Future Prospects

90 It's clear that online sexual harassment is not going to disappear. While cybercrime is an unwanted side effect of the Internet age, it's also part of a broader crime landscape. If there's a use for something, someone will always find a way to abuse it, and this includes computer technology and the connectivity provided by the Internet. Crime can never be eliminated, so tackling online sexual harassment is less about "'winning the war"' than about mitigating the risks associated with using the Internet. To manage the risk, the global society clearly needs a legal framework, together with appropriate and effective law enforcement agencies. There's little question that law enforcement agencies have developed increasing expertise in dealing with high-tech crime during the last decade, including joint policing operations across national borders. This must be further developed if we are to deal effectively with online sexual harassment. In particular, the extension of international legislation beyond developed countries, and the development of a "'cyber-Interpol"' to pursue criminals across geo-political borders, would contribute greatly to the fight against online sexual harassment. Law enforcement, however, is only part of the solution. We also need to ensure that individuals understand the risks and have the knowledge and tools to minimise their exposure to this threat. This problem is exacerbated by the growing number of people accessing the Internet for the first time. Society must find imaginative and varied ways of raising public awareness about online sexual harassment and about methods which can be used to mitigate the risks. The "'information super-highway"' is no different to any other public road. We need well-designed roads, safe cars, clear signs and competent drivers. In other words, we need a blend of appropriate legislation, effective policing and public awareness.

G. Conclusion

91 Due to the seeming invisibility and anonymity of the Internet, online sexual harassment has become a serious and social concern. The solution is not necessarily to avoid the Internet and other digital technologies; rather, more Internet safety education and prevention information are needed to raise awareness for youths, adults and practitioners. Adults, including helping professionals, who are not confident and do not feel well-versed in new digital technologies, must acknowledge that the Internet is a new space for individuals to connect and converse, both positively and negatively. Having the knowledge and skills to help online sexual harassment victims is necessary in this new era.

References:

A. Barak, Sexual Harassment on the Internet, Social Science Computer Review , vol. 23 no. 1, [2005].

A. Barak, Cross – c-Cultural Perspectives on Sexual Harassment. In W. O'Donohue (Ed.) Sexual Harassment: Theory, Research & Treatment, (Boston, Allyn & Bacon), [1997].

A. Barak & A. King, The Two Faces of the Internet: Introduction to the Special Issue on the Internet and Sexuality. CyberPsychology and Behavior, 3, [2000].

A. Chaudhuri, Are Social Networking Sites a Source of Online Harassment for Teens? Evidence from Survey Data, Net Institute, Online Working Paper, [2008].

A. Cooper, I. McLoughlin, P. Reich, J. Kent-Ferraro, Virtual Sexuality in the Workplace: A Wake-up Call for Clinicians, Employers and Employees. In A. Cooper (Ed.) Sex and the Internet: A Guidebook for Clinicians, (New York, Brunner – Routledge), pp. 109 – 128, [2002].

A. Cooper, G. Golden & J. Kent-Ferraro, Online Sexual Behaviors in the Workplace: How Can Human Resource Departments and Employee Assistance Programs Respond Effectively? Sexual Addiction and Compulsivity, 9, [2002].

B. Szoka et al., Cyberbullying Legislation: Why Education is Is Preferable to Regulation, The Progress & Freedom Foundation, Volume 16, Issue 12, [2009].

C. Cunneen & J. Stubbs, Male Violence, Male Fantasy and the Commodification of Women through the Internet. Interactive Review of Victimology, 7, [2000].

C. Wilson, Feds: Online Sextortion of Teens on the Rise, Online, NBCNews, available at <www.nbcnews.com>, (visited (16/3/ March 2013).

D. Harvey, Cyberstalking and Internet Harassment: What the Law Can doDo, Online, Internet Safety Group, available at <www.netsafe.org.nz>, [2003].

D. Sacco et al., Sexting: Youth Practices and Legal Implications, Berkman Center for Internet & Society, Research Publication No. 2010 – 8, [22 June, 22, 2010].

D. Taylor, Internet Service Providers (ISPs) and their Responsibility for Content under New French Legal Regime, Computer Law and Security Report, Vol. 20, Issue 4.

E. Lievens, Bullying & Sexting in Social Networks from a Legal Perspective: Between Enforcement and Empowerment, ICRI Working Paper 7/20102, [20 June 20, 2012].

F. Till, Sexual Harassment: A Report on the Sexual Harassment of Students. (Washington DC, Advisory Council on Women's Educational Programs), [1980].

G. Lovet, Fighting Cybercrime: Technical, Judicial & Ethical Challenges, Virus Bulletin Conference, September [2009], available at <www.fortiguard.com>.

J. Morahan- – Martin, Women and the Internet: Promise and Perils. CyberPsychology and Behavior, 3, [2000].

J. Richman et al., Sexual Harassment and Generalized Workplace Abuse among University Employees: Prevalence and Mental Health Correlates, American Journal of Public Health, 89, [1999].

J. Suler, To Get What You Need: Healthy and Pathological Internet Use. CyberPsychology and Behavior, 2, [1999], 385 – -394.

K. Mitchell, D. Finkelhor & J. Wolak, The Exposure of Youth to Unwanted Sexual Material on the Internet: A National Survey of Risk, Impact, and Prevention. Youth & Society, 34, [2003].

L. Ellison & Y. Akdeniz, Cyberstalking: The Regulation of Harassment on the Internet, Criminal Law Review, December, [1998].

L. Fitzgerald, M. Gelfand & F. Drasgow, Measuring Sexual Harassment: Theoretical and Psychometric Advances. Basic and Applied Social Psychology, 17, [1995].

L. Fitzgerld, V. Magley, F. Drasgow & C. Waldo, Measuring Sexual Harassment in the Military, The Sexual Experiences Questionnaire (SEQ – DoD). Military Psychology, 11, [1999].

M. Chawki, Online Child Sexual Abuse: The French Response, Journal of Digital Forensics, Security & Law, Vol. 4, No. 4, [2009].

M. de la Cerna, Sextortion, [Online], Cebu Daily News, available at: <www.newsinfo.inquirer.net>, (visited 16/03/2013).

McGuire & E. Casey, Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace. Journal of the American Academy of Psychiatry and the Law, 30, [2002].

N. Levy et al., Bullying in a Networked Era: A Literature Review, Berkman, Research Publication No. 2012 – 17, [2012], available online.

P. Bocij, Cyberstalking: Harassment in the Internet Age and How to Protect Your Family, Westport, CT: Praeger, [2004].

Q. Li, Gender and CMC: A Review on Conflict and Harassment, Australasian Journal of Educational Technology, 2005, 21 (3), pp. 382 – 406.

R. Kool, Prevention by All Means? A Legal Comparison of the Criminalization of Online Grooming and Its Enforcement, Utrecht Law Review, Vol. 7, No. 3, [2011].

S. Kierkegaard, Cybering, Online Grooming and Age Play, Computer Law & Security Report, 24, [2008].

S. Leiblum & N. Döring, Sex and the Internet: A Guidebook for Clinicians, New York: Brunner- – Routledge, [2002].

S. Schenk et al., Cyber- – Sexual Harassment: The Development of the Cyber- – Sexual Experiences Questionnaire, McNair Journal, Vol. 12, Issue 1, [2008].

T. Hoeren, The European Liability and Responsibility of Providers on Online – Platforms Such as Second Life , JILT, 1 [2009].

1 Mohamed CHAWKI, LL.B, BA, LL.M, Ph.D is a Senior Judge; Founder and Chairman of the International Association of Cybercrime Prevention (IACP) , Paris, France; & and Research Fellow at the Center of Terrorism Law , St. Mary's University School of Law, Texas, USA. ; Email: chawki@cybercrime-fr.org; . Yassin el SHAZLY, LL.B, LL.M, Ph.D is a Senior Lecturer at the Faculty of Law, University of Ain-Shams, Cairo, Egypt; & and Legal Expert at the National Telecommunication Supervisory Authority. ; Email: yassin_shazly@hotmail.com.

2 See B. Roberts & R. Mann, Sexual Harassment in the Workplace: A Primer, available at: <www3.uakron.edu>, (visited 14/02/ February 2013).

3 See Unwanted Sexual Attention, available at: <www.getiton/nhs.uk>, (visited 17/03/ March 2013).

4 Ibid.

5 See The Center for Health and Gender Equity, Ending Violence against Women, [1999], available at <www.info.k4health.org>, (visited 14/02/ February 2013).

6 See Internet Harassment, available at <www.unc.edu>, (visited 14/02/ February 2013).

7 Ibid.

8 See N. Goodno, Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws , Missouri Law Review, Vol. 72, [2007].

9 Ibid.

10 See ENISA Position Paper No. 1 "'Security Issues and Recommendations for Online Social Networks"', edited by Giles Hogben, [October 2007]. Available at <www.enisa.europa.eu>, (visited 18/03/ March 2013).

11 Ibid.

12 See ENISA Position Paper No. 1 "'Security Issues and Recommendations for Online Social Networks"', edited by Giles Hogben, [October 2007]. Available at <www.enisa.europa.eu>, (visited 18/03/ March 2013).

13 Ibid.

14 Ibid.

15 See E. Porterfield, Facebook Cyberstalking Shocker: Preteen Girls Charged In Issaquah Case, available at <www.huffingtonpost.com> (visited 18/03/ March 2013).

16 Ibid.

17 See ENISA Position Paper No. 1 "'Security Issues and Recommendations for Online Social Networks"', edited by Giles Hogben, [October 2007]. Available at <www.enisa.europa.eu>, (visited 18/03/ March 2013).

18 Ibid.

19 Ibid.

20 Ibid.

21 Ibid.

22 See Online Grooming Accused in Court, available at <www.theherald.com.au> , (visited 21/03/ March 2013).

23 Ibid.

24 Ibid.

25 See Sextortion, available at <www.gistmania.com>, (visited 17/03/ March 2013).

26 Ibid.

27 See Teen Arrested on Sexting Extortion Charges, available at <www.newstalk1010.com>, (visited 18/03/ March 2013).

28 Ibid.

29 Ibid.Ibid

30 See <www.secondlife.com>.

31 See Catherine Waerner, Thwarting Sexual Harassment on the Internet, available at: <www.uow.edu.au>, (visited (14/3/ March 2013).

32 Ibid.

33 Ibid.

34 See Predator Statistics, available at <www.internetInternetsafety101.org> , (visited 18/03/ March 2013).

35 Ibid.

36 Ibid.

37 Ibid.

38 Ibid.

39 Ibid.

40 Ibid.

41 Ibid.

42 Ibid.

43 Ibid.

44 Ibid

45 See Cyberstalking, available at <www.cyberguards.com> , (visited 21/03/2013).

46 Ibid

47 Ibid.

48 Ibid.

49 Arizona Criminal Code (1995): 13 -– 2921.

50 Alaska Criminal Law Sec. 11.41.270.

51 Connecticut Penal Code Sec. 53a -– 183.

52 New York Penal Code § 240.30.

53 Oklahoma Code (1996): § 21 -– 1173.

54 Wyoming Code, 6 – 2 -– 506.

55 See United States v. Baker, 104 F. 3d 1492, [Jan. 29, 1997].

56 See Sexual Offences Act 2003, Sections 45 and 15.

57 A 'telecommunications system"' is defined in section 4(1) of the Telecommunications Act 1984 as "'a system for the conveyance, through the agency of electric, magnetic, electromagnetic, electro-chemical or electro-mechanical energy, of: (a) Speech, music and other sounds. (b) Visual images. (c) Signals serving for the impartation.....of any matter otherwise than in the form of sounds or visual images..."'.

58 The Criminal Justice and Public Order Act 1994, s.92 increased the maximum fine for an offence under section 43 to level 5 from level 3 and made it an imprisonable offence with a maximum term of six months. The new sentencing powers brings the penalty more into line with the maximum sentence for transmitting indecent or obscene material through the post (which is 12 months' imprisonment) contrary to section 11(2) of the Post Office Act 1953.

59 Also note that the Malicious Communications Act 1988 s.1 creates an offence of sending letters which convey, inter alia, threats with the purpose of causing distress or anxiety. The

Act does not however cover telecommunications messages, however.

60 A person guilty of this offence is liable to imprisonment for a term not exceeding six months: s.2(2).

61 A person guilty of this offence is liable to imprisonment for a term not exceeding five years: s.4(4).

62 See Cyberstalker Targets Women in 16,000 Tweets, available at <www.quarduian.co.uk>, (visited 20/03/ March 2013).

63 Ibid.

64 Ibid.

65 See Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography.

66 Following the ratification by the Netherlands on 1 March 2010 and San Marino on 22 March 2010, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) entered into force on 1 July 2010.

67 See <www.cybersitter.com>.

68 See <http://www.netnanny.com/netnanny>.

69 Before adopting this law, the responsibility of ISPs was governed by the French law n°2000-719 of 1st August 2000. Under this law, ISPs were liable under French civil or criminal responsibility for the illegal content of the web sites to which they provide access, only if they have not promptly undertaken the appropriate measures to block access to such content after a judicial decision. See Estelle Halliday v Valentin Lacambre.

70 « 'Elle a pour objectif d'adapter la législation actuelle au développement de l'économie numérique afin de renforcer la confiance dans l'économie électronique et d'assurer le développement de ce secteur, tout en établissant un cadre juridique stable pour les différents acteurs de la société de l'information' ». Sénat (2007), Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, Report, Paris. Available at <www.senat.frwww.senat.fr>.

71 In fact, the Senate has deleted the amendments to Article 2 of the LEN covering the regime governing the responsibility of ISPs that had been included by the National Assembly. This thereby removed the specific obligation to monitor certain types of content, including paedophilepedophile and racist material, which undermined the general principle of no obligation to monitor content generally, ; See see D. Taylor op. cit. p. 270.

72 European Digital Rights was founded in June 2002. Currently 35 privacy and civil rights organisations have EDRI membership. They are based or have offices in 21 different countries in Europe.

73 See French Draft Law Obliges Providers to Monitor Internet, available at <www.edri.orgwww.edri.org>.

74 Ibid.

75 Article 225 – 6.

76 The AFA was created in 2000; it is the amalgamation of two previous associations: the Association Française des Professionnels de l'Internet created in 1996 and the Association des Fournisseurs d'Accès à des Services en ligne et à l'Internet created in 1997. Both associations were set up mainly to define common practices regarding illegal content, especially child pornography.

77 See J. Bonnici, Internet Service Providers and Self –Regulation: A Process to Limit Internet Service Providers Liability in Cyberspace, available at <www.rug.nl>.

78 Ibid.

79 Ibid.

80 Ibid.

81 Ibid.

Breathing Space for Cloud-Based Business Models

Exploring the Matrix of Copyright Limitations, Safe Harbours and Injunctions

by **Martin Senftleben**, Ph.D.; Professor of Intellectual Property, VU University Amsterdam; Senior Consultant, Bird & Bird, The Hague.

Abstract: Cloud-based services keep forming, changing and evaporating like clouds in the sky. They range from personal storage space for films and music to social media and user-generated content platforms. The copyright issues raised by these platforms seem as numerous as the liquid droplets and frozen crystals constituting clouds in the atmosphere of our planet. As providers of cloud-based services may seek to avoid dependence on creative industries and collecting societies, one of these questions concerns the breathing space that copyright law offers outside the realm of exclusive rights. Which limitations of protection can serve as a basis for the development of new business models? Which safe harbours may be invoked to avoid secondary liability for copyright infringement? Which obligations may result from injunctions sought by copyright owners? After outlining relevant cloud services (section 1) and identifying the competing interests involved (section 2), the inquiry will address these influence factors – limitations, safe harbours and injunctions (section 3). The analysis will yield the insight that the most effective protection of copyright in the cloud is likely to result from acceptance of a compromise solution that, instead of insisting on the power to prohibit unauthorised use, leaves room for the interests of users and the business models of platform providers (concluding section 4).

Keywords: Cloud Computing; Economic Policy Concerns; European Law; Competition Law

Recommended citation: Martin Senftleben, Breathing Space for Cloud-Based Business Models; Exploring the Matrix of Copyright Limitations, Safe Harbours and Injunctions, 4 (2013) JIPITEC 2, para 87

A. Cloud-Based Service

1 Before embarking on a discussion of breathing space for cloud-based business models, it is necessary to clarify the type of websites that will be addressed in the following analysis. As it is difficult to trace the conceptual contours of the 'cloud',[1] a wide variety of online platforms inevitably enters the picture. If the 'cloud' is equated with the Internet, the discussion may even degenerate into a general debate on the scope of copyright protection in the digital environment.

2 To avoid this generalization, the present inquiry will focus on services that offer individual users the opportunity of storing copyrighted material on an on-

line platform.[2] This clarification still leaves room for the inclusion of various types of platforms and services. A distinction can be drawn, however, with regard to the size of the target audience:

- an online platform for posting photographs, such as Flickr, or an online platform for posting videos, such as YouTube, allows individual users to make content generally available on the Internet. In this case, the general public with access to the Internet is the target audience.
- a social networking site, such as Facebook, allows individual users to post various types of works, such as texts, photographs and videos. In this case, the target audience is not the general public. It is a specific group of Internet users having access to the personal webpages of the individual user providing content.
- a digital locker service allowing individual users to upload personal copies of protected works to personal cloud storage space for later downloading or streaming on multiple devices, or a private video recorder allowing users to obtain recordings of TV programmes for the purpose of watching them at a more convenient time. In this case, the target audience is confined to the individual user.

B. Interests Involved

3 On the basis of this outline of relevant storage services, the different stakeholders involved can be identified: copyright owners, platform providers and individual users. If cloud-based services are used to disseminate protected works without prior authorization, copyright owners may want to invoke their exclusive rights to prohibit the use or claim an appropriate reward.[3] They will point out that without the enforcement of their rights, sufficient incentives for new creativity, on-going investment in cultural productions and an adequate income from creative work cannot be ensured.[4]

4 Platform providers, however, will argue that a general obligation to monitor the data streams generated by users is too heavy a burden, and that instead, the risk of platforms being held liable for copyright infringement must be minimized. Otherwise, exposure to that risk would force them to close down their websites. The vibrant Internet as we know it today would cease to exist.[5]

5 Finally, individual users benefitting from cloud-based services are not unlikely to emphasize that their interests go far beyond mere convenience and entertainment. Online platforms for publishing photographs and videos afford them the opportunity to get actively involved in the creation of online content. Enhanced user participation strengthens the role of the Internet as a democratic medium that offers room for a wide variety of opinions and contributions.[6] Social media offer new forms of self-expression and social interaction. Private video recorders can be seen as a service facilitating access to TV streams and, therefore, as a means of supporting the receipt of information.[7]

6 The protection of copyright is thus to be reconciled with several competing interests. Against this background, policy makers are not unlikely to weigh the rationales of copyright protection against other values, such as freedom of expression and information, the interest in maintaining an open Internet, the freedom to conduct a business and a participatory Internet culture. Moreover, it must not be overlooked that at the policy level, economic considerations may play a crucial role. As a medium that keeps generating new business models, the Internet still offers a remarkable potential for economic growth.[8] Breathing space for the development of cloud-based services, therefore, can be part of a country's innovation policies.[9]

C. Survey of Flexibility Tools

7 Given the diversity of interests involved, it is not surprising that different strategies have emerged to regulate the impact of copyright protection on cloud-based services. A survey of available regulatory instruments leads to a matrix of copyright limitations, safe harbours for hosting, and injunctions against online platforms. Copyright limitations can be adopted to exempt certain forms of generating online content from the control of the copyright owner (subsection C I). Safe harbours for hosting services can be introduced to shield platform providers against the risk of secondary liability for infringing content made available by users (subsection C II). Injunctions against platforms providers (subsection C III) can be granted to allow copyright owners to take action against infringers.

I. Copyright Limitations

8 As clarified above, the present inquiry focuses on services that offer individual users the opportunity of storing copyrighted material on an online platform. Depending on the involvement of the user in the creation of the content, and the target audience that is reached, different limitations of copyright can become relevant in this context. Breathing space may result from inherent limits of exclusive rights, such as limits set to the right of adaptation in national law. It may also result from the adoption of exceptions that exempt certain forms of use from the control of the copyright owner. To provide an over-

view, amateur remixes of protected works (C I 1) can be distinguished from the use of links (C I 2) and private copying (C I 3). The discussion, finally, leads to whether a more flexible approach to limitations is required to keep pace with the fast development of cloud-based services (C I 4).

1. Quotations, Adaptations and Remixes

9 In many cases, users of cloud-based services will upload their own literary or artistic creations to online platforms and social networking sites. If the protected work of another author is quoted, adapted or remixed, however, the question arises whether a copyright limitation can be invoked to justify the unauthorised use. In most countries, the debate on user-generated content has not yet led to agreement on specific exceptions.[10] The inclusion or adaptation of protected material thus depends on the scope of traditional copyright limitations. The taking of portions of a protected work can constitute a permissible quotation.[11] An adaptation seeking to ridicule the original work may fall under the exemption of parody.[12]

10 In copyright systems providing for an open-ended fair use limitation, specific criteria may be available to draw a line between infringing copying and permissible remix and reuse. Under the US fair use doctrine, for instance, the notion of transformative use traditionally constitutes an important factor capable of tipping the scales to a finding of fair use.[13] In the famous parody case Campbell v Acuff-Rose, the US Supreme Court explained with regard to the fair use analysis:

> *The central purpose of this investigation is to see [...] whether the new work merely supersedes the objects of the original creation [...] or instead adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message; it asks, in other words, whether and to what extent the new work is 'transformative'.*[14]

11 In comments on the fair use doctrine, the notion of transformative use is understood in the sense of productive use. The fair use must aim to employ the copyrighted matter in a different manner or for a purpose different from the original. Mere repackaging or republication is insufficient. By contrast, a use adding value to the original, transforming the original in new information, new aesthetics, new insights and understandings, constitutes 'the very type of activity that the fair use doctrine intends to protect for the enrichment of society'.[15] The identification of use that supports freedom of speech and cultural follow-on innovation, therefore, lies at the core of the analysis.

12 This rationale can serve as a guiding principle when a distinction must be drawn between infringing and permissible user-generated content. In Warner Bros. and J.K. Rowling v RDR Books, for instance, the US District Court for the Southern District of New York assessed the contents of an online Harry Potter fan site in the light of the notion of transformative use.[16] The platform Harry Potter – The Lexicon provides an encyclopaedia of the individual characters, magic spells, beasts, potions, etc. described in the Harry Potter books.[17] Inevitably, this requires the reuse of parts of the original Harry Potter books. The Court, however, took as a starting point that The Lexicon was transformative:

> *Because it serves these reference purposes, rather than the entertainment or aesthetic purposes of the original works, the Lexicon's use is transformative and does not supplant the objects of the Harry Potter works...*[18]

13 The recognition of this added value to the general public, however, did not hinder the judge from holding that verbatim copying on the fan site amounted to copyright infringement where it was in excess of the legitimate purpose of providing a reference tool. The wholesale taking of substantial portions of background material provided by J.K. Rowling herself, for instance, did not constitute fair use. The Court thus drew a line between permissible content supporting the transformative character of the website and infringing content that was unnecessary for the reference purposes served by The Lexicon.

14 Breathing space for user-generated adaptations of copyrighted works may also result from inherent limits set to the right of adaptation in national legislation. The adaptation right granted in the Dutch Copyright Act, for instance, does not cover adaptations constituting 'a new, original work'.[19] Hence, certain forms of adaptations remain free from the outset.[20] A similar mechanism for providing breathing space can be found in the German Copyright Act which contains a free use principle exempting adaptations that constitute 'independent works',[21] and the Austrian Copyright Act which exempts 'independent, new works' resulting from an adaptation.[22] Transformations of protected works falling under these free adaptation rules are immune against copyright claims brought by the copyright owner whose work served as a basis for the adaptation. Traditionally, the courts in Austria, Germany and the Netherlands created room for parody in this way.[23]

15 When a free adaptation rule of this kind is invoked, the crucial question becomes which criteria are applied to identify those adaptations that can be deemed free in the sense that they do not affect the copyright owner's right of adaptation. Under the German free adaptation rule, this question is answered by requiring a transformation of the original work to have new features of its own that make the individual features of the original work fade away.[24] Applying this standard, the German Federal Court of Justice recognised in parody cases that the required distance from the original work, making its in-

dividual features fade away, could not only be achieved through substantial alterations of the original work. By contrast, an inner distance, such as the distance created by a parodist's mockery, could also be sufficient.[25]

16 When applied broadly, this line of reasoning could become relevant in cases of user-generated content. Arguably, the individual, non-commercial nature of amateur remixes may also justify to assume an inner distance from the underlying original work. If the remix clearly constitutes an amateur creation that is presented on the Internet without profit motive, the contrast with the original work will be obvious to the Internet public. User-generated content falling in this category could then be exempted on the grounds that it constitutes an 'independent work' that makes the features of the original work fade away.[26] The fact that the rules on free adaptations have often been applied in parody cases does not exclude an extension to other areas, such as user-generated content. In the Perlentaucher case, for instance, the German Federal Court of Justice confirmed the general applicability of the principles governing the determination of free adaptations. In this case, the question of a free adaptation arose with regard to abstracts derived from book reviews in the German newspaper Frankfurter Allgemeine Zeitung.[27] The sound sampling case Metall auf Metall can serve as a further example of the universal applicability of the rules governing free adaptations.[28]

17 Breathing space for adaptations of protected works may thus follow from specific exceptions, such as the right of quotation and the exemption of parody. It may also result from open-ended copyright limitations supporting transformative use and free adaptation rules leaving room for derivative works that keep a sufficient (inner) distance from the original work. When a remix or adaptation does not amount to copyright infringement, the resulting derivative work can be disseminated on the Internet without encroaching upon the exclusive rights of the author whose work served as a basis for the remix. Breathing space for remixing and adapting protected works, thus, also creates breathing space for online platforms and social media that allow users to present their remixes and adaptations to the public.

2. Embedded Content

18 For sharing information about a literary or artistic creation, a user of cloud-based services need not necessarily upload the copyrighted work as such. Instead, a link can be sufficient to draw the attention of other users to protected content that has already been made available elsewhere on the Internet. The user of a social networking platform, for instance, may use a link to 'embed' protected content from an external source in her personal pages. The external content may then be displayed within a frame that is integrated in the user's webpages – a technique often referred to as 'framing' or 'in-line linking'. In contrast to the traditional hyperlink with underlined blue text, visitors of the personal pages need not leave the networking site when following the link. By contrast, the embedded content – for example, a music video – is shown within the framework of the personal pages. This advanced form of embedded linking raises delicate copyright issues.[29]

19 On the one hand, it may be argued that the embedded link makes the work available for a new public – the group of Internet users having access to the user's personal webpages. Viewed from this perspective, it may be qualified as a relevant act of communication to the public comparable with the further distribution of radio and TV signals in hotels, or a relevant act of public performance comparable with the playing of radio music in restaurants.[30] This parallel is doubtful, however, because at least a classical hyperlink does not extend the audience. It merely indicates the location of content that has already been made available to the Internet audience on another webpage.[31] With regard to 'frames' and 'in-line links', it would have to be explained against this background why the use of a more advanced linking technique justifies the assumption that there is a new audience to be distinguished from the audience formed by Internet users in general.[32]

20 Given these doubts, an emphasis may be laid, on the other hand, on the fact that the embedded link only provides a reference to protected content that is already available for Internet users on another website. As long as it is clear that the content stems from another online source,[33] the embedded link does not differ substantially from a traditional hyperlink that, according to established case law, does not constitute an infringing act of communication to the public. In the EU, the German Federal Court of Justice recognised in its famous Paperboy decision that without search services availing themselves of hyperlinks to indicate the location of online content, the abundant information available on the Internet could not be found and used in an efficient way.[34] In line with previous statements in literature,[35] hyperlinks were seen as mere footnotes: a means of safeguarding freedom of information in the digital environment and ensuring the proper functioning of the Internet. Taking this insight as a starting point, the Court arrived at the conclusion that a hyperlink – the case concerned deep links to press articles – did not amount to copyright infringement:

21 A person who sets a hyperlink to a website with a work protected under copyright law which has been made available to the public by the copyright owner, does not commit an act of exploitation under copyright law by doing so but only refers to the

work in a manner which facilitates the access already provided.[36]

22 The Court fortified this approach by pointing out that the person setting the hyperlink refrained from keeping the work on demand or transmitting it herself. Moreover, that person had no control over the availability of the work. If the web page containing the work was deleted, the hyperlink would miss its target and become pointless.[37] The courts in other EU Member States lent weight to similar arguments in the context of more advanced forms of linking. In the Vorschaubilder case, the Austrian Supreme Court, for instance, developed the following line of reasoning with regard to picture thumbnails of portrait photographs that had been displayed as search results together with the URL of the source webpage:

> *Only the person who has the original or a copy of a work can make that work available to other persons in a way that allows him to control access to the work. A person [...] who only provides a link that can be used to view the work at its original location, however, only facilitates access to a file included in the source website without making that work available himself in the sense of § 18a of the Copyright Act. Under these circumstances, he does not control access, as the file can be deleted without his intervention....*[38]

23 These examples show that breathing space for references to online content can be derived from an interpretation of the exclusive rights of copyright owners that leaves room for the application of different kinds of links. The considerations supporting the refusal of copyright infringement in the German Paperboy case and the Austrian Vorschaubilder case can be employed to exempt the use of 'frames' and 'in-line links' to provide references to external content on social networking pages.[39] As long as the use does not amount to an infringement of other intellectual property rights or an act of unfair competition, this exemption would have the result of platform providers being free to offer 'framing' and 'in-line linking' as features of their platforms and users being free to refer to content available elsewhere on the Internet.

3. Digital Lockers

24 While breathing space for the use of cloud-based services may thus result from limits that are set to exclusive rights, copyright exceptions can also constitute an important basis for new cloud-based services. The exemption of private copying, for instance, can serve as a basis for digital lockers or personal TV recorders. If a protected work is uploaded to a platform offering personal storage space for films and music, the creation of a cloud copy may qualify as a permissible act of private copying. This is true, at least, when the cloud copy is made by the private user and access to that copy is confined to the individual user making personal use of the digital locker for the purpose of private study and enjoyment.

25 In this vein, the US Court of Appeals for the Second Circuit held in the Cablevision case with regard to an online video recorder that, first, it was the user, rather than Cablevision as a provider, who did the copying produced by the recording system;[40] and, second, that the transmission of works required for the playback function of the service did not amount to a relevant act of public performance

> *[b]ecause each RS-DVR playback transmission is made to a single subscriber using a single unique copy produced by that subscriber.*[41]

26 Similarly, the German Federal Court of Justice held in the Shift.TV case that, rather than the provider of the service, the private user of the automated system for recording TV broadcasts was responsible for making copies of protected works, and that the public required for an act of communication to the public was missing because each individual copy was made available only to the subscriber who had made that copy.[42] However, this decision in favour of the applicability of private use privileges did not hinder the German Federal Court of Justice from also finding that the transmission of over-the-air TV signals to the online recorders of private subscribers could be qualified as an infringing act of retransmission.[43] The Court, therefore, neutralized its initial finding in favour of private use by also holding that the automated Shift.TV system might encroach upon the retransmission right of broadcasting organizations.[44]

27 From the outset, the invocation of private use as a defence was excluded by the Supreme Court of Japan in the Rokuraku II decision. In this case, an emphasis was laid on the preparatory acts of receiving and feeding TV broadcasts carried out by the service provider. As these preparatory acts finally enabled the private user to obtain a copy of the works, the Court held that it was not the private user, but the provider of the TV recorder system who made the copies of TV programmes.[45]

28 These divergent court decisions do not come as a surprise. Traditionally, the exception for private copying is one of the most controversial exceptions in copyright law.[46] National private copying systems differ substantially in terms of scope and reach. Restrictive systems may not offer more than the opportunity to make a recording of a TV programme for the purpose of watching it at a more convenient time ('time-shifting').[47] As demonstrated by the Cablevision case in the US, even a private copying regime with this limited scope may offer breathing space for an online service that facilitates time-shifting by allowing subscribers to make a recording of TV programmes in the cloud.

29 More generous private copying regimes are not confined to time-shifting. Several continental European copyright regimes may generally allow the uploading of copies to personal storage space in the cloud

for private use as long as the initiative for the reproduction is taken by the private user.[48] However, differences between these more generous systems follow from the individual configuration of the use privilege at the national level. Must the private copy be made by the private user herself? Or could it also be made by a third party on her behalf? In the latter case, does it matter whether this third person derives economic benefit from the private copying? Does private copying require the use of a legal source? Or may even an illegal source serve as a basis for a legitimate private copy?[49] Does it become relevant in this context whether the illegality was evident to the private user?[50]

30 While these nuances must be taken into account when determining the permissible ambit of operation of digital locker services, a further layer of legal complexity results from the fact that at least broad private copying exemptions not focusing on specific purposes will give rise to an obligation to provide for the payment of equitable remuneration. Otherwise, the private copying regime is not unlikely to cause an unreasonable prejudice to the legitimate interests of the copyright owner in the sense of the third step of the international three-step test.[51] The possibility of reducing an unreasonable prejudice to a reasonable level through the payment of equitable remuneration is reflected in the drafting history of the first international three-step test laid down in Article 9(2) BC. At the 1967 Stockholm Conference, Main Committee I – working on the substantive provisions of the Berne Convention – gave the following example to illustrate this feature of the international three-step test:

> *A practical example might be photocopying for various purposes. If it consists of producing a very large number of copies, it may not be permitted, as it conflicts with a normal exploitation of the work. If it implies a rather large number of copies for use in industrial undertakings, it may not unreasonably prejudice the legitimate interests of the author, provided that, according to national legislation, an equitable remuneration is paid. If a small number of copies is made, photocopying may be permitted without payment, particularly for individual or scientific use.*[52]

31 The determination of an adequate level of equitable remuneration for a broad private copying privilege is a challenging task. In the European Union, the Court of Justice of the European Union (CJEU) sought to provide an answer in the Padawan decision. The CJEU stated that

> *fair compensation must necessarily be calculated on the basis of the criterion of the harm caused to authors of protected works by the introduction of the private copying exception.*[53]

32 The Court also made it clear that a distinction had to be drawn between private users who could be expected to copy protected works,[54] and professional users who were unlikely to make private copies. While the payment of fair compensation had to cover the use made by private users, professionals would use the available storage space for professional purposes not involving the unauthorised reproduction of the protected works of third parties. Professional users thus had to be exempted from the payment obligation.[55]

33 In the case of a digital locker in the cloud, this approach taken in the EU would mean that the calculation of equitable remuneration requires an assessment of the harm flowing from the cloud service and a distinction between private and professional use. The impressive list of prejudicial questions on adequate remuneration that is currently pending before the CJEU[56] indicates that the application of this standard poses substantial difficulties already with regard to traditional storage media and copying equipment.[57] Private copying in the cloud is not unlikely to generate further prejudicial questions in the near future.[58]

4. Update of Exceptions

34 Besides the difficulty of ascertaining the amount of equitable remuneration, the uploading of private copies to digital lockers in the cloud also raises important questions with regard to the further development of the exception for private copying and copyright exceptions in general. In practice, the provider of private storage space in the cloud is not unlikely to avoid the multiplication of identical private copies on the server. If several subscribers upload the same film to their individual digital lockers, the provider may decide to give these users access to one central master copy instead of allowing them to make several identical copies.

35 In light of the rules established in copyright law, however, use of a master copy that can be accessed by a potentially large group of subscribers gives rise to the question whether the use can still be qualified as an act of private copying. On the one hand, the use possibilities of the individual users are not enhanced. From a functional perspective, the master copy is only used to achieve a result identical to the situation arising from the storage of a unique private copy for each individual subscriber. On the other hand, the use of a single master copy for the execution of several requests may be seen as an infringing act of making this master copy available to a broader public.[59] From a technical perspective, the fact remains that the subscriber does not have access to a unique cloud copy made on the basis of the file she has on her personal computer. Instead, she obtains access to a master copy that is made available by the provider of the digital locker.

36 Hence, the question arises whether the private copying exception can be interpreted flexibly on the basis of a functional analysis or must be read narrowly in line with a technical analysis. A functional analysis would focus on the use possibilities of the private

user. As long as these possibilities are not enhanced in comparison with a situation where a unique copy is made for each individual subscriber, use of a master copy would still fall within the scope of the private copying exception. The breathing space for digital locker services would thus increase. A technical analysis, by contrast, would allow the scrutiny of each individual act of use carried out by the provider of cloud storage space. Accordingly, it makes a difference whether each subscriber makes and obtains access to her own unique copy (communication to the public may be denied), or whether instead, the provider offers access to a master copy (communication to the public may be assumed).

37 In the EU, room for a flexible, functional approach to cloud-based private copying services cannot readily be derived from CJEU jurisprudence. Formally, the CJEU adhered to the dogma of strict interpretation of copyright exceptions in the Infopaq/DDF case. Scrutinizing the mandatory exemption of transient copies in EU copyright law,[60] the Court pointed out that for the interpretation of each of the cumulative conditions of the exception, it should be borne in mind that,

> *according to settled case-law, the provisions of a directive which derogate from a general principle established by that directive must be interpreted strictly [...]. This holds true for the exemption provided for in Article 5(1) of Directive 2001/29, which is a derogation from the general principle established by that directive, namely the requirement of authorisation from the rightholder for any reproduction of a protected work.*[61]

38 According to the Court,

> *[t]his is all the more so given that the exemption must be interpreted in the light of Article 5(5) of Directive 2001/29, under which that exemption is to be applied only in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.*[62]

39 This further consideration seems to indicate that the Court infers, from the three-step test enshrined in the Information Society Directive, the necessity of a strict interpretation of exceptions. In Football Association Premier League, however, the decision in Infopaq/DDF did not hinder the Court from emphasizing with regard to the same exemption the need to guarantee its proper functioning and ensure an interpretation that takes due account of the exemption's objective and purpose. The Court explained that, in spite of the required strict interpretation of the conditions set forth in Article 5(1) of the Information Society Directive,

> *the interpretation of those conditions must enable the effectiveness of the exception thereby established to be safeguarded and permit observance of the exception's purpose as resulting in particular from recital 31 in the preamble to the Copyright Directive and from Common Position (EC) No 48/2000 adopted by the Council on 28 September 2000 with a view to adopting that directive (OJ 2000 C 344, p. 1).*[63]

40 The Court went on to explain more generally that

> *[i]n accordance with its objective, that exception must allow and ensure the development and operation of new technologies and safeguard a fair balance between the rights and interests of right holders, on the one hand, and of users of protected works who wish to avail themselves of those new technologies, on the other.*[64]

41 In light of these considerations, the Court concluded that the transient copying at issue in Football Association Premier League, performed within the memory of a satellite decoder and on a television screen, was compatible with the three-step test in EU copyright law.[65] This ruling seems to indicate that the CJEU, as many national courts in EU Member States, formally adheres to the dogma of a strict interpretation of exceptions. The adoption of this general principle, however, need not prevent the Court from arriving at a more balanced solution in individual cases.[66] By contrast, the dogma of strict interpretation itself may be applied rather flexibly by the Court.

42 Against this background, it is of particular interest that in Painer/Der Standard, the CJEU again underlined the need for a fair balance between 'the rights and interests of authors, and [...] the rights of users of protected subject-matter'.[67] More specifically, the Court clarified that the right of quotation in EU copyright law[68]

> *was intended to strike a fair balance between the right of freedom of expression of users of a work or other protected subject-matter and the reproduction right conferred on authors.*[69]

43 Along these lines drawn in the Football Association Premier League and Painer/Der Standard decisions, the CJEU may arrive at a flexible, functional approach to the exception for private copying with regard to digital lockers in the cloud. This flexible approach to the private copying exception would lead to additional revenue streams flowing from levies that are due for private copying in the cloud.[70] It is noteworthy that the Court already opted for such a functional approach in the UsedSoft/Oracle case. Answering the question whether the downloading of software from the Internet exhausts the distribution right of the copyright owner, the Court drew a functional parallel with the sale of software on CD-ROM or DVD. According to the CJEU, it makes no difference

> *whether the copy of the computer program was made available to the customer by the rightholder concerned by means of a download from the rightholder's website or by means of a material medium such as a CD-ROM or DVD.*[71]

44 In this vein, it may be argued that it makes no difference whether the private user has access to a cloud copy of her own copy of a film, or to a master copy of the same film that is used by the provider of digital lockers in the cloud to satisfy individual requests by private users who have the film in their personal collection.

II. Safe Harbours

45 Whereas copyright exceptions exempt certain forms of generating online content from the control of the copyright owner and, accordingly, lead to the exclusion of direct liability for unauthorised use, safe harbours concern the question of secondary liability. A safe harbour can be introduced to shield platform providers against the risk of secondary liability for infringing content made available by users of online platforms. Safe harbours for hosting are of particular importance in this context (section C II 1). The invocation of this type of safe harbour, however, depends on appropriate reactions to notifications about infringing content (section C II 2). The breathing space for cloud-based services resulting from safe harbour regimes thus depends on the requirements that follow from accompanying obligations, such as the establishment of efficient notice-and-takedown systems.

1. Safe Harbour for Hosting

46 The so-called safe harbour for hosting relates to the storage of third-party content without any active involvement in the selection of the hosted material. In the EU, the E-commerce Directive refers to an information society service that consists of 'the storage of information provided by a recipient of the service'. This kind of safe harbour rests on the assumption that a general monitoring obligation would be too heavy a burden for platform providers. Without the safe harbour, the liability risk would thwart the creation of platforms depending on third party content and frustrate the development of e-commerce.[72]

47 With regard to safe harbours in the EU – covering all types of intellectual property[73] – the conceptual contours of the safe harbour for hosting have been clarified by the CJEU in cases that concerned the unauthorised use of trademarks in keyword advertising and in offers made on online marketplaces.[74] Because of the horizontal applicability of EU safe harbours across all types of intellectual property, the rules evolving from these trademark cases are also relevant to cases involving copyrighted works. In Google France/Louis Vuitton, the CJEU qualified the advertising messages displayed by the Google keyword advertising service as third-party content provided by the advertiser and hosted by Google. These advertising messages appear once the search terms selected by the advertiser are entered by the Internet user. The advertising is thus triggered by specific 'keywords'. In the keyword advertising cases decided by the CJEU, these keywords consisted of protected trademarks. Accordingly, the question arose whether the search engine would be liable for trademark infringement. As to the applicability of the safe harbour for hosting in these circumstances, the Court pointed out that it was necessary to examine

> *whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores.*[75]

48 The financial interest which Google has in its advertising service is not decisive in the framework of this examination. An active involvement in the process of selecting keywords, by contrast, would be relevant to the assessment of eligibility for the safe harbour.76 In the further case L'Oréal/eBay, the CJEU arrived at a more refined test by establishing the standard of 'diligent economic operator'. The Court explained that it was sufficient,

> *in order for the provider of an information society service to be denied entitlement to the exemption [for hosting], for it to have been aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question.*[77]

49 While stressing that this new diligence test should not be misunderstood to impose a general monitoring obligation on platform providers, the Court indicated that, under this standard, own investigations of the platform provider would have to be taken into account. Moreover, a diligent economic operator could be expected to consider even imprecise or inadequately substantiated notifications received in the framework of its notice-and-takedown system. According to the Court,

> *the fact remains that such notification represents, as a general rule, a factor of which the national court must take account when determining [...] whether the [service provider] was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality.*[78]

50 In sum, the current development of the requirements to be met for successfully invoking the safe harbour for hosting in the EU reflects a shift from a general exemption from investigations to an obligation to consider even imprecise notifications. Platform providers must set up a knowledge management system that reaches a certain level of sophistication.[79]

51 On the one hand, this development may be deemed desirable and consistent when focusing on service providers that are highly profitable enterprises. Market leaders in the area of online information services are capable of investing in enhanced content monitoring and improved knowledge management. On the other hand, it must not be overlooked that the prerequisites for invoking the safe harbour for hosting also determine the entrance level for newcomers on the market. The prerequisite of neutrality and passivity constitutes a relatively low entrance requirement that can be met by newcomers even if their financial resources are limited. A challenging knowledge management obligation that requires extra staff, by contrast, leads to a substantial

hurdle that newcomers without much capital may find insurmountable.

52 A high threshold for invoking the safe harbour for hosting, therefore, enhances the risk of market concentration. While well-established, profitable businesses may have little difficulty in fulfilling knowledge management obligations, the risk of being held liable because of insufficient knowledge management is not unlikely to inhibit newcomers from entering the market. Shying away from the risk of liability for third-party content, they may sell their ideas for new platforms to market leaders with fewer budget constraints. As a result, the vibrant Internet we know today – an effervescent source of new business models and services often invented and implemented by small providers – may become a medium governed by only a few major players.[80]

2. Notice-and-Takedown Procedures

53 As to the diversity and openness of online content, the requirements with regard to notice-and-takedown procedures are to be considered as well. In many countries, a platform provider availing itself of the immunity following from the safe harbour for hosting is under an obligation to promptly take action once sufficiently substantiated information about infringing content is received.[81] While the obligation to take measures upon notification seems to constitute a widely-shared standard, a survey of national regulations in this area sheds light on substantial differences. The detailed norms in the US Digital Millenium Copyright Act include not only a notice-and-takedown mechanism but also rules on counter-notices that may lead to the reinstatement of content.[82]

54 An unjustified takedown can thus be corrected if the user who had posted the content sends a counter-notice and rebuts the arguments supporting the initial takedown. Ultimately, unjustified 'censorship' may thus be remedied if the effort to bring a successful counter-notice keeps within reasonable limits. Nonetheless, concerns about unjustified takedowns have been articulated even under this system of notices and counter-notices.[83] Against this background, it is of particular interest that recent legislation in Canada departs from the notice-and-takedown model and provides for a notice-and-notice system instead.[84] When receiving information about infringing content, the platform provider is not obliged to remove the content. It is sufficient for the provider to inform the user who had posted the content about the notice. The Canadian lawmaker, therefore, does not see a need for a prompt removal of allegedly infringing content.[85]

55 EU legislation reflects an opposite focus on removal. Rules on counter-notices are sought in vain. The EU system generally provides for notice-and-takedown rather than preferring notice-and-notice procedures with regard to certain kinds of websites, such as social media. Upon receipt of a sufficiently substantiated notification about infringing content, the platform provider is obliged to act expeditiously to remove or disable access to the content at issue.[86] It is an open question whether this rudimentary harmonization stopping at the takedown step offers sufficient safeguards against unjustified removals. The current notice-and-action initiative in the EU may address this issue. Besides a quicker takedown for rights owners and increased legal certainty for platform providers, additional safeguards for fundamental rights, such as freedom of expression, are on the agenda.[87]

III. Injunctions Against Platforms

56 The survey of legal standards defining the breathing space for cloud-based services would be incomplete without the consideration of injunctions which copyright owners may obtain against platforms hosting infringing content. Under EU legislation, copyright owners 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.[88] Irrespective of the immunity against secondary liability that may follow from safe harbours for hosting, online platforms may thus be obliged to take measures against infringing use of their services. The liability question is to be distinguished from obligations resulting from an injunction. In particular, the exemption from liability for hosting does not shield an online platform against obligations to terminate or prevent an infringement.[89]

1. Impact on Cloud-Based Services

57 The potential impact of these injunctions on cloud-based services must not be underestimated. At EU level, the conceptual contours of injunctions seeking to terminate and prevent infringing use have been traced in cases concerning trademark rights. In the context of measures against trademark infringement on online marketplaces, the CJEU clarified in the L'Oréal/eBay case that it was possible

> *to order an online service provider, such as a provider making an online marketplace available to internet users, to take measures that contribute not only to bringing to an end infringements committed through that marketplace, but also to preventing further infringements....*[90]

58 While the Court pointed out that this did not imply a general and permanent prohibition on the use of goods bearing a specific trademark,[91] it did make clear that measures had to be taken against repeat infringers. The Court explained that

> *if the operator of the online marketplace does not decide, on its own initiative, to suspend the [infringer] to prevent further infringements of that kind by the same seller in respect of the same trade marks, it may be ordered, by means of an injunction, to do so.*[92]

59 Hence, a proper balance is to be found between the interest of the right owner in effectively stopping current and preventing future infringements, and the interest of online platforms in not becoming subject to a general monitoring obligation that may be too heavy a burden to continue the cloud-based service. Hence, the question of threshold requirements to be met by newcomers seeking to set up a new cloud-based service platform again becomes relevant in this context. As knowledge management obligations arising from safe harbour regimes, obligations resulting from injunctions may constitute an entrance barrier for newcomers. A heavy obligation with regard to the termination and prevention of copyright infringement is not unlikely to form a market entry requirement that newcomers without many financial resources will find difficult to meet. Too heavy a termination and prevention obligation, therefore, enhances the risk of market concentration.

2. Filtering Online Content

60 The complexity of the balancing exercise resulting from these considerations clearly comes to the fore in the debate on the filtering of online content – a debate that, in the EU, culminated in the Scarlet/*Sabam* ruling rendered by the CJEU. The background to this ruling was an initiative taken by the Belgian collecting society *Sabam* to impose an obligation on the Internet access provider Scarlet to put an end to the infringement of copyright through P2P networks. *Sabam* sought an order that would have obliged Scarlet to generally prevent its customers from sending or receiving files containing a musical work of the authors, composers and editors represented by *Sabam* if these right owners have not given their prior permission.

61 In its decision, the CJEU addressed the different interests at stake by balancing copyright protection against freedom of expression and information, the right to privacy of Internet users, and the freedom of conducting a business enjoyed by online intermediaries. On its merits, the balancing carried out by the Court can be understood as an attempt to establish a harmonious relationship between different legal positions supported by fundamental rights and freedoms.[93]

62 In the context of this complex balancing of rights and freedoms, the Court found that the broad injunction sought by *Sabam* – amounting to the establishment of a system for the general filtering of online content – encroached upon the fundamental rights and freedoms of Internet users and online intermediaries. For this reason, the Court rejected the injunction sought by SABAM:

> *Consequently, it must be held that, in adopting the injunction requiring the ISP to install the contested filtering system, the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other.*[94]

63 The ruling illustrates the outer limits of injunctions against online intermediaries: a general filtering obligation goes too far. Online intermediaries are neither obliged to embark on a systematic analysis of online data streams nor bound to collect data about users sending copyrighted content via the network. Moreover, a general filtering system is hardly capable of distinguishing adequately between unlawful and lawful content. Its introduction would inevitably affect lawful communications, such as the sending of files with permissible parodies or quotations of protected musical works, or with musical works that have already fallen into the public domain.

64 The rejection of a general filtering obligation in Scarlet/SABAM, however, leaves the question unanswered whether specific filters remain permissible, such as a filtering obligation relating to a specific music file and a specific user.[95] As discussed above, the CJEU already held in L'Oréal/eBay that measures against repeat infringers are legitimate. Against this background, it can be hypothesized that, between the two poles explored in CJEU jurisprudence – the general filtering rejected in Scarlet/*Sabam* and the specific filtering in the case of repeat infringers – there is room for configuring intermediate filtering systems that may give rise to new litigation and further attempts to balance the right to intellectual property against freedom of expression and information, the right to privacy, and freedom to conduct a business.[96]

3. Blocking of Website Access

65 A variation of the filtering theme – the blocking of access to websites hosting or facilitating the dissemination of infringing content – already led to injunctions against Internet access providers in several EU Member States.[97] These cases shed light on an important difference between access and hosting services. While the ban on general filtering systems in Scarlet/*Sabam* exempts Internet access providers from the obligation to filter all communications running through their networks, the ban did not hinder national courts from impeding access to individual hosting platforms by ordering Internet access providers to block access to these websites. While the courts are prepared to keep the burden of filtering within certain limits, there seems to be increasing willingness to order the blocking of platforms that

host infringing content or systematically facilitate copyright infringement.

66 A general court practice of granting injunctions that oblige Internet access providers to block access to online platforms, however, may finally lead to industry standards impacting the diversity of online content. Once the courts have clarified the prerequisites for the blocking of websites in several decisions, the creative industries and telecom operators may find it too burdensome to continue arguing about access control before the courts. Instead, they may return to the negotiation table to reach agreement on platforms that should be blocked.

67 This scenario gives rise to concerns about de facto censorship of online content without control through democratic institutions. The creative industries will strive for the blocking of websites that are suspected of facilitating copyright infringement. Telecom companies will seek to minimize costs and risks by reaching a widely shared standard on blocked content.[98] However, parties seeking to safeguard the openness of the Internet and diversity of online content may be absent from the negotiation table.[99] In consequence, the list of blocked websites resulting from the negotiations may become longer than any list to which courts would have agreed after a careful balancing of all fundamental rights and freedoms involved. The voice of users appreciating information diversity and pluralism on the Internet may easily be overheard in negotiations focusing on the reconciliation of industry interests.[100]

D. Conclusion

68 A survey of flexibility tools in the area of copyright law shows that breathing space for cloud-based services can be derived from

- a cautious interpretation of exclusive rights, in particular the right of adaptation and the right of communication to the public;
- copyright exceptions for quotations, parodies and private copying; and
- safe harbours that can be invoked by online platforms hosting user-generated content.

69 The availability of sufficient room for new services finally depends on the obligations coming along with these flexibility tools. A flexible private copying regime will require the payment of equitable remuneration. Broad safe harbours for hosting will be accompanied by knowledge management obligations to be fulfilled in the context of notice-and-takedown procedures. Eligibility for immunity under a safe harbour regime does not exclude obligations arising from court orders to terminate or prevent copyright infringement.

70 An examination of these influence factors leads to delicate questions about the scope of copyright protection and the limits of liability for infringement. Should the right of adaptation be understood to cover amateur remixes of protected works that are presented on an online platform, such as YouTube? Should the right of communication to the public be extended to links that are embedded in a Facebook page? Should private copying exceptions cover the use of master copies by the providers of digital lockers? Should eligibility for the safe harbour for hosting depend on a sophisticated knowledge management system capable of memorizing all information that may help to identify infringing use? Should notice-and-takedown procedures be replaced with notice-and-notice procedures? Should the filtering of online content be permissible? Should websites that facilitate copyright infringement be blocked?

71 While it is beyond the scope of the present inquiry to answer all these questions, the overview of issues surrounding cloud-based services shows that copyright is embedded in a complex matrix of competing interests. User interests may be supported by the fundamental guarantee of freedom of expression and information, and the right to privacy. The providers of cloud-based services may invoke freedom of expression and information for enabling users to receive and impart information. In the EU, the fundamental freedom to conduct a business is to be factored into the equation as well.

72 The Preamble of the Berne Convention recalls that the countries of the Berne Union are

> *equally animated by the desire to protect, in as effective and uniform a manner as possible, the rights of authors in their literary and artistic works...*

73 While this desire is not reduced in any way when it comes to the question of breathing space for cloud-based services, it follows from the analysis that in the cloud, protection 'in as effective and uniform a manner as possible' can only be achieved through a fair balancing of all rights and interests involved. In this balancing exercise, copyright represents an important value among others to be taken into account.

74 Therefore, the most effective protection of copyright in the cloud follows from a weighing process in which the goals of copyright protection – incentives for the creative industry, an appropriate reward for the creative work of individual authors – are balanced against the need to offer sufficient room for the fundamental rights and freedoms of users and providers of cloud-based services.

75 As a result of this balancing exercise, copyright will no longer be perceived as an outdated relic of the analogue past. Users and providers of cloud services will understand that copyright is an integral part of the quid pro quo governing the use of cultural productions in the cloud. In consequence, copyright protection will no longer hang by the thread of exclusive rights granted in copyright statutes – exclusive rights that seem less and less enforceable. By contrast, copyright protection will obtain the social legitimacy and societal support necessary to uphold the copyright system in the cloud environment.[101]

1 As to the difficulty of defining cloud services, see W.R. Denny, 'Survey of Recent Developments in the Law of Cloud Computing and Software as a Service Agreement', The Business Lawyer 66 (2010), p. 237 (237): '[T]here is no uniform definition of cloud computing available.'; M.H. Willow/D.J. Buller, 'Cloud Computing: Emerging Legal Issues for Access to Data, Anywhere, Anytime', Journal of Internet Law 14 (2010), p. 1 (5): '[E]xperts differ on a precise definition of "cloud computing"'. However, see also the attempts made by M.A. Melzer, 'Copyright Enforcement in the Cloud', Fordham Intellectual Property, Media and Entertainment Law Journal 21 (2011), p. 403 (404): 'Cloud computing refers to a set of approaches to diffuse computing power across more than one physical computer.'; and D.J. Gervais/D.J. Hyndman, 'Cloud Control: Copyright, Global Memes and Privacy', Journal on Telecommunications and High Technology Law 10 (2012), p. 53 (56): 'Cloud computing is a term used to describe a global technological infrastructure in which the user of a computer accesses and uses software and data located outside of the user's personal computer or other digital device. The user connects to these external devices by way of an Internet connection, but typically has no knowledge of the nature or even location of the server on which the data and software are located. This anonymous, external, and often unidentifiable interaction is known as "cloud computing" or simply "the Cloud".' See also the description given by W.H. Page, 'Microsoft and the Limits of Antitrust', Journal of Competition Law and Economics 6 (2010), p. 33 (49-50): 'Cloud computing offers virtually unlimited, on-demand computing resources. Your applications now live in a new platform – a computing cloud. In the cloud, your applications take advantage of the seemingly limitless processor cycles, memory storage, and network bandwidth along with extensive software capabilities.'

2 It is this feature of cloud-based services that challenges the exclusive rights of copyright owners. Cloud-based services allow users to access and share their own or third-party content anywhere around the globe. Cf. Melzer, supra note 1, p. 407. The result is generalized access to entire repertoires of cultural productions via a wide variety of devices with Internet functionality, ranging from personal computers to mobile phones. Cf. Gervais/Hyndman, supra note 1, p. 65.

3 This will be different in the case of copyright owners opting for a creative commons licence or another open access model. As to the debate on creative commons, cf. N. Elkin-Koren, 'Exploring Creative Commons: A Skeptical View of a Worthy Pursuit', L.M.C.R. Guibault/P.B. Hugenholtz (eds.), The Future of the Public Domain – Identifying the Commons in Information Law, The Hague/London/New York: Kluwer Law International 2006, p. 325. With regard to the specific problem of share-alike obligations, see T. Gue, 'Triggering Infection: Distribution and Derivative Works Under the GNU General Public Licence', Journal of Law, Technology and Policy 2012/1, p. 95.

4 As to these rationales of copyright protection, see A. Strowel, Droit d'auteur and Copyright: Between History and Nature, in: B. Sherman/A. Strowel, Of Authors and Origins, Oxford: Clarendon Press 1994, p. 235 (241-251); P.E. Geller, Must Copyright Be For Ever Caught Between Marketplace and Authorship Norms?, in: B. Sherman/A. Strowel, ibid., p. 159 (170); S.P. Calandrillo, An Economic Analysis of Property Rights in Information: Justifications and Problems of Exclusive Rights, Incentives to Generate Information, and the Alternative of a Government-Run Reward System, Fordham Intellectual Property Media and Entertainment Law Journal 9 (1998), p. 301 (310).

5 Cf. M.A. Lemley, 'Rationalizing Internet Safe Harbors', Journal on Telecommunications and High Technology Law 6 (2007), p. 101 (112). For an overview of jurisprudence on secondary liability of platform providers and the central role of safe harbours in the creation of the legal certainty necessary for innovation in the area of online platforms and services, see Melzer, supra note 1, p. 423-439.

6 As to 'consumer-participants', see N. Elkin-Koren, 'Making Room for Consumers Under the DMCA', Berkeley Technology Law Journal 22 (2007), p. 1119 (1138); C. Soliman, 'Remixing Sharing: Sharing Platforms as a Tool for Advancement of UGC Sharing', Albany Law Journal of Science and Technology 22 (2012), p. 279 (280-293); G. Mazziotti, EU Digital Copyright Law and the End-User, Berlin/Heidelberg: Springer 2008; L. Leung, 'User-generated content on the internet: an examination of gratifications, civic engagement and psychological empowerment', New Media and Society 11 No. 8 (2009), p. 1327; T. Daugherty/M.S. Eastin/L. Bright, 'Exploring Consumer Motivations for Creating User-Generated Content', Journal of Interactive Advertising 8 No. 2 (2008), p. 16.

7 As to this aspect of the freedom to receive and impart information guaranteed in Article 10 of the European Convention on Human Rights, see European Court of Human Rights, 22 May 1990, application no. 12726/87, Autronic/Switzerland, para. 47: 'Furthermore, Article 10 applies not only to the content of information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information.' Cf. C. Geiger, Droit d'auteur et droit du public à l'information, Paris: Litec 2004, p. 134-136; N.W. Netanel, 'Copyright and a Democratic Civil Society', Yale Law Journal 106 (1996), p. 283.

8 This has been highlighted, for instance, in OECD, 'Participative Web: User-Created Content', document DSTI/ICCP/IE(2006)7/ Final, dated 12 April 2007, available online at <http://www.oecd.org/internet/ieconomy/ 38393115.pdf>. For an approach based on legal theory, see C. Geiger, 'Die Schranken des Urheberrechts als Instrumente der Innovationsförderung – Freie Gedanken zur Ausschließlichkeit im Urheberrecht', Gewerblicher Rechtsschutz und Urheberrecht – Internationaler Teil 2008, p. 459.

9 For instance, see the consultation in the UK, HM Government, Modernising Copyright: A Modern, Robust and Flexible Framework, final government response dated 20 December 2012, available at <http://www.ipo.gov.uk/ response-2011-copyright-final.pdf>, pp. 8-10.

10 Canada is an exception to this rule. Under the new Article 29.21 of the Copyright Act of Canada, as introduced by Bill C-11, 'Copyright Modernization Act', adopted on 18 June 2012, non-commercial user-generated content that is based on copyrighted material does not amount to infringement. As to the general debate on user-generated content, see S.D. Jamar, 'Crafting Copyright Law to Encourage and Protect User-Generated Content in the Internet Social Networking Context', Widener Law Journal 19 (2010), p. 843; M. Knopp, 'Fanfiction – nutzergenerierte Inhalte und das Urheberrecht', Gewerblicher Rechtsschutz und Urheberrecht 2010, p. 28; N. Helberger/L. Guibault/E.H. Janssen/N.A.N.M. Van Eijk/C. Angelopoulos/ J.V.J. Van Hoboken, Legal Aspects of User Created Content,

Amsterdam: Institute for Information Law 2009, available at <http://ssrn.com/ abstract=1499333>; E. Lee, 'Warming Up to User-Generated Content', University of Illinois Law Review 2008, p. 1459; B. Buckley, 'SueTube: Web 2.0 and Copyright Infringement', Columbia Journal of Law and the Arts 31 (2008), p. 235; T.W. Bell, 'The Specter of Copyism v. Blockheaded Authors: How User-Generated Content Affects Copyright Policy', Vanderbilt Journal of Entertainment and Technology Law 10 (2008), p. 841; S. Hechter, 'User-Generated Content and the Future of Copyright: Part One – Investiture of Ownership', Vanderbilt Journal of Entertainment and Technology Law 10 (2008), p. 863; G. Lastowka, 'User-Generated Content and Virtual Worlds', Vanderbilt Journal of Entertainment and Technology Law 10 (2008), p. 893.

11 The international right of quotation set forth in Article 10(1) BC has been implemented in the EU in Article 5(3)(d) EU Information Society Directive 2001/29. For an example of the evolution of a flexible quotation right under this standard, see M.R.F. Senftleben, 'Quotations, Parody and Fair Use', in: P.B. Hugenholtz/A.A. Quaedvlieg/D.J.G. Visser (eds.), A Century of Dutch Copyright Law – Auteurswet 1912-2012, Amstelveen: deLex 2012, p. 359, available online at <http://ssrn.com/ abstract= 2125021>. With regard to the current debate on the consistency of this broadening of the quotation right, see M. de Zwaan, 'Ruimte in het citaatrecht in Europa? Zoekmachine vindt niets bij "search naar flexibilities"', Tijdschrift voor auteurs-, media- en informatierecht 2012, p. 141.

12 See Article 5(3)(k) EU Information Society Directive 2001/29. As to the question whether parody can be qualified as a specific kind of quotation that may be covered by Article 10(1) BC, see A.A. Quaedvlieg, 'De parodiërende nabootsing als een bijzondere vorm van geoorloofd citaat', RM Themis 1987, p. 279.

13 Cf. P.N. Leval, 'Toward a Fair Use Standard', Harvard Law Review 103 (1990), p. 1105 (1111); N.W. Netanel, 'Copyright and a Democratic Civil Society', Yale Law Journal 106 (1996), p. 283 (381). As to the application of the fair use doctrine in practice, see M. Sag, 'Predicting Fair Use', Ohio State Law Journal 73 (2012), p. 47, available online at <http://ssrn.com/abstract=1769130>; P. Samuelson, 'Unbundling Fair Uses', 77 Fordham Law Review 2537 (2009); B. Beebe, 'An Empirical Study of U.S. Copyright Fair Use Opinions, 1978-2005', University of Pennsylvania Law Review 156 (2008), p. 549.

14 Supreme Court of the United States of America, 7 March 1994, 510 U.S. 569 (Campbell v Acuff-Rose), section A. The case concerned a rap version of Roy Orbison's and William Dees' song 'Oh, Pretty Woman' which the rap group 2 Live Crew had composed to satirize the intact world built up in the original.

15 Leval, supra note 28, p. 1111.

16 Cf. A. Schwabach, 'The Harry Potter Lexicon and the World of Fandom: Fan Fiction, Outsider Works, and Copyright', University of Pittsburgh Law Review 70 (2009), available at <http://ssrn.com/abstract=1274293>; M.W.S. Wong, 'Transformative User-Generated Content in Copyright Law: Infringing Derivative Works or Fair Use?', Vanderbilt Journal of Entertainment and Technology Law 11 (2009), p. 1075 (1124-1130).

17 See <http://www.hp-lexicon.org/>.

18 United States District Court Southern District of New York, 8 September 2008, Warner Bros. and J.K. Rowling v RDR Books, 07 Civ. 9667 (RPP). Cf. the case comment by A.J. Sanders, European Intellectual Property Review 2009, p. 45.

19 Article 13 Dutch Copyright Act.

20 In fact, the central test applied in this context is not whether the adaptation constitutes a creation satisfying the originality test. As pointed out by J.H. Spoor, 'Verveelvoudigen: Reproduction and Adaptation under the 1912 Copyright Act', in: P.B. Hugenholtz/A.A. Quaedvlieg/D.J.G. Visser (eds.), A Century of Dutch Copyright Law – Auteurswet 1912-2012, Amstelveen: deLex 2012, p. 197 (206-212), courts in the Netherlands are not unlikely to ask whether the allegedly infringing work presents the original features of the earlier work to such an extent that the overall impressions given by both works differ insufficiently to consider the former an independent work.

21 § 24 German Copyright Act. For an overview of German case law, see G. Schulze, in: T. Dreier/G. Schulze, Urheberrechtsgesetz – Kommentar, 4th ed., Munich: C.H. Beck 2013.

22 § 5(2) Austrian Copyright Act.

23 For instance, see Austrian Supreme Court, 13 July 2010, case 4 Ob 66/10z, 'Lieblingshauptfrau'; German Federal Court of Justice, 20 March 2003, case I ZR 117/00, 'Gies-Adler'; Dutch Supreme Court, 13 April 1984, case LJN: AG4791, 'Suske en Wiske', Nederlandse Jurisprudentie 1984, no. 524. For a discussion of this free adaptation principle against the background of international obligations, see Senftleben, supra note 11, p. 374-381; P.E. Geller, 'A German Approach to Fair Use: Test Cases for TRIPs Criteria for Copyright Limitations?', Journal of the Copyright Society of the U.S.A. 57 (2010), p. 901.

24 See the overview provided by P.E. Geller, 'A German Approach to Fair Use: Test Cases for TRIPs Criteria for Copyright Limitations?', Journal of the Copyright Society of the U.S.A. 57 (2010), p. 901; F.W. Grosheide, 'De grondslagen van de parodie-exceptie', in: F.W. Grosheide (ed.), Parodie – parodie en kunstcitaat, The Hague: Boom Juridische uitgevers 2006, p. 1 (19-25); H.E. Ruijsenaars, 'Een onoverwinnelijke Galliër? Enkele opmerkingen t.a.v. de parodie op stripfiguren', Informatierecht/AMI 1993, p. 143 (149).

25 See G. Schulze, in: Th. Dreier, G. Schulze, Urheberrechtsgesetz – Kommentar, 4th ed., Munich: C.H. Beck 2013, commentary on § 24.

26 For a similar approach seeking to create 'a space for noncommercial flow', see D. Halbert, 'Mass Culture and the Culture of the Masses: A Manifesto for User-Generated Rights', Vanderbilt Journal of Entertainment and Technology Law 11 (2009), p. 921 (955-959). Cf. also R. Tushnet, 'Copy this Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It', Yale Law Journal 114 (2004), p. 535 (552), pointing out that creative use of protected works typically involves 'both copying and reworking'.

27 German Federal Court of Justice, 1 December 2010, case I ZR 12/08 (Perlentaucher), Gewerblicher Rechtsschutz und Urheberrecht 2011, p. 134 (137-138), available online at <www.bundesgerichtshof.de>.

28 Cf. German Federal Court of Justice, 20 November 2008, case I ZR 112/06 (Metall auf Metall), Gewerblicher Rechtsschutz und Urheberrecht 2009, p. 403, available online at <www.bundesgerichtshof.de>; F.J. Dougherty, 'RIP, MIX and BURN: Bemerkungen zu aktuellen Entwicklungen im Bereich des digitalen Sampling nach US-amerikanischem und internationalen Recht', Gewerblicher Rechtsschutz und Urheberrecht – Internationaler Teil 2007, p. 481. With regard to the sound sampling debate in the US, see D.M. Morrison, 'Bridgeport Redux: Digital Sampling and Audience Recording', Fordham Intellectual Property, Media and Entertainment Law Journal 19 (2008), p. 75.

29 For an overview of these issues, see D.J.G. Visser, 'Het "embedden" van een YouTube filmpje op en Hyves-pagina', Mediaforum 2010, p. 12; S. Ott, 'Haftung für Embedded Videos von YouTube und anderen Videoplattformen im Internet', Zeitschrift für Urheber- und Medienrecht 2008, p. 556.

30 In this sense, District Court of The Hague, 19 December 2012, case 407402/HA ZA 11-2675, Buma v Nederland.FM, available at <www.ie-forum.nl>, para. 4.5. As to a potential parallel with the use of broadcasts in hotels and restaurants, see Article 11bis(1)(ii) and (iii) BC. With regard to the situation in the EU, see CJEU, 7 December 2006, case C-306/05, SGAE v Rafael Hoteles, finding that the further distribution of broadcasting signals in hotels aims at a new public; and CJEU, 15 March 2012, case C-135/10, SCF v Marco Del Corso, para. 86 and 96, esta-

blishing a de minimis threshold for the assumption of a new public that is not met in the case of a dentist's waiting room.

31 Cf. A. Strowel/N. Ide, 'Liability with Regard to Hyperlinks', Columbia Journal of Law and the Arts 24 (2001), p. 403 (425).

32 As to the difficulty of distinguishing between different audiences and the risk of the notion of a (new) 'public' becoming too vague and unreliable, see J.H. Spoor, 'Hooggeschat Publiek', Tijdschrift voor auteurs-, media- en informatierecht 2007, p. 141.

33 Even if a certain risk of confusion cannot be ruled out, this need not exclude a ruling in favour of the user who embeds content. See US Court of Appeals for the Ninth Circuit, 16 May 2007, Perfect 10, Inc. v Google Inc., Fd 3d. 701 (USCA, 9th Cir. 2007), para. 7: 'While in-line linking and framing may cause some computer users to believe they are viewing a single Google webpage, the Copyright Act, unlike the Trademark Act, does not protect a copyright holder against acts that cause consumer confusion.' Measures to prevent confusion about the origin of the embedded content, however, may support a finding that the 'framing' does not amount to copyright infringement. See Austrian Supreme Court, 17 December 2002, case 4Ob248/02b, METEO-data, p. 4.

34 German Federal Court of Justice, 17 July 2003, case I ZR 259/00, Paperboy, available at <www.bundesgerichtshof.de>, p. 25. The decision is published in Gewerblicher Rechtsschutz und Urheberrecht 2003, p. 958. As to the impact of the decision on the regulation of online information flows, cf. T. Hoeren, 'Keine wettbewerbsrechtliche Bedenken mehr gegen Hyperlinks? Anmerkung zum BGH-Urteil "Paperboy"', Gewerblicher Rechtsschutz und Urheberrecht 2004, p. 1; G. Nolte, 'Paperboy oder die Kunst den Informationsfluss zu regulieren', Zeitschrift für Urheber- und Medienrecht 2003, p. 540.

35 For instance, see J. Litman, Digital Copyright: Revising Copyright Law for the Information Age, New York: Prometheus Books 2001, p. 183, who draws a line between hyperlinks and traditional footnotes.

36 German Federal Court of Justice, ibid., p. 20 (para. 42).

37 German Federal Court of Justice, ibid., p. 20 (para. 42).

38 Austrian Supreme Court, 20 September 2011, case 4Ob105/11m, Vorschaubilder, p. 22-23.

39 In this sense also L. Bently et al., 'The Reference to the CJEU in Case C-466/12 Svensson', University of Cambridge Legal Studies Research Paper No. 6/2013, available at <http://ssrn.com/abstract=2220326>, pp. 13-14. However, see S. Ott, 'Die urheberrechtliche Zulässigkeit des Framing nach der BGH-Entscheidung im Fall "Paperboy"', Zeitschrift für Urheber- und Medienrecht 2004, p. 357 (362-365); 'Haftung für verlinkte urheberrechtswidrige Inhalte in Deutschland, Österreich und den USA', Gewerblicher Rechtsschutz und Urheberrecht – International Teil 2007, p. 14, who agrees that the universal Paperboy criteria developed with regard to deep links seem equally valid with regard to framing and in-line linking. Pointing to differences in the presentation of 'framed' links, however, he proposes assuming a relevant act of communication to the public.

40 US Court of Appeals for the Second Circuit, 4 August 2008, 536 F.3d 121 (2d Cir. N.Y. 2008), Cartoon Network LLP/CSC Holding, Inc., p. 26, at 11-16.

41 US Court of Appeals for the Second Circuit, ibid., p. 43, at 11-16.

42 German Federal Court of Justice, 22 April 2009, case I ZR 216/06, Internet-Videorecorder, published in Gewerblicher Rechtsschutz und Urheberrecht 2009, p. 845, para. 23 and 26.

43 German Federal Court of Justice, ibid., para. 33 and 35.

44 In fact, the Court of Appeals of Dresden, 12 June 2011, 'Shift.TV', published in Zeitschrift für Urheber- und Medienrecht 2011, p. 913, to which the case had been remanded, finally found an infringement of the retransmission right.

45 Supreme Court of Japan, 20 January 2011, 65-1 Minshû 399, Rokuraku II. Cf. the discussion of the case by T. Ueno, 'The making available right in the 'cloud' environment', elsewhere in this book.

46 For a detailed discussion of private copying, see G. Hohagen, Die Freiheit der Vervielfältigung zum privaten Gebrauch, München: C.H. Beck 2004. As to the debate on private copying in the digital environment, see C. Geiger, 'The Answer to the Machine Should not be the Machine: Safeguarding the Private Copy Exception in the Digital Environment', European Intellectual Property Review 2008, p. 121.

47 For instance, see the decision of the US Supreme Court in Sony Corporation of America v Universal City Studios, Inc., 464 US 417 (1984), IV B. Cf. W.J. Gordon, 'Fair Use as Market Failure: A Structural and Economic Analysis of the Betamax Case and its Predecessors', Columbia Law Review 82 (1982), p. 1600.

48 For a description of the flexible Dutch private copying regime as an example of a broad continental European private copying system, see D.J.G. Visser, 'Private Copying', in: P.B. Hugenholtz/A.A. Quaedvlieg/D.J.G. Visser (eds.), A Century of Dutch Copyright Law – Auteurswet 1912-2012, Amstelveen: deLex 2012, p. 413. For a comparison between continental European and Anglo-American private copying systems, see J.N. Ullrich, 'Clash of Copyrights – Optionale Schranke und zwingender finanzieller Ausgleich im Fall der Privatkopie nach Art. 5 Abs. 2 lit. B) Richtlinie 2001/29/EG und Dreistufentest', Gewerblicher Rechtsschutz und Urheberrecht – Internationaler Teil 2009, p. 283 (286-290).

49 An affirmative answer to this question has been given by the Dutch legislator in the framework of the implementation of the EU Information Society Directive 2001/29 into Dutch law. For a discussion of this position in the light of the three-step test, see M.R.F. Senftleben, 'Tegengif of overdosis? Over rechtszekerheid bij privé-kopiëren uit illegale bron', Tijdschrift voor Auteurs-, Media- & Informatierecht 2011, p. 153. In the meantime, this standpoint has led to prejudicial questions to the CJEU. See Dutch Supreme Court, 21 September 2012, case LJN BW5879, ACI/Thuiskopie, available at <www.rechtspraak.nl>.

50 This question is relevant, for instance, under the German regulation of private copying. The private copying privilege does not apply in case an 'evidently unlawful source' is used. Cf. K. Fangerow/D. Schulz, 'Die Nutzung von Angeboten auf www.kino.to – Eine urheberrechtliche Analyse des Film-Streamings im Internet', Gewerblicher Rechtsschutz und Urheberrecht 2010, p. 677 (679-680); T. Reinbacher, 'Strafbarkeit der Privatkopie von offensichtlich rechtswidrig hergestellten oder öffentlich zugänglich gemachten Vorlagen', Gewerblicher Rechtsschutz und Urheberrecht 2008, p. 394.

51 For a more detailed discussion of this point, see M.R.F. Senftleben, Copyright, Limitations and the Three-Step Test – An Analysis of the Three-Step Test in International and EC Copyright Law, The Hague/London/New York: Kluwer Law International 2004, p. 235-241.

52 See Report on the Work of Main Committee I, Records of the Intellectual Property Conference of Stockholm June 11 to July 14, 1967, Geneva: WIPO 1971, p. 1145-1146.

53 CJEU, 21 October 2010, case C-467/08, Padawan/SGAE, para. 42.

54 CJEU, ibid., para. 56.

55 CJEU, ibid., para. 53.

56 See the questions asked in case C-457/11, VG Wort/Kyocera Mita (German Federal Court of Justice; Opinion AG Sharpston, 24 January 2013); case C-521/11, Amazon.com (Austrian Supreme Court; Opinion AG Mengozzi, 7 March 2013); case C-435/12, ACI/Thuiskopie (Dutch Supreme Court); case C-463/12, Copydan/Nokia (Danish Supreme Court), available at <www.curia.eu>.

57 See the description of difficulties that have arisen in different EU Member States by T. Dreier, 'Living with Copyright from Luxembourg', Tijdschrift voor auteurs-, media- en informatierecht 2012, p. 243 (Germany); S. Dussollier, 'De invloed van de Padawan-uitspraak op het ongelijke veld van thuiskopieheffingen in België', ibid., p. 247 (Belgium); V. Still, 'Is the Copyright Levy System Becoming Obsolete?', ibid., p. 250 (Finland); R. Xalabarder, 'The Abolishment of Copyright Levies in Spain', ibid., p. 259 (Spain).

58 For a discussion of several problem areas, see M. Bisges, 'Beeinträchtigung des Systems der Urhebervergütung für Privatkopien durch Cloud-Dienste', Gewerblicher Rechtsschutz und Urheberrecht 2013, p. 146.

59 This follows at least from decisions taken with regard to the analogue environment. In CJEU, 15 March 2012, case C-162/10, Phonographic Performance (Ireland)/Ireland, para. 69, the CJEU held for instance, 'that a hotel operator which provides in guest bedrooms [...] other apparatus and phonograms in physical or digital form which may be played on or heard from such apparatus, is a "user" making a "communication to the public" of a phonogram within the meaning of Article 8(2) of Directive 2006/115/EC.' This ruling may indicate that the Court is prepared to also hold that use of master copies by the provider of digital lockers amounts to an infringing act of communication to the public. For a discussion of the situation in the US, see M. Rasenberger/ C. Pepe, 'Copyright Enforcement and Online File Hosting Services: Have Courts Struck the Proper Balance?', Journal of the Copyright Society of the U.S.A. 59 (2012), p. 501 (512-517).

60 Article 5(1) Information Society Directive 2001/29/EC.

61 CJEU, 16 July 2009, case C-5/08, Infopaq International/Danske Dagblades Forening, para. 56-57.

62 CJEU, ibid., para. 58.

63 CJEU, 4 October 2011, cases C-403/08 and C-429/08, Football Association Premier League/QC Leisure, para. 162-163.

64 CJEU, ibid., para. 164.

65 Article 5(5) Information Society Directive 2001/29/EC. See CJEU, ibid., para. 181.

66 National court decisions in EU Member States show that, in practice, the dogma of strict interpretation may be applied flexibly. In a 2002 decision concerning the scanning and storing of press articles for internal e-mail communication in a private company, the German Federal Court of Justice, for instance, held that digital press reviews had to be deemed permissible just like their analogue counterparts, if the digital version – in terms of its functioning and potential for use – essentially corresponded to traditional analogue products. The Court noted in this context that the evolution of new technologies required a flexible interpretation of exceptions. See German Federal Court of Justice, 11 July 2002, case I ZR 255/00, Gewerblicher Rechtsschutz und Urheberrecht 2002, p. 963. See case comment T. Dreier, Juristenzeitung 2003, p. 473; T. Hoeren, 'Pressespiegel und das Urheberrecht', Gewerblicher Rechtsschutz und Urheberrecht 2002, p. 1022

67 CJEU, 1 December 2011, case C-145/10 (Eva Maria Painer v Standard VerlagsGmbH), para. 132-133.

68 Article 5(3)(d) Information Society Directive 2001/29/EC.

69 CJEU, ibid., para. 134.

70 This scenario raises the further question whether it makes sense to insist on the grant of exclusive rights allowing the exclusion of users from the enjoyment of cultural productions. From a practical perspective, enhanced (collective) licensing and remuneration schemes may offer comparable revenues while not restricting access to protected works. Cf. Gervais/ Hyndman, supra note 1, p. 76: 'Cultural industries that will do well in the Cloud will be Sherpas, not park rangers. Intellectual property rules make this possible, but the solution is licensing and more access, and enforcement limited to professional pirates.'

71 CJEU, 3 July 2012, case C-128/11 (UsedSoft v Oracle), para. 47. Cf. the case comments by M. Stieper, Zeitschrift für Urheber- und Medienrecht 2012, p. 668; M.R.F. Senftleben, 'Die Fortschreibung des urheberrechtlichen Erschöpfungsgrundsatzes im digitalen Umfeld', Neue Juristische Wochenschrift 2012, p. 2924; F.W. Grosheide, 'Een revolutie in het EU-auteursrecht? Enkele kanttekeningen bij het UsedSoft vs Oracle-arrest', Tijdschrift voor auteurs-, media- en informatierecht 2013/2 (forthcoming).

72 Cf. Melzer, supra note 1; Lemley, supra note 5. As to the remaining liability risk under different national systems, see T. Hoeren/S. Yankova, 'The Liability of Internet Intermediaries: The German Perspective', International Review of Intellectual Property and Competition Law 43 (2012), p. 501; C. Alberdingk Thijm, 'Wat is de zorgplicht van Hyves, XS4All en Marktplaats?', Ars Aequi 2008, p. 573. For a broad discussion of potential obligations of platform providers and a sophisticated differentiation of warning, monitoring, control and prevention obligations on the basis of active or neutral involvement, see M. Leistner, 'Von 'Grundig-Reporter(n) zu Paperboy(s)' Entwicklungsperspektiven der Verantwortlichkeit im Urheberrecht', Gewerblicher Rechtsschutz und Urheberrecht 2006, p. 801.

73 For a comparative analysis of this horizontal safe harbour approach with the specific copyright safe harbour regime in the US, see M. Peguera, 'The DMCA Safe Harbour and Their European Counterparts: A Comparative Analysis of Some Common Problems', Columbia Journal of Law and the Arts 32 (2009), p. 481; H. Travis, 'Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law', Notre Dame Law Review 84 (2008), p. 331; and against the background of French case law J.C. Ginsburg, 'Separating the Sony Sheep From the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs', Arizona Law Review 50 (2008), p. 577 (590-608).

74 With regard to the development of jurisprudence concerning keyword advertising in the EU, cf. M.R.F. Senftleben, 'Adapting EU Trademark Law to New Technologies – Back to Basics?', in: C. Geiger (red.), Constructing European Intellectual Property, Cheltenham: Edward Elgar 2013, p. 176, available at <http://ssrn.com/abstract=1875629>; A. Ohly, 'Keyword Advertising auf dem Weg zurück von Luxemburg nach Paris, Wien, Karlsruhe und Den Haag', Gewerblicher Rechtsschutz und Urheberrecht 2010, p. 776; J. Cornthwaite, 'AdWords or Bad Words? A UK Perspective on Keywords and Trade Mark Infringement', European Intellectual Property Review 2009, p. 347; R. Knaak, 'Keyword Advertising – Das aktuelle Key-Thema des Europäischen Markenrechts', Gewerblicher Rechtsschutz und Urheberrecht International 2009, p. 551; C. Well-Szönyi, 'Adwords: Die Kontroverse um die Zulässigkeit der Verwendung fremder Marken als Schlüsselwort in der französischen Rechtsprechung', Gewerblicher Rechtsschutz und Urheberrecht International 2009, p. 557; G. Engels, 'Keyword Advertising – Zwischen beschreibender, unsichtbarer und missbräuchlicher Verwendung', Markenrecht 2009, p. 289; M. Schubert/S. Ott, 'AdWords – Schutz für die Werbefunktion einer Marke?', Markenrecht 2009, 338; O. Sosnitza, 'Adwords = Metatags? Zur marken- und wettbewerbsrechtlichen Zulässigkeit des Keyword Advertising über Suchmaschinen', Markenrecht 2009, p. 35; Ch. Gielen, 'Van adwords en metatags', in: N.A.N.M. van Eijk et al. (eds.), Dommering-bundel, Amsterdam: Cramwinckel 2008, p. 101; O. van Daalen/A. Groen, 'Beïnvloeding van zoekresultaten en gesponsorde koppelingen. De juridische kwalificatie van onzichtbaar merkgebruik', BMM Bulletin 2006, p. 106.

75 CJEU, 23 March 2010, cases C-236/08-238/08, Google France and Google/Louis Vuitton et al., para. 114. The Court also held

that the search engine offering a keyword advertising service did not use affected trademarks in the sense of trademark law. Direct liability arising from keyword advertising services thus seems to be excluded in the EU. See CJEU, ibid., para. 57. As to the debate on potential direct liability and primary infringement, see, however, G.B. Dinwoodie/M.D. Janis, 'Lessons From the Trademark Use Debate', Iowa Law Review 92 (2007), p. 1703 (1717), pointing out in the light of developments in the US that 'the sale of keyword-triggered advertising and the manner of presentation of search results potentially create independent trademark-related harm, thus making it an appropriate subject of direct liability'.

76 CJEU, ibid., para. 116-118. As to the discussion on 'financial benefit directly attributable to the infringement' in the US, see B. Brown, 'Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World', Berkeley Technology Law Journal 23 (2008), p. 437 (445-453).

77 CJEU, 12 July 2011, case C-324/09, L'Oréal/eBay, para. 120.

78 CJEU, ibid., para. 122. The notion of 'diligent economic operator' recalls the test whether 'a reasonable person operating under the same or similar circumstances' would find that infringing activity was apparent. This latter test was proposed in the legislative history of the safe harbour provisions in the US to determine whether an intermediary was aware of facts or circumstances from which infringing activity is apparent. Cf. Brown, supra note 76, p. 455-458; Rasenberger/Pepe, supra note 59, p. 555-560.

79 National approaches to this knowledge management requirement differ from country to country and between the courts. See the overview provided by R. Matulionyte/S. Nerisson, 'The French Route to an ISP Safe Harbour, Compared to German and US Ways', International Review of Intellectual Property and Competition Law 42 (2011), p. 55. For a far-reaching obligation to manage infringing links, including searches for comparable links and additional measures with regard to the affected work, see Court of Appeals Hamburg, 14 March 2012, case 5 U 87/09, Rapidshare II.

80 This risk is emphasised by Lemley, supra note 5, p. 112. For an example of how unclear liability rules may strengthen the market position of big enterprises via-à-vis small competitors, see B. Leary, 'Safe Harbor Startups: Liability Rulemaking Under the DMCA', New York University Law Review 87 (2012), p. 1134 (1167-1169), who discusses Apple's iCloud service that is based on the scanning of a user's computer to identify song files and the subsequent granting of streaming and downloading access to Apple's own copies of those songs.

81 However, it is to be noted that at least with regard to personal storage space in digital lockers in the cloud, this quid pro quo underlying present safe harbour regimes is unlikely to work. As content in personal digital lockers is not publicly available, there is no possibility for copyright owners to monitor this content and use the notice-and-takedown system to put an end to infringement. This problem is pointed out by Leary, supra note 79, p. 1160, who proposes to 'modify the DMCA to extend liability immunity only to user-content service providers who comply with safe harbor rulemaking and would delegate power to the Librarian of Congress, with the advice of the Copyright Office, to issue periodic rules approving and requiring the implementation of specific anti-infringement measures – substitutes for notice and takedown'. While this proposal relies on the regulation of anti-infringement measures, a more generous private copying regime generating revenue streams through levy systems may be a further solution – at least in countries that already provide for flexible private copying regimes, such as many EU Member States.

82 Section 512(g)(1) of the US Copyright Act provides that, if the user who had posted content that has later been taken down serves a counter-notice accompanied by a statement under penalty of perjury that the content was removed or disabled through mistake or misidentification, the intermediary must put back the material within 10 to 14 days unless the copyright owner seeks a court order against the user. As to the practical importance of this counter-notice system – for instance, with regard to fair use privileges – see I. Chuang, 'Be Wary of Adding Your Own Soundtrack: Lenz v. Universal and How the Fair Use Policy Should be Applied to User Generated Content', Loyola of Los Angeles Entertainment Law Review 29 (2009), p. 164 (165-166); M.S. Sawyer, 'Filters, Fair Use & Feedback: User-Generated Content Principles and the DMCA', Berkeley Technology Law Journal 24 (2009), p. 363 (391).

83 See W. Seltzer, 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment', Harvard Journal of Law and Technology 24 (2010), p. 171 (177-179); J.M. Urban/L. Quilter, 'Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act', Santa Clara Computer and High Technology Law Journal 22 (2006), p. 621, showing, among other things, that 30% of DMCA takedown notices were legally dubious, and that 57% of DMCA notices were filed against competitors. Even though the DMCA offers the opportunity to file counter-notices and rebut unjustified takedown requests, Urban and Quilter find that instances in which this mechanism is used are relatively rare. However, cf. also the critical comments on the methodology used for the study and a potential self-selection bias arising from the way in which the analysed notices have been collected by F.W. Mostert/M.B. Schwimmer, 'Notice and Takedown for Trademarks', Trademark Reporter 101 (2011), p. 249 (259-260).

84 See new Articles 41.25 and 41.26 of the Copyright Act of Canada, as introduced by Bill C-11, 'Copyright Modernization Act', adopted on 18 June 2012. Under the new Article 41.26(1)(a), an online intermediary receiving a notification about infringing content must 'as soon as feasible forward the notice electronically to the person to whom the electronic location identified by the location data specified in the notice belongs and inform the claimant of its forwarding or, if applicable, of the reason why it was not possible to forward it'.

85 A reform of safe harbour provisions is also discussed in the US. For the results of a working group of twenty copyright scholars and practitioners seeking to develop a model for modifying the DMCA safe harbours, see P. Samuelson, 'The Copyright Principles Project: Directions for Reform', Berkeley Technology Law Journal 25 (2010), p. 1175 (1217), proposing the creation of a fifth safe harbour for service providers applying 'reasonable, effective, and commercially available' technology for deterring infringement.

86 Article 14(1)(b) of the E-commerce Directive 2000/31/EC. The rudimentary harmonization in the Directive, however, seems to leave room for more sophisticated systems at the national level. In France, for instance, a statutory notification procedure has been introduced that, among other things, requires correspondence with the author or editor of allegedly infringing content. Cf. Peguera, supra note 66, p. 490-491.

87 Further information on this initiative, the public consultation and relevant background documents are available at <http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm>.

88 Article 8(3) Information Society Directive 2001/29/EC; Article 11 Enforcement Directive 2004/48/EC.

89 Article 14(3) E-commerce Directive 2000/31/EC.

90 CJEU, 12 July 2011, case C-324/09, L'Oréal/eBay, para. 131.

91 CJEU, ibid., para. 140.

92 CJEU, ibid., para. 141.

93 CJEU, 24 November 2011, case C-70/10, para. 49-50. With regard to the foundations of these legal positions, see Article 17, and particularly 17(2) EU Charter of Fundamental Rights, on the one hand, and Articles 8, 11 and 16 of the Charter on

the other. As to the explicit recognition of intellectual property in Article 17(2) of the Charter, see C. Geiger, 'Intellectual Property Shall be Protected!? Article 17(2) of the Charter of Fundamental Rights of the European Union: A Mysterious Provision with an Unclear Scope', European Intellectual Property Review 2009, p. 113. As to the influence of freedom of speech guarantees on copyright, cf. C. Geiger, '"Constitutionalising" Intellectual Property Law? The Influence of Fundamental Rights on Intellectual Property in the European Union', International Review of Intellectual Property and Competition Law 37 (2006), p. 371; A. Strowel/F. Tulkens/D. Voorhoof (eds.), Droit d'auteur et liberté d'expression, Brussels: Editions Larcier 2006; P.B. Hugenholtz, 'Copyright and Freedom of Expression in Europe', in: N. Elkin-Koren/N.W. Netanel (eds.), The Commodification of Information, The Hague/London/Boston: Kluwer 2002, p. 239; Th. Dreier, 'Balancing Proprietary and Public Domain Interests: Inside or Outside of Proprietary Rights?', in: R. Dreyfuss/D. Leenheer-Zimmerman/H. First (eds.), Expanding the Boundaries of Intellectual Property. Innovation Policy for the Knowledge Economy, Oxford: Oxford University Press 2001, p. 295; S. Macciacchini, Urheberrecht und Meinungsfreiheit, Bern: Stämpfli 2000; Y. Benkler, 'Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain', New York University Law Review 74 (1999), p. 355; N.W. Netanel, 'Copyright and a Democratic Civil Society', Yale Law Journal 106 (1996), p. 283. The impact of the guarantee of freedom to conduct a business has not yet been explored in literature to a comparable degree.

94 CJEU, ibid., para. 53.

95 Cf. J. Reus, 'De bescherming van IE-rechten op platforms voor user-generated content', Intellectuele eigendom en reclamerecht 2012, p. 413; E.J. Dommering, 'De zaak Scarlet/*Sabam* – Naar een horizontale integratie van het auteursrecht', Tijdschrift voor auteurs-, media en informatierecht 2012, p. 49. As to general shortcomings of filtering technology in terms of adequate evidence, regard for copyright exceptions and limitations, and sufficient safeguards for a due process, see S.K. Katyal/J.M. Schultz, 'The Unending Search for the Optimal Infringement Filter', Columbia Law Review Sidebar 112 (2012), p. 83 (89, 96 and 102).

96 For instance, see Court of Appeals of Leeuwarden, 22 May 2012, case LJN: BW6296, Stokke/Marktplaats, available at <www.rechtspraak.nl>, where the Court sees room for filtering on the basis of specific criteria, such as a particular text (para. 8.2), but arrives at the conclusion that this would be disproportionate in light of the impediment of the free movement of goods (para. 8.9-8.10). Text filters have also been rejected by Court of Appeals Hamburg, 14 March 2012, case 5 U 87/09, Rapidshare II.

97 For instance, see District Court of The Hague, 11 January 2012, BREIN/Ziggo and XS4All, published in Tijdschrift voor auteurs-, media- en informatierecht 2012, p. 119. The practice of blocking websites has also led to prejudicial questions pending before the CJEU. See Austrian Supreme Court, 11 May 2012, case 4 Ob 6/12d, kino.to/UPC, published in Gewerblicher Rechtsschutz und Urheberrecht – Internationaler Teil 2012, p. 934.

98 Cf. S.K. Katyal, 'Filtering, Piracy Surveillance and Disobedience', Columbia Journal of Law and the Arts 32 (2009), p. 401 (408); J. Gibson, 'Risk Aversion and Rights Accretion in Intellectual Property Law', Yale Law Journal 116 (2007), p. 882.

99 This point has also been raised with regard to the UGC Principles agreed upon in 2007 by Disney, CBS, NBC Universal, Fox, Viacom, Microsoft, MySpace, Veoh and Dailymotion. The Principles are included in A.N. Braverman/T. Southwick, 'The User-Generated Content Principles: The Motivation, Process, Results and Lessons Learned', Columbia Journal of Law and the Arts 32 (2009), p. 471 (476-480). As to the critique based on consumer groups not being represented in the negotiations, see Chuang, supra note 82, p. 189; Sawyer, supra note 82, p. 403.

100 For instance, the UGC Principles, supra note 99, p. 477, provide for a filtering process to be carried out prior to the uploading of content by users of UGC platforms. While this process is described in some detail in the principles, the safeguard for use privileges evolving from the US fair use doctrine is confined to the principle that 'Copyright Owners and UGC Services should cooperate to ensure that the Identification Technology is implemented in a manner that effectively balances legitimate interests in (1) blocking infringing user-uploaded content, (2) allowing wholly original and authorised uploads, and (3) accommodating fair use'. Formally, fair use is thus taken into account. However, it is doubtful whether this vague principle ('...should cooperate to ensure...') lends sufficient weight to the fundamental guarantee of freedom of speech underlying the fair use doctrine. In any case, it does not address the question of how to determine privileged fair use. While copyright owners may adopt a restrictive approach, the interpretation developed by a court might be more flexible. Cf. Katyal, supra note 98, p. 411-416 and 422, and the analysis of fair use case law in the literature supra note 13. See also, on the one hand, the reaction by the Electronic Frontier Foundation and other activist groups insisting on clearer guidelines, 'Fair Use Principles for User Generated Video Content', available at <https://www.eff.org/pages/fair-use-principles-user-generated-video-content>; and on the other hand, the more optimistic assessment by Ginsburg, supra note 65, p. 588-589, pointing out that filters may become more sophisticated over time. As to the impact of intermediary liability on the marketplace of speech, cf. more generally S.F. Kreimer, 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link', University of Pennsylvania Law Review 155 (2006), p. 11; R. Tushnet, 'Power Without Responsibility: Intermediaries and the First Amendment', George Washington Law Review 76 (2008), p. 986 (1004).

101 For similar recommendations for stabilizing copyright's societal acceptance, see Geiger, supra note 8, p. 468.

A Model Framework for publishing Grey Literature in Open Access

by **Matěj Myška** PhD, Institute of Law and Technology, Masaryk University, Brno

Jaromír Šavelka PhD, Institute of Law and Technology, Masaryk University, Brno

The publication of this paper is supported by the Czech Science Foundation – Free Licences Integration Project – registration no. P408/12/2210.

Abstract: In this paper we present a model framework for placing grey literature documents into an online, publicly accessible repository, providing an effective mechanism to avoid liability for a grey literature repository operator. 'Grey literature' is a term (originating in library and information science) referring to documents that are not published commercially, e.g. research and technical reports, governmental documents and working papers. Despite their undeniable value (usually derived from their originality and from containing recent and up-to-date information), these documents are often difficult to access. This creates an obvious problem of not providing the public with valuable information associated with the necessity to fund the production of particular information that already exists and could have been easily offered to the public. One of many possible solutions to make grey literature available seems to be the establishment of centralised on-line repositories of grey literature supported (or maintained) by official agencies. Putting aside the most important issue of financing such an effort, the agency has to face many difficult legal issues, among others. As the task of the agency would be to actively seek the documents to be placed into the repository, it also has to deal with several legal issues. In this paper we try to identify and discuss these legal problems and design a framework for obtaining GL documents from various subjects in such a way that the risk of copyright infringement would be minimised. The proposed framework is based on the practical experience gained from the efforts of the National Library of Technology (of Czech Republic) to establish the National Repository of Grey Literature.

Keywords: Grey Literature, Open Access, Repository, Public Licences

Recommended citation: **Matěj Myška, Jaromír Šavelka,** A model framework for publishing grey literature in Open Access ,4 (2013) JIPITEC 2, para 104.

A. Introduction

1 Greyliterature (hereinafter referred to as 'GL') and its usage is an emerging phenomenon that is gradually drawing more and more academic attention.[1] In the first section of this paper we will define GL, its value and its importance. In the second section we will discuss the issues of accessibility of GL, including its relation to the Open Access movement. These sections should provide for a theoretical introduction to the GL concept. Next the mode of operation for making GL available will be described. The main focus lies in identifying the possible problematic legal issues (namely, copyright, liability for infringement and personal data processing) and proposing solutions for how to tackle them. Thus the system and workflow for rights clearing of GL documents

will be presented. The further parts then focus on the case study of a publicly funded GL repository in Czech Republic, namely the National Repository of Grey Literature (hereinafter referred to as 'NRGL'). The paper concludes with remarks on the main issues identified with both the NRGL and making the GL available to the public in general.

B. Defining grey literature

2 Due to the various types of documents and materials that could be marked as GL, it is not an easy task to provide a comprehensive and all-encompassing definition of GL. The currently most-used one is the 'New York definition' of GL from 2004, which reads as follows: '[Grey literature is] that which is produced on all levels of government, academics, business and industry in print and electronic formats, [...] but which is not controlled by commercial publishers, i.e., where publishing is not the primary activity of the producing body'.[2] Contrary to traditionally published 'white literature' (i.e. books and journals), GL is therefore not primarily aimed at commercial dissemination and is not circulated by conventional distribution channels. This is indeed a very broad definition, leading some scholars to go as far as proclaiming that 'virtually everything we read outside of journals and books can be considered grey literature'.[3] Thus GL may entail diplomas and doctoral theses, research studies, various government reports, supplementary teaching materials, corporate prints (like manuals, product catalogues, annual reports, product handbooks) but also tweets, blog entries, programs of cultural events or even satellite data.[4] This plethora of documents that could be marked as grey literature poses a serious challenge to the attempts to regulate its use explicitly by law. Polčák[5] developed a legal classification of GL based on the goals achieved by the production of the GL. Any GL may therefore fall under one of the following categories: (1) fulfilment of academic or qualification obligations; (2) reporting academic activities; (3) exchanging ideas for academic discussion; (4) developing technical standards; or (5) compliance with legal obligations. Correspondingly, there is a significant multitude of producers of GL. The spectrum ranges from mere individual researchers to organised teams employed by a university/research institution or governmental bodies. Consequently, the subject entitled to exercising the economic rights to the GL may vary. According to Polčák's legal classification of GL,[6] the typical situations in GL production as regards the entity exercising the economic rights are the following: (1) works created by students or candidates; (2) works created by a researcher or a research team for its employer or subsidy provider or created by a hired agency; (3) works created by a single author; (4) works/public documents created by an official or employee of a professional organization; (5) works created by an employee for a private or public employer. The term 'grey literature' itself is not reflected in any national, European or supranational act; it does not constitute any special category of copyrighted works, and therefore the standard copyright rules apply. However, there are certain special peculiarities stemming from the various types of documents involved and from the producers of GL as will be practically demonstrated further in this paper.

3 The *value and importance* of grey literature lies mainly in its complexity, topicality and financial availability. As noted by Schöpfel and Farace, GL 'represents a substantial part of the scientific production'.[7] As GL is not published in a 'traditional way', it logically contains information not available/searchable/indexed by the standard librarian tools (e.g. standard library catalogues). Due to this fact, GL should always be included in literature searches as it limits the potential bias.[8] A mere reliance on the officially published sources may lead to a 'subjective one sided research path'.[9] GL also contains more detailed information, an example being a technical report with detailed descriptions, diagrams and data sets that would be never published in traditional journals.[10] Compared[11] to 'white literature', GL tends to be more up-to-date as it is usually not subject to traditional and time consuming pre-publishing processes. The quality of GL literature is still debatable[12] as it is usually not subject to a quality process like peer-reviewing, in the case of published papers in traditional scientific journals. However, Seymour[13] claims that grey literature is subject to various levels of internal quality assessment – an example being the review process in the case of master's or PhD theses. Also the 'publishing' institution's name and reputation is at stake, so a certain quality check is to be expected. Lastly, due to its non-commercial character, GL is usually available for free as in 'free beer'[14], i.e. without monetary compensation. As discussed in the next section, the emergence of the Open Access movement is also opening up GL, with 'free' in the sense of 'free speech'.

C. Making grey literature available

4 The seminal disadvantage of GL, stemming logically from its definition mentioned above, is its complicated availability.[15] Boukacem-Zeghmouri and Schöpfel characterised GL even as 'underground literature',[16] and called searching for it a 'time-consuming, sometimes expensive and even frustrating experience'.[17] One of the main reasons for the status quo of GL is the absence of a long-term archiving institution. Compared to 'white literature', where a deposit of a published work is a statutory obligation of the publisher, no such obligation is foreseen for the 'publishers' of GL.[18] Thus GL cannot be obtained

in one place (i.e. bought or subscribed to like books and journals) because the multitude of GL 'publication' platforms corresponds to the numerous types of GL producers as described above. The development of the Internet provided for yet another way to make GL available, e.g. on company or personal websites, blogs or in institutional repositories. Standard general search engines (e.g. Google) do not provide a solution to this problem because GL is mainly located in the 'deep web' that is not wholly indexed.[19] Further, there is no centralised and standardised access point like the standard brick-and-mortar library. This is caused mainly by the absence of interoperability standards, missing or incomplete metadata or restricted access to full-text. Systematic collection and making available of GL, therefore, requires 'specific attention, competency and procedures' [20] and, as will be elaborated further, a specific legal approach.[21]

5 One possible solution, at least at the national level, seems to be a publicly funded national GL repository (as described in detail in the following sections).[22] Using appropriate standards and a common interface, the national repositories could then be linked together and accessible via a unified (e.g. European GL) search engine. Such a theoretical concept, however, adds other legal issues that have to be tackled. Apart from the legal questions identified,[23] the acquisition and making available of GL constitutes a further use of the work. In addition, the *sui generis* database rights would need to be cleared because the collecting of GL could be facilitated in an automated manner and would equal extraction or re-utilisation of the whole or parts of the database content.[24]

6 Another challenge to GL is posed by the development of the Open Access movement,[25] whose foundations were formulated in the famous BBB Statements.[26] Accordingly, an Open Access document (contribution) should be: (1) accessible to the reader without any obstacles, preferably online; (2) granting the user a wide set of rights;[27] and (3) deposited in a suitable form and in a repository ensuring long-term archiving.[28] The aim of the Open Access movement was aptly summarised by Bargheer et al. as 'providing for an access to all the relevant information to all the researchers, students and teacher no matter of their location and/or financial situation'.[29] Primarily the Open Access principles and the related effort of making scientific results openly available are targeted at the standard peer-reviewed journals published by traditional publishing houses like Springer, Wiley or Elsevier. GL is characterised by its primarily non-commercial means of distribution and thus meets the first of the above-mentioned Open Access conditions as regards availability without remuneration. The application of the remaining conditions – i.e. rights granting and long-term accessibility – could be seen as the much-needed development in collecting and making GL available. From a legal point of view, it has to be emphasised that Open Access principles require more than just simply placing a document online in an online repository.[30] By doing so, GL could be used merely in the regime of copyright exceptions (limitations) and/or free use as provided for in the relevant national acts.[31] The user of this GL would not be able to disseminate, re-use or build upon this document. Thus another expression of will of the subject exercising the rights to the work is needed – namely, a licence. According to the Berlin Declaration, such a licence shall grant 'to all users a free, irrevocable, worldwide, right of access to, and a licence to copy, use, distribute, transmit and display the work publicly and to make and distribute derivative works, in any digital medium for any responsible purpose, subject to proper attribution of authorship'.[32] Usually a licence is agreed upon between two individual parties; however, this mode of contracting is unfeasible in the online environment. The practical use of such tailored individual licensing would bring a significant raise in transactional costs both to the licensor and licensee. A viable solution to address this problem would be 'public licences'.[33] As the discussion of the legal nature of public licences is outside the scope of this article,[34] we could very simply characterize them as a contract offered to an unspecified group of offerees that is concluded by use of the work. The terms of such a contract are specified in the chosen version of the 'ready-made' licence. To make the contracting process simpler, the terms (or a link directing to the full text of the licence) are attached to the respective work. Further, the usage of a specific public licence can also be emphasised by using a graphic logo symbolising the respective licence. A plethora of standardised 'ready-made' licences have been made available online for public use, the most prominent being the Creative Commons licensing suite.[35] [36] The author (or the subject entitled to exercise the rights to the copyrighted work) could choose from a variety of licensing options by using one of the pre-determined variants of the licensing agreement wording. The author may therefore prohibit/allow making of derivative works by opting/not opting for the licensing feature NoDerivs (ND). A special option of this condition is the allowance of making of derivative works only if the resulting work is licensed under the same or a similar public licence (Share-Alike - SA). A further option is the exclusion or allowance of commercial use of the work, which is achieved by including/omitting the NonCommercial (NC). Every time the user is obliged to properly attribute the work to the author (Attribution – BY) and thus respect its moral rights. The first two conditions of the abovementioned Open Access principles are fulfilled by granting the user the relatively broad 'worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright)'[37] licence to reproduce, distribute and publicly perform the licensed work. It must be noted that only the most permissive version of the Crea-

tive Commons licence is compliant with the Open Access principles as noted above.[38] However, using the Creative Commons licences in the context of making GL available under the Open Access principles again complicates the function of the GL repository from a legal point of view. Offering a work under one of the Creative Commons licenses itself means logically the granting of the licence, and thus has to be regarded as an exercise of economic rights that is reserved only for the properly entitled person. As no one is generally entitled to transfer more rights than he himself has, such use constitutes a perpetuating copyright infringement because the Creative Commons licences are irrevocable.

D. Legal issues

7 Building up a centralised GL repository, however, raises some serious legal issues that will be addressed in this section. These risks can be identified and will be discussed below in detail as follows: (1) copyright issues (GL as copyrighted work, school works, databases) and liability for copyright infringement and (2) personal data processing.

I. Copyright and liability for copyright infringement

8 We provided a thorough exposition of the concept of grey literature in the second section of this paper. At this point, it is our intention to develop the account with respect to legal issues surrounding GL. The first question concerns the subject matter of copyright protection. Despite the term used – grey literature – not all the GL documents can be automatically regarded as 'literary works' within the meaning of Aricles 2(5) and 8 of the Berne Convention. Moreover, the term 'grey literature' also encompasses other types of works apart from literary works, e.g. graphic works, motion pictures, sound recordings or mixes (interactive presentations, texts accompanied with graphics, etc.). Thus the conditions in the national legal orders have to be individually examined in every document that is to be placed in the GL repository. On the European level, the Court of Justice of the European Union has taken quite a broad approach[39] in the Infopaq case,[40] stating that the decisive criterion of 'the author's own intellectual criterion' has to applied. Under Czech law (Sec. 2 of the Czech Copyright Act[41]), however, a work has to be expressed in an objectively perceivable manner and be an outcome of the author's own creative activity in order to enjoy the full copyright protection. These distinguishing traits are often difficult to evaluate, especially the creative nature of an author's activity.[42] The following definition may be used as a guide: 'creative activity (...), the core concept of copyright law, can be characterised as an activity that consists in creation of an intangible artefact. Such a result depends on the personal traits of its creator in absence of which it would not have occurred'.[43] To put it simply: if the outcome of an activity performed by various people has to be different, then by necessity the concerned activity is most likely creative. In the case of identical or similar outcomes, it is probably not possible to speak about an involvement of creative activity – therefore, the criterion of statistical probability applies. In order to mitigate the risk of copyright infringement, it is reasonable to treat the GL documents as copyrighted works rather than unprotected information. If a document which in fact does not qualify to be a literary work is considered to be protected by copyright, the negative outcome consists in either abstaining from its use or unnecessary activity connected with asking for a licence. Such results are therefore not detrimental to the operator of the repository. However, the other scenario – i.e. treating the copyrighted work as mere unprotected information – may consequently result in the liability of the GL repository operator. Thus in order to avoid the related negative consequences (i.e. lengthy court proceedings, judgement ordering the payment of damages and unjust enrichment) it makes sense to anticipate the existence of copyright protection in cases in which it is difficult to assess the nature of the individual document.

9 Additionally, the copyright and *sui generis* protection of databases has to be taken into account.[44] This issue would be relevant primarily in cases of the placement of large document volumes into the repository. The database protection also comes into play when the GL repository plans to extract and re-utilize the GL producer's databases of GL documents. In these cases it would not suffice to analyse the legal status of the individual documents. Additionally, it needs to be determined whether database rights are vested in the used collection or not. With respect to copyright protection, it is again advisable to take the same defensive approach as in the case of individual GL documents and treat the database as a copyrighted work. And it also needs to be decided whether *sui generis* protection applies. In this area, Czech law is completely harmonised by Directive 96/9/EC and does not deviate from the already-established case law.[45] Thus the protection is available for the database that is 'a collection of independent works, data, or other items arranged in a systematic or methodical manner and individually accessible by electronic or other means, irrespective of the form of the expression thereof'.[46] Rights *sui generis* are held by the maker of the database. However, this is the case only if 'the formation, verification or presentation of the content of the database represents a contribution, which is substantial in terms of quality or quantity, irrespective of whether the database or the contents thereof are subject to copyright protection or any other type of protection'.[47] If the *sui generis* rights exist, the maker of the data-

base has the exclusive rights to 'extraction or re-utilisation of the entire content of the database or of its part substantial in terms of quality or quantity, and the right to grant to another person the authorisation to execute such a right'.[48] In order to clear the above-mentioned rights, the GL repository operator needs to enter into contract with the GL producer, not only as regards the particular contained works but also as regards respective database.

10 This defensive approach is not needed with the GL documents that do not fulfil the above-mentioned conditions for copyright protection. These documents could therefore be considered mere information not protected by copyright. These include GL documents that fall under the definition of an official work within the meaning of Sec. 3 CCA that excludes copyright protection for such works. In the sense of Article 2(4) of the Berne Convention, the Czech Republic does not consider the following documents ('official texts') copyrighted: legal regulation, court decision, public charter, publicly accessible register and collection of its documents, and also any official draft of an official work and other preparatory official documentation including the official translation of such a work, Chamber of Deputies and Senate publications, a memorial chronicle of a municipality (municipal chronicles), a state symbol and symbol of a municipality, and any other such works where there is public interest in their exclusion from copyright protection. However, the absence of copyright protection does not logically exclude other protective regimes (such as trade secrets, know-how and personal data protection) as will be elaborated further.

11 Under Czech law, special attention has to be paid to one category of GL documents, namely, school works produced as a fulfilment of academic obligations. A special exception is stipulated in Section 47b of the Czech Act No. 111/1998 Sb. on Higher Education Institutions[49] Czech Republic.[50] According to this provision, the higher educational institutions are 'obliged to make public, at no profit to themselves, the doctoral, Master's, Bachelor's and advanced Master's ('rigorózní') theses that have been defended at their institutions, including the readers' reports and results of the defence'. It is basically up to the educational institution which means are used to fulfil the requirement – this provision is a blanket norm providing that the further details of making available should be stipulated in an internal regulation of the institution.[51] The institution could therefore decide to use the GL repository as a way to fulfil its statutory obligation. The higher educational institution (i.e. the GL producer) may also use the online repository. The consent of the author of the thesis for this use is not needed as it is presumed to be given at the time when the student hands in the thesis. However, no other uses are permitted. It must be noted that this exception to the reproduction right as stipulated on the European level in Article 2 of the InfoSoc Directive[52] was not undisputed. The Copyright Department of the Ministry expressed in its Opinion[53] that such a use is contradictory to the three-step test – that is, unlike in the other Member States, regulated directly in the national Copyright Act (Sec. 29 CCA). However, no national court has yet ruled that such use of the theses constitutes an infringement on the basis that it conflicts with a normal exploitation of the work and unreasonably prejudices the legitimate interests of the right holder.

12 As explained above, GL documents are better treated as copyrighted work and thus fully protected by the relevant national copyright laws (e.g. Czech Copyright Act). Thus any unauthorised use of the work results in copyright infringement. In order to avoid such infringement, the operator of a GL repository needs to enter into a proper licence agreement with the GL producer (i.e. in most cases, the proper subject entitled to exercise the economic rights). This agreement shall cover at least the reproduction rights, the making available right and the right to include the copyrighted work in a database. Further, if the GL operator plans to offer the GL documents under the Open Access principles, the agreement should also include the possibility to make use of the above-mentioned public licences. In practice this condition means that the copyright holder should vest the GL repository with enough rights to make use of the above-mentioned public licences.

13 The modus operandi of acquiring of the GL documents also plays a significant role in determining the liability for potential copyright infringement. The operator of a GL repository may acquire the GL documents either ad hoc or on a permanent framework agreement basis. In the first case, the GL operator acts as the sole 'publisher' of the documents and is directly liable for potential copyright infringement. The possibility to regress the possible negative results of such proceedings shall be stated in the licence agreement between the GL repository operator and GL producer. This agreement shall consequently contain a provision stipulating the empowerment of the GL producer to license the work and also the proclamation that no third party's rights are vested in this work. However, the possibility to regress is generally regulated in the respective national civil law codices (as in Czech Act No. 40/1964 Sb., Civil Code, as further amended). The role of the GL repository operator changes when the operator provides only for a platform that allows publication of the GL documents directly by the GL producer. Practically, such a situation emerges when the GL repository operator establishes a direct publication access into the system to the GL producer, typically an educational institution. This is convenient, however, only if a permanent cooperation between the GL producer and GL repository is planned. In this case, the GL repository may qualify in the sense of

'hosting' an information society service provider and benefiting from the liability exception provided for in Sec. 5 of Act No. 480/2004 Sb., Act on Certain Information Society Services, as amended[54] that implements Article 15 of the E-Commerce Directive.[55] However, the Czech implementation is a rather peculiar one. Whereas the E-Commerce Directives provides for 'safe harbour', ensuring that the ISP is not liable unless the foreseen circumstances arise, the Czech legislator took the reverse approach, stating that the hosting information society service provider is liable unless the conditions of safe harbour are fulfilled. These include either the absence of constructive knowledge of the infringing conduct (unconscious negligence: Sec. 5(a) Act No. 480/2004 Sb., Act on Certain Information Society Services, as amended) or failure to remove or disable access to the infringing information (Sec. 5(b) of the same Act). The Czech provisions on ISP liability, however, should be interpreted to conform with the acquis, i.e. the ISP is to be held liable after the loss of safe harbour according to special laws, not just merely because he lost it. The aim of the Directive, as Husovec[56] notes, should be to delimit the moment to which the ISP is not liable. The Czech courts have not dealt with the liability of the ISP provider specifically in the case of copyright infringement. However, in the Prolux[57] case that concerned the responsibility of the operator of a website for defamatory remarks contained in the discussion below an article, the High Court in Prague ruled that for liability under Sec. 5(a), the illegality of the information must be apparent to the ISP. In the case of the actual knowledge, the mere disputability of the illegal nature might be enough. For the GL repository operator, who should have a certain degree of knowledge about copyright law, this would mean, for example, that he could be held liable for placing the clearly marked final theses under one of the public licences.

II. Personal data processing

14 As mentioned earlier, even if the GL documents do not enjoy copyright protection, further legal protection regimes may apply, the most common being the protection of personal data. The GL documents may contain various data and metadata related to authors and other individuals.[58] First, it must be assessed whether this data constitutes personal data. On the European level, the guidance is to be found in Directive 95/46/EC.[59] Czech law relied very heavily on the original text of this Directive, and thus, for example, the definition of personal data in Sec. 4(b) of the Czech Act on Protection of Personal Data (hereinafter referred to as 'PDPA'),[60] 'personal data' is basically a literal translation of the definition in the Directive. Therefore, 'personal data' shall mean 'any information relating to an identified or identifiable data subject. A data subject shall be considered identified or identifiable if it is possible to identify the data subject directly or indirectly in particular on the basis of a number, code or one or more factors specific to his/her physical, physiological, psychical, economic, cultural or social identity'. The name itself is not always able to identify the data subject. However, the further metadata may make the subject quite easily identifiable. Also the Czech Office for Personal Data Protection employs a rather broad notion of the term 'personal data' as expressed in the Position of the Office for Personal Data Protection No. 3/2012 - On the Notion of Personal Data.[61] According to this opinion, the decisive factor for marking data as personal is the possibility to identify a subject even only indirectly, i.e. with the help of other publicly available information. Especially in the case of academia, a simple name and academic position are usually sufficient to identify the respective individual. Therefore, the data and metadata gathered by the GL repository operator in the process of acquiring the GL (apart from the above-mentioned date of birth, e-mail address, etc.) could be linked to an individual and therefore constitute personal data, but rarely sensitive data. Thus the gathered data about the authors should be, for the sake of mitigating the possible legal risks,[62] regarded as personal data; its collection should be regarded as personal data processing and must comply with the legal obligations stipulated in the Personal Data Protection Directive (hereinafter referred to as 'PDPD') or national law (referred to as PDPA). Article 24 of the PDPD found its reflection in Chapter VII of the PDPA that bans the unlawful processing of personal data as an administrative offence that is punishable by significant financial fines (up to CZK 10,000,000). In the context of processing personal data, the legal roles of the GL producer and the GL repository operator have to be distinguished. The personal data stem primarily from GL producers who also act as personal data controllers (Art. 2(d) PDPD - Sec. 4(j) PDPA) of GL authors' data or third persons.[63] This processing has to be legitimate, therefore based upon consent of the data subjects or law or without consent if prescribed by law. The data controller transfers personal data to the GL repository operator who is consequently to be regarded as the data processor (Art. 2(e) Personal Data Protection Directive - Sec. 4(j) PDPA).[64] An individual agreement on such personal data processing needs to be concluded pursuant to Sec. 6 PDPA (which implements Article 17 PDPD) between the GL repository operator and the respective GL producer. This agreement must be made in writing and shall 'explicitly stipulate the scope, purpose and period of time for which it is concluded'. Furthermore, the agreement must contain guarantees by the processor related to technical and organisational securing of the protection of personal data. A similar agreement must be concluded if the data processor (GL repository operator) intends to transfer the personal data to a third party. Lastly, if the GL repository ope-

rator obtains the GL documents from the authors/other natural persons acting as GL producers then as a data controller, thus a proper notification to the Personal Data Protection Office is needed.

15 With the new proposed regulation[65] ahead, changes to the processing of personal data are to be expected.[66] However, the legislative text is still in a state of flux and constantly debated. A prime example is the notion of consent defined in Article 4(8) of the proposed Regulation. Originally it was 'explicit', but lately it was changed back to the 'specific and informed' (i.e. 'unambiguous' which is the current definition in the PDPD and the current PDPA). As regards the GL repository, the newly proposed duties for a data processor stipulated in Article 26 are to be taken into account. The current status quo (both on the European level and in Czech law) is that the obligations need to be imposed on the data processor from the data controller contractually (see supra). The new Regulation introduces direct regulation of the obligations of data processors, such as the obligation to maintain appropriate documentation (Art. 28(2) of the Regulation), co-operate with the supervisory authority (Art. 29), appoint a data protection officer (Art. 35) of the Regulation) and direct liability for data breaches (Art. 79) of the Regulation).

16 The above-mentioned issues were identified as the basic legal issues any GL repository has to deal with in general, with a special focus on the Czech law. In the next section we will take a closer look at how these issues have been solved practically in the National Repository of Grey Literature of the National Technical Library in Czech Republic.

E. National Repository of Grey Literature

17 In these three general sections we have shown that, despite its peculiarities, making GL available raises relatively complicated legal issues. Next, it was important to find out which organizations were about to carry the most important legal duties within the framework that was about to be established. In the following case study, we provide an overview of how these issues have been addressed in the Czech National Repository of Grey Literature. Between 2008 and 2011, the National Technical Library of Czech Republic (hereinafter referred to as 'NTL') played a pivotal role in the establishment of what is today known as the National Repository of Grey Literature. It is an online search engine that allows searching through a repository of grey literature documents.[67] Both the search engine and the repository are maintained and supported by the NTL. Furthermore, the NTL spreads awareness regarding grey literature, its value and the possibilities NRGL opens. Also, the NTL engages in negotiations with producers of grey literature and established a mechanism of placing their documents into NRGL. Finally, the NTL maintains and keeps up the repository and leads negotiations with those who would like to use NRGL in ways that exceed simple acquiring of documents.

18 In 2009, when NRGL was about to be launched, extensive preparatory work was culminating, including a legal assessment of the status of the NRGL. The legal analysis was prepared by the researchers at the Institute of Law and Technology, Masaryk University, Brno, and is available online in Czech.[68] This analysis and the accompanying template contract documents later became the central reference materials for dealing with legal issues that appeared immediately after the launch. The main purpose of the analysis was to place the above-mentioned issues in all their complexity on solid legal ground.

19 As the key players in the NRGL system, the NTL and the GL producer were identified. Whereas there is no legal problem regarding the position of the NTL, the term 'GL producer' needed to be specified. As was also briefly sketched out in part A of this paper, the GL producer may comprise different parties with different interests and levels of empowerment to exercise the economic rights.

20 Least complicated is the situation where the GL producer is a sole author who is unlimited in the exercise of his rights. Here the licence agreement is concluded directly between the two parties. Logically, in the case of a co-authored work, the consent to use the work is needed from all the authors. In the case of employee work, the subject entitled under Czech law to exercise the economic rights is the employer, unless agreed otherwise in the employment contract (Sec. 58 CCA). As regards the moral rights, according to Sec. 58(4) CCA it is presumed that the employee 'has given his consent to the work's being made public, altered, adapted (including translation), combined with another work, included into a collection of works and, unless agreed otherwise, also presented to the public under the employer's name'. In this case, the NTL has to enter into negotiation with the respective representative of the employer/employing institution. In the case of school works (Sec. 60 CCA), the simple making available by the GL producer (in this case by definition an educational institution] is covered by the above-mentioned exception of Sec. 47b, Act No. 111/1998 Sb. on Higher Education Institutions as amended. However, the inclusion into other database (such as NRGL) is considered a separate use of work, and offering the work under public licence has to be authorised by the author (in this case, the student) in a licence agreement with the GL producer.

21 As regards the personal data protection and consent to process them, again the situation is dependent on the subject of the GL producer. A sole author may

freely give consent to process her personal data. As stated above, in this case the GL repository acts as a data controller and has to fulfil all legal duties. If the GL producer has already amassed the personal data, the GL repository operator will then act solely as a data processor. Here an appropriate written contract would be one as described above. The GL producer (e.g. a university) can process the data only on the basis of the consent of data subjects (Art. 7 PDPD; Sec. or if it is foreseen by law (Sec. 5(2)(a) and (d) PDPA that correspond to Art. 7 PDPA). An illustrative case where no consent of the data subject is needed and where the GL producer is fulfilling its legal obligations is the situation discussed above concerning the making available of the theses stipulated in Act No. 111/1998 Sb. on Higher Education Institutions as amended.

22 In practice, the procedure for obtaining and making GL available should aim at mitigating (eliminating) the most legal risk (i.e. the liability) in the beginning with reasonable personal and time costs. The first step is the establishment of initial contact between NTL and the GL producer. The librarian inquires about the possibilities of obtaining the producer's consent to make the GL document available. If a mutual desire for cooperation arises, the librarian tries to outline the details of further cooperation.

23 What follows depends on the volume of the documents that are about to be made available. If their number is rather limited, the librarian produces the list of GL to be acquired and fills in the most appropriate template contract prepared by the lawyer. These two documents are then forwarded to the lawyer. The lawyer usually identifies documents that are in some way risky – usually those documents whose making available would require the consent of persons who have not yet been involved in the process – and instructs the librarian regarding what further information should be gathered. Once the librarian gathers the necessary information or recognizes its unavailability she immediately informs the lawyer about the result. Consequently, the lawyer informs the librarian about the risks associated with making the documents available that have been recognised as potentially 'harmful'. Taking this particular information into account, the librarian informs the lawyer about the final decisions regarding the set of GL documents that is going to be made available.

24 If a continual placement of the GL documents in the NRGL based on the quantity of the GL documents is foreseen (for example, as in the case of making the bachelor, diploma and dissertation theses available in the sense of Sec. 47b), a permanent cooperation framework has to be established. In this case, the involvement of legal and IT staff is significantly higher. The template cooperation agreement that includes the appropriate licence agreement and specific clause regarding the personal data processing/transfer and appropriate safeguards is gradually tailored based upon the requests and remarks of the parties involved. As mentioned earlier in this phase, it is crucial for the GL producer to succeed in obtaining the respective rights to the intended GL documents, as well as the proper consent to transfer personal data to the NTL. The technical conditions of obtaining the GL documents (i.e. the parameters of the interface) prepared by the NRGL IT technician form an annex to the aforementioned contract.

F. Conclusions

25 'Grey literature is here to stay',[69] and so is the Open Access movement.[70] Even though the access, collecting and making available are regarded as problematic and remain a constant challenge from a librarian's point of view,[71] the emerging legal issues (i.e. the legal nature of GL, the licensing issues and personal data processing) are solvable by setting up a proper process, including adequate contractual arrangements of rights as we have tried to show in this paper.

26 However the further making available of the GL documents under the terms of selected public licences such as the Open Access principles foresees additional requirements on the scope of the entitlement the right-holder has to have, and thus the risk of third parties' rights violations increases. Taking into account the irrevocability of the public licences, the infringement is perpetual – any other party obtaining the licence may use the work as stipulated in good faith. However, this is not a problem of the legal regulation of public licences but a simple lack of knowledge on the side of the parties involved. Due to the public licences' 'free connotation', these are especially regarded as a panacea to all of the emerging legal question of GL. One reason for this seems to be the relative suppression of the importance of the economic rights to GL. Because they are not primarily aimed at commercial distribution, the GL documents are prone to be treated as not qualified enough for copyright protection. As we have found out in this paper, the copyright protection applies fully, provided that they fulfil the needed legal conditions no matter the economic or social value of GL. The inclusion of the trained lawyer in the described model of placing the GL documents into a repository (the NRGL in particular) should minimize the risk of copyright infringement and control the 'making available' enthusiasm, though one can never guarantee that a document that should not be placed into the NRGL will one day pass the protective procedure and be made available, even under public licence. As this situation has not yet occurred, one can only speculate what the results of the respective copyright infringement proceedings will be. The emer-

ging case law, however, will provide an optimal subject for further researches.

References:

Act No. 101/2000 Sb., on the Protection of Personal Data and on Amendment to Some Acts, as amended. Full and updated official English translation is available from <http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&lang=en>.

Act No. 121/2000 Sb., on Copyright and Rights Related to Copyright and on Amendment to Certain Acts (the Copyright Act), as amended. Full and partly updated official English translation is available from <http://www.mkcr.cz/assets/autorske-pravo/12-AZ_2006_v_AJ.pdf>.

Act No. 37/1995 Sb., on Non-Periodical Publications as amended.

Act No. 46/2000 Sb., on the rights and duties in the publication of the periodical press and on the amendment of certain laws (Press Act) as amended.

Act. No. 111/1998 Sb. on Higher Education Institutions as amended.

BANKS, Marcus, A. How the Success of Open Access Publishing Can Stimulate Improved Access to Grey Literature [online]. Urban Library Journal. 2007. Vol. 14, No. 1. Accessed 15 June 2013. Available at <http://ojs.cunylibraries.org/index.php/ulj/article/view/36/61>.

BANKS, Marcus, A. Towards a continuum of scholarship: the eventual collapse of the distinction between grey and non-grey literature, 2005. In GL7: Seventh International Conference on Grey Literature, Nancy (France), December 2005 (in press) [Conference Paper]. Accessed 15 June 2013. Available at <http://eprints.rclis.org/bitstream/10760/7287/1/GL7Paper_Final.pdf>.

BARGHEER et al. In: SPINDLER, Gerald (Ed.) Rechtliche Rahmenbedingungen von Open Access-Publikationen, Göttinger Schriften zur Internetforschung, Band 2, Universitätsverlag Göttingen, 2006. Accessed 15 June 2013. Available at <http://univerlag.uni-goettingen.de/OA-Leitfaden/oaleitfaden_web.pdf>.

BOUKACEM-ZEGHMOURI, Chérifa; SCHÖPFEL, Joachim. Access and document supply: A comparative study of grey literature. Seventh International Conference on Grey Literature: Open Access to Grey Resources, 5-6 December 2005. Available at <http://www.opengrey.eu/data/69/78/07/GL7_Boukacem_et_al_2006_Conference_Preprint.pdf>.

Compromise text of the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2012/0011 (COD). 10227/13. Available at <http://register.consilium.europa.eu/pdf/en/13/st10/st10227-ad01.en13.pdf. Accessed 15 June 2013>.

COONIN, Brina. Grey literature: An annotated bibliography [online]. 2003. Last modified 18 June 2003. Accessed 15 June 2013. Available at <http://personal.ecu.edu/cooninb/Greyliterature.htm>.

COSTA, Luiz. Poullet. Privacy and the regulation of 2012. Computer Law & Security Review. Volume 28, Issue 3, June 2012, pp. 254-262, ISSN 0267-3649, 10.1016/j.clsr.2012.03.015. Available at <http://www.sciencedirect.com/science/article/pii/S0267364912000672>.

DE CASTRO, Paola De Castro; SALINETTI, Sandra. Quality of grey literature in the open access era: Privilege and responsibility. Publishing research quarterly. 2004. Vol. 20, No. 1, p. 4. ISSN 10538801.

DE HERT Paul, PAPAKONSTANTINOU, Vagelis. The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals Computer Law & Security Review. Volume 28, Issue 2, April 2012, pages 130-142, ISSN 0267-3649, 10.1016/j.clsr.2012.01.011. Available at <http://www.sciencedirect.com/science/article/pii/S0267364912000295>.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. Official Journal L 167 , 22/06/2001 P. 0010 – 0019.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

FARACE, Dominic John; SCHÖPFEL, Joachim. Grey literature in library and information studies. Berlin: De Gruyter Saur, 2010. 282 p.

HE, Bin; PATEL, Mitesh; ZHANG Zhen; CHANG, Kevin Chen Chuan. Accessing the deep web. Commun. ACM. Vol. 50, No. 5. (May 2007), pp. 94-101, doi:10.1145/1230819.1241670.

HUSOVEC, Martin. Zodpovednos poskytovate a za obsah diskusných príspevkov. Revue pro právo a technologie. Vol. 2, Issue 2, 2011, pp. 40-42. ISSN 1804-538.

MACKENZIE, Owen, John. The expanding horizon of Grey Literature. 1997. In GL3: Third International Conference on Grey Literature, Luxembourg. 1997. Available at <http://hdl.handle.net/10760/5654>.

MCAULEY, Laura; PHAM, Ba'; TUGWELL, Peter; MOHER, David. Does the inclusion of grey literature influence estimates of intervention effectiveness reported in meta-analyses? The Lancet. 2000. Vol. 356, Issue 9237, pp. 1228-1231.

PEJŠOVÁ, Petra (ed.). Grey literature repositories. Zlín : VeRBuM, 2010. 156 p. Available at <http://nrgl.techlib.cz/images/Book.pdf>. ISBN 978-80-904273-6-5.

POLČÁK, Radim. Legal Aspects of Grey Literature. In PEJŠOVÁ, Petra (ed.). Grey literature repositories. Zlín : VeRBuM, 2010. 156 p. Available at <http://nrgl.techlib.cz/images/Book.pdf>. ISBN 978-80-904273-6-5.

POLČÁK, Radim. ŠAVELKA, Jaromír. Digitální zpracování tzv. šedé literatury pro Národní úložiště šedé literatury. 2009. Accessed 21 October 2012. Available at <http://invenio.nusl.cz/record/111528/files/idr-284_1.pdf>.

POLČÁK, Radim. ŠAVELKA, Jaromír. Digitální zpracování tzv. šedé literatury pro Národní úložiště šedé literatury. 2009. Accessed 15 June 2013. Available at <http://invenio.nusl.cz/record/111528/files/idr-284_1.pdf>.

Position of the Office for Personal Data Protection No. 3/2012 - On the Notion of Personal Data. Available online in Czech at <http://www.uoou.cz/files/stanovisko_2012_3.pdf>.

SCHÖPFEL, Joachim. Access to European Grey Literature. In: PEJŠOVÁ, Petra (ed.). Grey literature repositories. Zlín : VeRBuM, 2010. 156 p. Available at <http://nrgl.techlib.cz/images/Book.pdf>. ISBN 978-80-904273-6-5.

SCHÖPFEL, Joachim. Towards a Prague Definition of Grey Literature. Twelfth International Conference on Grey Literature: Transparency in Grey Literature. Grey Tech Approaches to High Tech Issues. Prague, 6-7 December 2010, Czech Republic (2010). Author manuscript available at <http://archivesic.ccsd.cnrs.fr/docs/00/58/15/70/PDF/GL_12_Schopfel_v5.2.pdf>. Accessed 15 June 2013.

SEYMOUR, Deni J. Sanctioned Inequity and Accessibility Issues in the Grey Literature in the United States. Archaeologies Journal of the World Archaeological Congress. 2010. 6(2). pp. 233-269. DOI 10.1007/s11759-010-9144-6.

VELTEROP, Johannes. Open Access Publishing and Scholarly Societies: A Guide. New York: Open Society Institute. 2005. Available at <http://www.opensocietyfoundations.org/openaccess/pdf/open_access_publishing_and_scholarly_societies.pdf>. Accessed 15 June 2013.

27

1 See e.g. the activities of the Grey Literature Network Service, available at <www.greynet.org>. As a reference and general introduction to the topic of GL, see FARACE, Dominic John; SCHÖPFEL, Joachim. Grey literature in library and information studies. Berlin: De Gruyter Saur, 2010. 282 p. and PEJŠOVÁ, Petra (ed.). Grey literature repositories. Zlín: VeRBuM, 2010. 156 p. Available at <http://nrgl.techlib.cz/images/Book.pdf>. ISBN 978-80-904273-6-5.

2 SCHÖPFEL, Joachim. Towards a Prague Definition of Grey Literature. Twelfth International Conference on Grey Literature: Transparency in Grey Literature. Grey Tech Approaches to High Tech Issues. Prague, 6-7 December 2010, Czech Republic (2010). Author manuscript available at <http://archivesic.ccsd.cnrs.fr/docs/00/58/15/70/PDF/GL_12_Schopfel_v5.2.pdf>. Accessed 21 October 2012. p. 2.

3 COONIN, Brina. Grey literature: An annotated bibliography [online]. 2003. Last modified 18 June 2003. Accessed 21 October 2012. Available at <http://personal.ecu.edu/cooninb/Greyliterature.htm>.

4 For an exhaustive overview of the various document types, see <http://www.greynet.org/greysourceindex/documenttypes.html>.

5 POLČÁK, Radim. Legal Aspects of Grey Literature. In PEJŠOVÁ, Petra (ed.). Grey literature repositories. Zlín: VeRBuM, 2010. 156 p. Available at <http://nrgl.techlib.cz/images/Book.pdf>. ISBN 978-80-904273-6-5. p. 68.

6 Ibid, p. 69.

7 SCHÖPFEL, Joachim; Farace, DJ (2009). Grey Literature. In: Bates, MJ; Maack, MN (eds). Encyclopedia of Library and Information Sciences. 3rd edition. Taylor & Francis. As cited in: Usage of grey literature in open archives: state of the art and empirical results, p. 74.

8 See MCAULEY, Laura; PHAM, Ba'; TUGWELL, Peter; MOHER, David. Does the inclusion of grey literature influence estimates of intervention effectiveness reported in meta-analyses? The Lancet. 2000. Vol. 356, Issue 9237, pp. 1228-1231. HOPEWELL, Sally; McDONALD, Steve; CLARKE, Mike J; EGGER, Matthias. Grey literature in meta-analyses of randomized trials of health care interventions. Cochrane Database of Systematic Reviews. 2007, Issue 2. Art. No.: MR000010. Available at

9 VASKA, Marcus. In: PEJŠOVÁ, Petra (ed.). Grey literature repositories. Zlín: VeRBuM, 2010. 156 p. Available at <http://nrgl.techlib.cz/images/Book.pdf>. ISBN 978-80-904273-6-5. p. 12.

10 DE CASTRO, Paola; SALINETTI, Sandra. Quality of grey literature in the open access era: Privilege and responsibility. Publishing research quarterly. 2004. Vol. 20, No. 1, p. 4. ISSN 10538801.

11 For a thorough comparison between 'grey' and 'white' literature, see MACKENZIE, Owen, John. The expanding horizon of Grey Literature. 1997. In GL3 : Third International Conference on Grey Literature, Luxembourg. 1997. Available at <http://hdl.handle.net/10760/5654>.

12 See supra FN 10.

13 SEYMOUR, Deni J. Sanctioned Inequity and Accessibility Issues in the Grey Literature in the United States. Archaeologies Journal of the World Archaeological Congress. 2010. 6(2). pp. 233-269. DOI 10.1007/s11759-010-9144-6.

14 Paraphrasing the famous characterisation of Free Software by Free Software Foundation.

15 See e.g. BANKS, Marcus, A. Towards a continuum of scholarship: The eventual collapse of the distinction between grey and non-grey literature, 2005. In GL7: Seventh International Conference on Grey Literature, Nancy (France), December 2005 (in press) [Conference Paper]. Available at <http://eprints.rclis.org/bitstream/10760/7287/1/GL7Paper_Final.pdf>.

16 BOUKACEM-ZEGHMOURI, Chérifa; SCHÖPFEL, Joachim. Access and document supply: A comparative study of grey literature. Seventh International Conference on Grey Literature: Open Access to Grey Resources, 5-6 December 2005. Available at <http://www.opengrey.eu/data/69/78/07/GL7_Boukacem_et_al_2006_Conference_Preprint.pdf>. p. 2.

17 Ibid.

18 In Czech Republic this obligation of the publisher to deposit a printed copy of a published periodical or non-periodical publication at the National Library is stipulated by Act No. 46/2000 Coll., on the rights and duties in the publication of the periodical press and on the amendment of certain laws (Press Act) as amended and Act No. 37/1995 Sb., on Non-Periodical Publications as amended.

19 See HE, Bin; PATEL, Mitesh; ZHANG, Zhen; CHANG, Kevin Chen Chuan. Accessing the deep web. Commun. ACM. Vol. 50, No. 5. (May 2007), pp. 94-101, doi:10.1145/1230819.1241670.

20 SCHÖPFEL, Joachim. Access to European Grey Literature. In: PEJŠOVÁ, Petra (ed.). Grey literature repositories. Zlín: VeRBuM, 2010. 156 p. Available at <http://nrgl.techlib.cz/images/Book.pdf>. ISBN 978-80-904273-6-5. p. 20.

21 It is not the aim of this paper to provide for a solution from the information and library studies point of view. For this approach, see resources cited supra 1.

22 See generally PEJŠOVÁ, Petra (ed.). Grey literature repositories. Zlín: VeRBuM, 2010. 156 p. Available at <http://nrgl.techlib.cz/images/Book.pdf>. ISBN 978-80-904273-6-5.

23 The question is whether the GL document constitutes a copyrighted work, and if so, who is the subject entitled to exercise the economic rights.

24 Good examples are the databases of publicly available theses defended at the respective universities. (E.g. in Czech Republic, the Masaryk University makes the theses available through its Information System, available at <https://is.muni.cz/thesis/?lang=en>). However, this is not to be understood as making available in the sense of using copyrighted work, but as fulfilling the legal obligation stipulated by Sec. 47b of Act. No. 111/1998 Sb. on Higher Education Institutions as amended.

25 BANKS, Marcus, A. How the Success of Open Access Publishing Can Stimulate Improved Access to Grey Literature [online]. Urban Library Journal. 2007. Vol. 14, No. 1. Accessed 21 October 2012. Available at <http://ojs.cunylibraries.org/index.php/ulj/article/view/36/61>.

26 Budapest Open Access Initiative (2002), Bethesda Statement on Open Access Publishing (2003) and Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities (2003).

27 See infra for details.

28 VELTEROP, Johannes. Open Access Publishing and Scholarly Societies – A Guide. New York: Open Society Institute. 2005. Available at <http://www.opensocietyfoundations.org/openaccess/pdf/open_access_publishing_and_scholarly_societies.pdf>, p. 6.

29 BARGHEER et al. In: SPINDLER, Gerald (Ed.) Rechtliche Rahmenbedingungen von Open Access-Publikationen, Göttinger Schriften zur Internetforschung, Band 2, Universitätsverlag Göttingen, 2006. Available at <http://univerlag.uni-goettingen.de/OA-Leitfaden/oaleitfaden_web.pdf>, pp. 7-8.

30 On the regulatory aspects of Open Access, see Säcker, FJ (2010). Open Access and Competition Law. Open Access and Competition Law, Vol. 1 (urn:nbn:de:0009-29-27928).

31 The mere access and consumption is not (yet) regarded as a 'use' of the work in the copyright law sense. For the gradual erosion of this concept, see EFRONI, Zohar. Access-right: the future of digital copyright law. Oxford: Oxford University Press, 2011, xxiv, 608 p.

32 Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities. 2003. Available at <http://oa.mpg.de/lang/en-uk/berlin-prozess/berliner-erklarung/>.

33 Also referred to as free or open licences. For a general overview of the legal issues related to open licensing, see Guibault, Lucie; Angelopoulos, Christina (eds.). Open Content Licensing: From Theory to Practice, Amsterdam University Press 2011.

34 For further discussion of the legal nature of the public licences, see GUADAMUZ, Andrés. The License/Contract Dichotomy in Open Licenses: A Comparative Analysis. University of La Verne Law Review. Vol. 30, No. 2, pp. 101-116, 2009. Available at SSRN: <http://ssrn.com/abstract=1372040>.

35 The Digital Peer Publishing Licence has been developed specifically for the purpose of dissemination.

36 See <www.creativecommons.org>.

37 As stated in Art. 3 of the Creative Commons Attribution 3.0 Unported licence. Available at <http://creativecommons.org/licenses/by/3.0/legalcode>.

38 Specifically online, the Creative Commons Attribution and Creative Commons Attribution-ShareAlike are truly Open Access-compliant.

39 Even though this criterion was originally set up on the European level only for photographs, computer programs and databases. See van Eechoud, M (2012). Along the Road to Uniformity: Diverse Readings of the Court of Justice Judgments on Copyright Work. jipitec, Vol. 3 (urn:nbn:de:0009-29-33226).

40 ECJ 16 July 2009, Case C-5/08, Infopaq, [2009] ECR I-06569.

41 Act No. 121/2000 Sb., on Copyright and Rights Related to Copyright and on Amendment to Certain Acts (the Copyright Act), as amended. Full and partly updated official English translation is available at <http://www.mkcr.cz/assets/autorske-pravo/12-AZ_2006_v_AJ.pdf>. Hereinafter referred to as 'CCA'.

42 Both pursuant to the wording of Sec. 2 para 1 of CCA.

43 Quoted from TELEC, Ivo; TŮMA, Pavel. Autorský zákon: komentář. 1. vyd. Praha: C.H. Beck, 2007, p. 18 (author's translation).

44 See Sec. 2 para 2 and 88 et seq. of CCA for the national legislation; and Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, [1996] OJ L 77/20.

45 British Horseracing Board v William Hill Organization, C-203/02 of 9 November 2004; Fixtures Marketing v OPAP, C-444/02 of 9 November 2004; Football Dataco and others v Yahoo! UK, C-604/10 of 1 March 2012; Football Dataco and others v Sportradar GmbH and Sportradar AG, C-173/11 of 18 October 2012.

46 Pursuant to Sec. 88 CCA.

47 Pursuant to Sec. 88a para 1 CCA.

48 Pursuant to Sec. 90 para 1 CCA.

49 Act No. 111/1998 Sb. on Higher Education Institutions. Full and partly updated official English translation is available at <http://www.msmt.cz/uploads/Areas_of_work/higher_education/Act_No_111_1998.pdf>.

50 Not all Member States opted for all of the possible exceptions and limitations as foreseen in Art. 5(2) of the Directive

2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. Official Journal L 167 , 22/06/2001 P. 0010 – 0019. For a comparative overview, see GUIBAULT Lucie. Why Cherry-Picking Never Leads to Harmonisation: The Case of the Limitations on Copyright under Directive 2001/29/EC. jipitec, Vol. 1 (urn:nbn:de:0009-29-26036).

51 For example, the Masaryk University operates the Repository of Theses at <ttp://is.muni.cz/thesis/?lang=en>. All the defended theses are available in full-text.

52 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society Official Journal L 167 , 22/06/2001 P. 0010 – 0019.

53 Ministerstvo kultury ČR. Stanovisko Samostatného oddělení autorského práva Ministerstva kultury k aplikaci § 47b zákona o vysokých školách č. 111/1998 Sb. 11. 6. 2006. Available at <http://www.msmt.cz/vzdelavani/stanovisko-mk-k-aplikaci-47b-zakona-o-vysokych-skolach>. Accessed 15 June 2013.

54 For general info about the ISP liability in Czech Republic, see POLČÁK, Radim. The legal classification of ISPs: The Czech Perspective. Journal of Intellectual Property, Information Technology and E-Commerce Law. 1 (2010) JIPITEC 172. Available at <http://www.jipitec.eu/issues/jipitec-1-3-2010/2795/polcakisp.pdf>. Accessed 15 June 2013.

55 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. Official Journal L 167 , 22/06/2001 P. 0010 – 0019.

56 HUSOVEC, Martin. Zodpovednos poskytovate a za obsah diskusných príspevkov. Revue pro právo a technologie. Vol. 2, Issue 2, 2011, pp. 40-42. ISSN 1804-538.

57 Judgement of the High Court in Prague from 2 March 2011. File No. 3 Cmo 197/2010 – 82.

58 E.g. full name, date of birth, and locale of the author (i.e. birthplace and/or workplace of the author). However, some GL may also contain data of a very sensitive nature – e.g. salaries – as is the case in the scientific reports.

59 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

60 Act No. 101/2000 Sb., on the Protection of Personal Data and on Amendment to Some Acts, as amended. Full and updated official English translation is available at <http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&lang=en>.

61 Position of the Office for Personal Data Protection No. 3/2012 - On the Notion of Personal Data. Available in Czech at <http://www.uoou.cz/files/stanovisko_2012_3.pdf>.

62 Unlawful processing of personal data is an administrative offence that is punishable by significant financial fines (up to CZK 10,000,000) according to Chapter VII of the PDPA.

63 Again the Czech law relies heavily on Article 2(e) of the Personal Data Protection Directive: Sec. 4(j) PDPA: 'controller' shall mean any entity that determines the purpose and means of personal data processing, carries out such processing and is responsible for such processing. The controller may empower or charge a processor to process personal data, unless a special Act provides otherwise.

64 Also in this case, the Czech law relies heavily on Article 2(e) of the PDPD: Sec. 4 (k) PDPA 'processor' shall mean any entity processing personal data on the basis of a special Act or authorisation by a controller.

65 The latest available version of the proposed regulation is the compromise text of the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2012/0011 (COD). 10227/13. Available at <http://register.consilium.europa.eu/pdf/en/13/st10/st10227-ad01.en13.pdf>.

66 For a general overview, see COSTA, Luiz. Poullet. Privacy and the regulation of 2012. Computer Law & Security Review. Volume 28, Issue 3, June 2012, pp. 254-262, ISSN 0267-3649, 10.1016/j.clsr.2012.03.015. (http://www.sciencedirect.com/science/article/pii/S0267364912000672) and DE HERT, Paul; PAPAKONSTANTINOU, Vagelis. The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals Computer Law & Security Review. Volume 28, Issue 2, April 2012, pp. 130-142, ISSN 0267-3649, 10.1016/j.clsr.2012.01.011. Available at <http://www.sciencedirect.com/science/article/pii/S0267364912000295>.

67 Regarding the types of documents, the Czech NRGL distinguishes between author works (preprints, papers); trade literature (annual reports, product catalogues, manuals); conference materials (posters, presentations, collections, programmes, papers); university qualification works (bachelor, master, dissertation and habilitation theses); course materials (curricula, exam topics, lecture notes, course texts); reports (research, annual, final, technical, study reports); studies; analyses; statistics. See PEJŠOVÁ, Petra. The development of grey literature in the Czech Republic. In: PEJŠOVÁ, Petra (ed.). Grey literature repositories. Zlín: VeRBuM, 2010. 156 p. Available at <http://nrgl.techlib.cz/images/Book.pdf>. ISBN 978-80-904273-6-5>, p. 37.

68 POLČÁK, Radim. ŠAVELKA, Jaromír. Digitální zpracování tzv. šedé literatury pro Národní úložiště šedé literatury. 2009. Available at <http://invenio.nusl.cz/record/111528/files/idr-284_1.pdf>. Accessed 15 June 2013.

69 SEYMOUR, Deni J. Sanctioned Inequity and Accessibility Issues in the Grey Literature in the United States. Archaeologies Journal of the World Archaeological Congress. 2010. 6(2). p. 233-269. DOI 10.1007/s11759-010-9144-6. p. 261.

70 So far more than four hundred institutions have signed the Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities. See <http://oa.mpg.de/lang/en-uk/berlin-prozess/signatoren/>. Accessed 15 June 2013.

71 SCHÖPFEL, Joachim. Access to European Grey Literature. In: PEJŠOVÁ, Petra (ed.). Grey literature repositories. Zlín: VeRBuM, 2010. 156 p. Available at <http://nrgl.techlib.cz/images/Book.pdf. ISBN 978-80-904273-6-5>. p. 20. Accessed 15 June 2013.

Injunctions against Innocent Third Parties:

The Case of Website Blocking

by Martin Husovec, Doctoral Fellow at International Max Planck Research School for Competition and Innovation at Max Planck Institute for Intellectual Property and Competition Law in Munich.

Abstract: The paper discusses the phenomenon of injunctions against third parties that are innocent from the tort law perspective. One such type of injunction, website blocking, is currently appearing in the spotlight around various European jurisdictions as a consequence of the implementation of Article 8(3) of the Information Society Directive and Article 11 of the Enforcement Directive. Website-blocking injunctions are used in this paper only as a plastic and perhaps also canonical example of the paradigmatic shift we are facing: the shift from tort-law-centric injunctions to in rem injunctions. The author of this paper maintains that the theoretical framework for the latter injunctions is not in the law of civil wrongs, but in an old Roman law concept of 'in rem actions' (actio in rem negatoria). Thus the term 'in rem injunctions' is coined to describe this paradigm of injunctions. Besides the theoretical foundations, this paper explains how a system of injunctions against innocent third parties fits into the private law regulation of negative externalities of online technology and explores the expected dangers of derailing injunctions from the tracks of tort law. The author's PhD project – the important question of the justification of an extension of the intellectual property entitlements by the in rem paradigm, along with its limits or other solutions – is left out from the paper.

Keywords: Injunctions; Third Parties; InfoSoc Directive; Tort Law; In Rem actions; Enforcement Directive; Liability of ISPs; Intermediaries

Recommended citation: Martin Husovec, Injunctions against Innocent Third Parties: The case of Website Blocking 4 JIPITEC, 2, para. 116.

A. European Union law

1 The last two years in Europe were marked by an interesting growing enforcement practice of privately litigated website blocks. In more than eight European jurisdictions, various blocking orders were reportedly issued.[1] The website-blocking cases are usually civil proceedings of private plaintiffs holding copyright or trademark rights against the Internet access providers, who as defendants are asked to employ certain technical means to make the access to disputed websites more difficult for its subscribers (an uncircumventable website block is technically impossible). In these cases, the plaintiffs invoke injunctions against Internet access providers who are *not* liable in terms of tort law. The vehicle used to receive such injunctions is the national implementation of Article 8(3) of the InfoSoc Directive (for copyright and related rights) and the third sentence of Article 11 of the Enforcement Directive (for other intellectual property rights).

I. Injunctions against intermediaries

2 The wording of the relevant part of the provision of the Enforcement Directive reads:

> *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.*

3 Article 8(3) of the InfoSoc Directive is identical. The only change is a reference to 'copyright or related right' instead of 'intellectual property right' at the end of the sentence. Practical consequence s of these two provisions were rather latent until very recently. A common reading of Article 11 was based on recital 23:

> *Without prejudice to any other measures, procedures and remedies available, rightsholders should have the possibility of applying for an injunction against an intermediary whose services are being used by a third party to infringe the rightsholder's industrial property right.* **The conditions and procedures relating to such injunctions should be left to the national law of the Member States.**

4 EU Member States thus implemented various conditions enabling such injunctions against intermediaries whose services are used by third parties to infringe intellectual property rights. It was by no means clear whether the injunctions should disregard the tort law boundaries at all. This common reading, however, was recently challenged by a decision of the Court of Justice of the European Union in *L'Oreal v eBay* C-324/09. In this case, the Court faced this question:

> *[This] provision requires the Member States to ensure that the operator of an online marketplace may,* **regardless of any liability of its own** *in relation to the facts at issue, be ordered to take, in addition to measures aimed at bringing to an end infringements of intellectual property rights brought about by users of its services, measures aimed at preventing further infringements of that kind.*

5 CJEU used a contextual reading of Article 11 to point out that injunctions against intermediaries stipulated in the third sentence differ from 'injunctions which may be obtained against infringers of an intellectual property right' (injunctions against infringers) as stipulated in the first sentence of the very same provision (para 128). From how CJEU rephrased the submitted question (above), it becomes clear that the Court does not intend to limit injunctions by any liability in the tort law. One could argue that injunctions against infringers refer only to direct infringers, i.e. persons who themselves act against the scope of the right, and thus injunctions against intermediaries can as a separate category require a secondary liability in the tort law; however, from reading the subsequent paragraphs of the judgment (paras 134, 144) this becomes rather unconvincing. The European Commission also seems to have a clear reading of this provision that goes exactly in this direction. In the official report on the application of the Enforcement Directive,[2] it *inter alia* says the following:

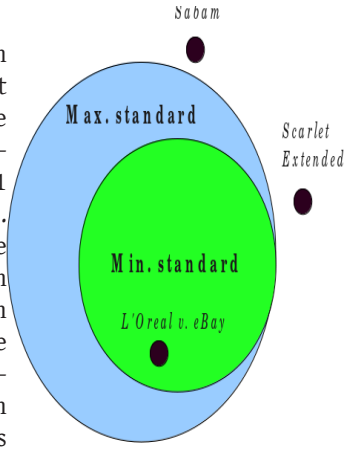
> *[...] it appears that in some Member States it is not possible to issue injunctions unless the liability of an intermediary is established. However,* **neither Article 11** *(third sentence) of the Directive,* **nor Article 8(3)** *of Directive 2001/29* **link injunctions with the liability of an intermediary.** *[...] Injunctions against intermediaries are not intended as a penalty against them, but are simply based on the fact that such intermediaries (e.g. Internet service providers) are in certain cases in the best position to stop or to prevent an infringement.*

6 Last but not least, in the *Frisdranken* case (C-119/10) Advocate General Kokott presented an identical reading of Article 11 of the Enforcement Directive, when opining that in order to trigger such injunctions,

> *it suffices that the [infringing] use of the sign displayed on the cans can be attributed to the client of the intermediary [...] in contrast to the sanction applicable where an intermediary infringes a trade mark, the third sentence of Article 11 of Directive 2004/48 does not provide for damages, these can be obtained in accordance with the national provisions governing participation in a tort or delict – in particular as accessory – in the trade mark infringement committed by the client. However, as a rule, negligence alone is unlikely to suffice for the purposes of establishing participation. (para 39 of the Opinion)*[3]

II. Consequences

7 This interpretation creates an interesting situation. On the one hand, the conditions for issuing such injunctions are up to Member States to create. On the other hand, the CJEU indicates that they are provided irrespective of the intermediary's liability. Because intermediaries often do not act within the scope of the right, their negative externalities are regulated only by secondary liability doctrines.[4] Despite the efforts of the CJEU,[5] however, secondary liability is still perceived as a domain of the national law. In other words, injunctions have to be provided irrespective of something that is not defined. Member States thus don't have a common line which these injunctions should overstep. As a consequence, in a country with no or very limited secondary liability, injunctions against intermediaries can in great part also fulfil functions of the missing or underdeveloped domestic tort law (without compensation claims, of course). In the country with broad secondary liability on the other hand, the injunctions can act as a real and visible entitlement extension.



8 The natural question to ask in this context is where exactly the minimal standard required by Article 11 of the Directive lies. The Court of Justice of EU in its decision says that although 'the rules for the operation of the injunctions for which the Member States must provide under the third sentence of Article 11 of the directive, such as those relating to the conditions to be met and to the procedure to be followed, are a matter for national law', those *'rules of national law must be designed in such a way that the objective*

pursued by the directive may be achieved' (para 135, 136, *L'Oreal v eBay).* The CJEU then concludes that 'measures concerned must be effective and dissuasive'. This means that EU Member States are free to create their own requirements for injunctions against intermediaries only within a certain room that is limited by the *minimal standard* of 'effective and dissuasive measures' and the *maximal ceiling* set by Article 3 of the Enforcement Directive.[6] It remains to be seen how big this room for the Member States is and how close the minimal standard and maximal standard actually are. What we know today is only that injunctions in *L'Oreal v eBay* were seen as a part of the minimal standard and that injunctions in *Sabam* C-360/10 and *Scarlet Extended* C-70/10 were found to go beyond the maximal admissible ceiling. And this brings us back to our case of website blocking. The currently pending case of UPC Telekabel Wien C-314/12 is trying to resolve whether website blocking injunctions are compatible with the maximal standard of the Enforcement Directive. If the CJEU views website blocking as compatible with the maximal standard, the question remains whether it is also part of the minimal required standard, or only an option for the Member States to implement.

B. Paradigm of *in rem* injunctions

9 Article 8(3) of the InfoSoc Directive and Article 11 of the Enforcement Directive thus stipulate an instrument that is difficult to understand with a pure tort law mind-set. This can also be seen from the quoted official report of the European Commission that explains that these injunctions 'are not intended as a penalty against [intermediaries], but are simply based on the fact that such intermediaries [...] are in certain cases in the best position to stop or to prevent an infringement'. The tort law is not about cooperation, however, but compensation. Thus the possibility of injunctions against non-infringing persons (intermediaries) as well might seem a conceptually unexplored concept. And partially it is. In this paper, however, I argue that for civil law jurisdictions,[7] strong theoretical foundations for this paradigm of injunctions can be found outside of the intellectual property law, in the system of protection of tangible property in some civil law countries. The concept to which I refer to as in rem injunctions.

I. *In rem* actions

10 Injunctions with in rem character were originally a civil law doctrine.[8] It developed from the Roman law concepts of rei vindicatio and actio negatoria as a complex way of protecting tangible property.[9] In rem injunctions today represent a separate system of the tangible property protection with its own scope and characteristic features. This system of *injunctive protection* operates independently next to other two systems of property protection, i.e. *tort law* and *unjust enrichment*.

11 In Roman law, one of the in rem actions was particularly important. It was called rei vindicatio, i.e. a legal action by which the plaintiff demands that the defendant return a thing that belongs to the plaintiff. Rei vindicatio, as opposed to the common law concept of conversion, did *not* rely on any tortuous obligation that arose in the meantime between plaintiff and defendant, but on the rightholder's exclusive legal power over the tangible object of protection (res).[10] Such an action would thus focus on a factual situation of disharmony between law and reality, not on a person and his conduct that led to that situation. Common law, on the other hand, would rely on a tort of conversion focusing on a *person* who triggered the situation and *hois conduct.*[11] This conceptual difference yields different results in some cases. For instance, if a ball is blown into a garden by the wind, under rei vindicatio, the owner of the garden automatically has a legal duty to provide the ball back to its owner. Under the tort of conversion, as long as the garden owner doesn't know about it, such a legal duty cannot arise. It will arise only after he learns about the situation and subsequently does nothing, which as a voluntary action (omission) will qualify him for such liability in a tort and thus create an obligation upon which the plaintiff can then rely.[12]

12 Of course, Roman law did not use these concepts as we know them today in some countries (e.g. France, Germany, Austria and Slovakia). However, an important understanding of the in rem claim already existed. This understanding was later extended to actio negatoria, i.e. a legal action by which the plaintiff demands that the defendant refrain from disturbing his property (system of injunctions). In fact, actio negatoria and rei vindicatio can be seen as one system of complex injunctive protection of a tangible property.[13] However, some countries (e.g. France) with an in rem understanding of rei vindicatio would rather use a tort-law-centric approach to actio negatoria. This means that they will focus on a person and his conduct to trigger injunctions, not on a situation. And such person will be defined by the external tort law system. In other countries, however, actio negatoria would be firmly established as an in rem action (Germany, Austria and Slovakia).[14] These countries would thus not only protect against those who disturb property by their conduct (disturber-by-conduct), but also against those who disturb it by their mere status (disturber-by-status), such as being the owner of a garden where a ball was blown by the wind. This extended radius of addresses of injunctions to disturbers-by-status is one of the consequences of this concept, that is of our interest here. Although it might seem that all disturbers-by-con-

duct will be covered by tort-law-linked injunctions, it is not necessarily the case (see below).

13 The core distinguishing feature between a tort-law-centric view of injunctions and in rem injunctive protection, therefore, is the notion of an 'action in rem' as a remedy of law of property and not law of torts. As Professor Maduro explains,[15] at the core of an action in rem is a right in rem as a direct power over the res (thing) that can be raised *erga omnes* and not an obligation involving a specific debtor. If one can say that such a right entails an 'obligation', it is merely an obligation on the whole world not to interfere with it without the consent of the owner.[16] In the right *in rem*, the power of the owner over the thing is central – the power to the exclusion of all unauthorised interference with that res (thing). In the right in personam, on the contrary, it is the legal obligation that binds specific persons which is central, e.g. tort law obligations.[17] Therefore, in an action in rem relating to immovable property, the plaintiff invokes the right *to establish* its extent, content, possible charges, servitudes or other restrictions that may limit it and to protect the estate against any interference incompatible with the prerogatives inherent to his right. As Professor Maduro states in his opinion in the *ČEZ* C-343/04 case:

> *Putting an end to interference with property is possible in the private law of most European legal systems, not only through actions* in personam*, but also through actions* in rem *[...][18] in most legal systems in continental Europe the protection of property rights can be achieved through actions that have the res and the right over it as their immediate object.[...] for instance, with the* actio negatoria*, which is well known namely in Germany, Italy and also in Austria [...], by which the owner of the land asserts its freedom from foreign interference that would otherwise amount to a servitude, charge or limitation to his right of ownership.*

14 A common law understanding of in rem actions greatly differs and is more of a procedural nature. It derives its meaning from the fact that the lawsuit targets only an object, without naming any real person as a defendant.[19] It is thus possible that an action in rem, under a common law understanding, is in fact a regular in personam action in a civil law system,[20] and that an action in rem in a civil law system is an in personam action for common law lawyers. For instance, website blocking is a regular in personam action under a common law understanding, but for a civil law lawyer, as I suggest, it should be seen as an in rem action, because it in fact asserts a freedom from foreign interference that would otherwise amount to a limitation to the right of ownership, without assessing any wrongfulness. Although Professor Maduro states that 'other European legal systems [...] unfamiliar with actions such as the actio negatoria [...] are able [...] to arrive at equivalent final results in terms of protection of immovable property through legal institutions that place emphasis instead on the conduct of the person responsible for the interference', it is not always the case. Injunctions against innocent third parties (in a tort law sense) are one of such examples.[21]

II. Different paradigms of injunctions

15 When I speak of a tort-law-centric view of injunctions, I do not intend to say that injunctions are necessarily seen as a monolithic remedy of law of torts in respective countries. What I mean to say is that they are *not* seen as a remedy materializing the right that originates directly in the source of the right, but rather as a cause of action defined by an external system - the tort law. I also use this term only as a prototype for other absolute rights, regardless of whether they are considered to be a part of property or not (e.g. personality rights). Injunctions in the property law in various countries oscillate between a remedy from the law of property and a remedy from the law of torts. Helmut Koziol, for instance, writes[22] that

> *[...] it is almost generally accepted that the primary aim of tort law is the compensation of loss suffered by the victim. As far as I am aware, the widespread opinion is that injunctions are not a subject of tort law and that they need fewer requirements than claims for compensation.*

16 Depending on the legal system, one of the obvious less strict requirements Koziol refers to is that damage or fault, unlike in the law of torts, is not required to trigger injunctive relief.[23] In other countries, injunctions are furthermore not limited by the tort law notion of delictual capacity of persons.[24] Or even in some countries, injunctions would not be considered pure obligations but legal relationships *sui generis*, with a different applicability of certain rules of the law of obligations (e.g. inapplicability of rules on prescription or rules on discharge from the obligation by a subsequent impossibility, etc.).[25]

17 This concept is nicely described by Willem H. van Boom, who in a different context writes

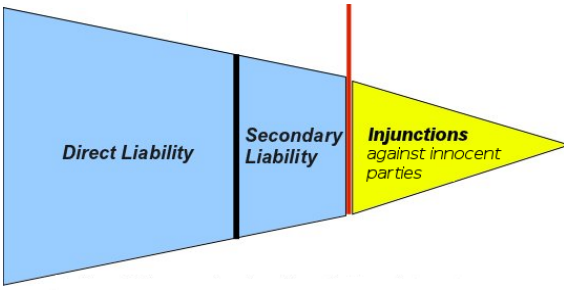
> *[...] it is theoretically conceivable to consider prohibitory injunction as a totally separate response to infringement of property rights, which would link injunctive relief as a procedural sequel to ownership (*actio negatoria*,* rei vindicatio*) and* **would leave issues of wrongfulness untreated** *[emphasis mine].*

18 Although van Boom views injunction as a procedural instrument here, which is a bit counter-intuitive for countries that view injunctive relief as a substantial law remedy, his quotation unveils an important paradigm: that injunction is seen as a remedy directly supporting a legal right of a private individual rather than as a sanction for wrongful behaviour.[26] The remedy thus aims at putting factual reality in harmony with its legal template, not at punishing for any conduct.

19 In a tort-law-centric understanding, on the other hand, injunction is understood as an in personam claim, i.e. an injunction against the specific person who qualified himself for such liability by his *personal conduct*. Although an injunction will not require damage, it will often be dependent on the wrongfulness of the act as defined by tort law (an external system). Hence it will focus on the categories of direct infringers and secondary infringers to define the group of persons against whom the action can be brought. As I said before, this is different for in rem injunctions that focus on a situation of disharmony between the factual and legal and which needs to be solved. Persons are taken into account only as an important element when considering the practicability and proportionality of issuing such injunctions. This is especially true because the principle of *ad impossibilia nemo obligatur* – i.e. nobody is required to achieve the impossible – also has to be respected here.

III. Importance

20 The concept of in rem injunctions realizes *de iure* the exclusivity of the right of a person to the protected object (res) by enabling enforceability against everyone. With the tort-law-centric system of injunctions, the right is naked (not enforceable) in certain situations, although *de iure* its exclusionary power is effective towards all (*erga omnes*). The concept *de facto* creates an additional layer of injunctions that are provided on the top of what the regular systems with tort law's secondary liability doctrine would gave us. In tort law terms, it gives us a power of injunctions provided against persons who are not only primary and secondary infringers, but also those who are non-infringing (innocent) in a tort law sense. The remedies landscape in such a system looks as seen below (please note: in rem injunctions also cover direct and secondary liability; the picture just shows the entitlement extension in yellow).



21 The picture above depicts a remedy landscape in some civil law jurisdictions mostly in regard to a property over *tangible objects*. The enlargement of this system of protection to other absolute rights, such as intellectual property rights, is not so obvious. This extension cannot be merely mechanical and requires a deeper justification debate because in rem paradigm, by extending the enforceability of the right, also extends the property entitlement. Thereby encroachment upon the constitutional principle of 'everything which is not forbidden is allowed' occurs. Maybe this is the reason why even some European countries (e.g. Austria) with a strong culture of in rem injunctions in a tangible property (§§ 364(2), 523 ABGB), did not *initially* extend it to the protection of other absolute rights such as intellectual property. The injunctive protection for intellectual property would be rather closely linked to the tort law, and its scope mostly depends on the tort law concepts of tort feasors (primary or secondary infringers).[27] Other countries (e.g. Germany) would also extend in rem injunctions (§ 1004 BGB) outside of tangible property protection, though with such adjustments to its scope and nature that bring it again very close to the tort law system (namely, the tort of negligence for a third party wrongdoing).

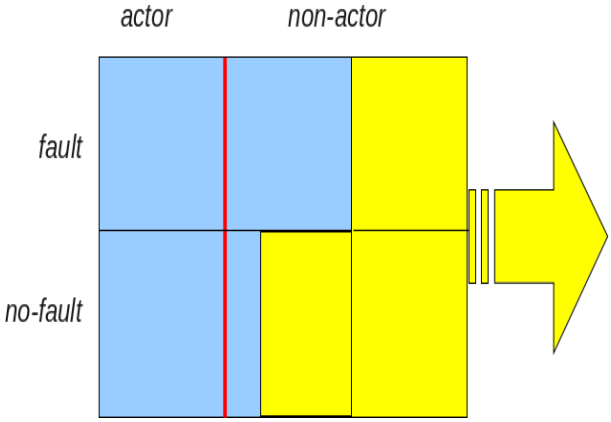
IV. Examples

22 Germany and Austria also demonstrate that there is no common understanding of how far such injunctions can extend and what exactly are its preconditions.[28] In Germany, the scope is wider for tangible property than for intellectual property. The scope of injunctions is limited by the notion of a 'disturber' (§ 1004 BGB), which is more broad than the tort law notion of a 'tort feasor'. A disturber in tangible property law can be anybody who either caused a disturbance of the property by his own conduct (disturber-by-conduct) or who causes such a disturbance by a third party in an adequate way, provided that it is possible and reasonable for him to prevent this action (disturber-by-status).[29] The same notion of the disturber was extended to intellectual property law,[30] but at the same time was narrowed in its scope by requiring a certain breach of duty of care. This duty of care, however, is arguably broader than the usual tort law standards of duty of care known from other jurisdictions.[31]

23 In Austria, the scope in the property law seems even broader than in Germany. According to the Austrian Supreme Court, injunctions extend not only to the person who caused the disturbance of the property by their own conduct (disturber-by-conduct), but also to any person having the factual and legal possibility to stop the disturbance (disturber-by-status).[32] This notion of injunctions was recently also extended to the protection of personality rights.[33] Interestingly enough, it seems, that although in rem injunctions are not similarly established in intellectual property law where a injunctions are linked to tort liability,[34] Austrian law here allows injunctions outside of the tort law categories as an implementation of the above-mentioned topic-tailored Union law against intermediaries.[35]

V. Summary

24 In summary, whereas in rem injunctions aim at solving the situation of disharmony between a factual situation and legally granted rights irrespective of wrongfulness, the tort-law-centric view of injunctions concentrates more on the personal wrongful conduct (what stems from the sanctional nature of the law of torts). In rem injunctions assume that the scope of the enforcement of a right is broader than the scope of a right, an assumption which is in fact also shared by secondary liability in tort. However, whereas the law of civil wrongs extends enforcement beyond the scope of the right only exceptionally (as defined by doctrines of secondary liability), in rem injunctions make the enforceability a general rule, to which we have to craft exceptions in the form of (external) enforcement limits. This entitlement extension is then visible to us (see diagram)[36] as injunctions against innocent third parties.



C. Website blocking injunctions

25 The recent demand of right holders for website-blocking injunctions shows that exclusionary protection of the absolute rights by tort law categories can in certain situations *fail*. This is especially the case where it is impossible or impracticable to identify or sue any of the tort-liable persons due to the cross-border context, the anonymity of tort feasors or merely due to enforcement inefficiency (e.g. massive scale). After all, the tort liability of a non-actor (in the sense of the scope of the right) for an actor's conduct (see diagram above) has its limits based on generally accepted principles of tort (e.g. causality, fault). What right holders see, however, is that there are certain persons in the infrastructure of the Internet economy who have technical and legal means and resources to reduce negative externalities impacting upon their rights, but are too far for the tort law (e.g. Internet access providers).

26 One way of answering their demand for a solution is by rejecting it with the argument that the fact that rights are in some cases practically unenforceable should be seen as an intentional limitation of their entitlement (e.g. similar to copyright exceptions when it comes to the scope of the right, here the limitation applies to the scope of its enforcement). Another way of answering their demand is to undertake a thorough analysis as to whether the extension of such a right is *justified*. However, the reality of the legislative process and of judicial activism does not follow this approach; therefore, with the Union law legislation explained above, we are already asking this questions *ex post*. But as I stated at the very beginning, the issue of justification exceeds the scope of this paper. Instead, I will try to illustrate some of the problems of the website-blocking practice as a type of in rem injunction that might be typical for the entire concept, which leads to injunctions against innocent third parties.

I. Effectiveness

27 In theory, website blocking could yield more economically efficient results. This presumes, first, that the *situation of the right holder* will substantially improve, and second, that the *situation for the rest of the society*, including that of Internet access providers, will worsen to a lesser extent (called the Kaldor Hicks improvement[37]). If this equation does not hold, we cannot speak of any improvement because society pays more than it receives by allowing such a practice. The UK judge Justice Arnold granted his first website-blocking injunction in the *Newzbin II*[38] case, arguing that

> *[i]f, in addition to paying for (a) a Usenet service and (b) Newzbin2, the users have to pay for (c) an additional service for circumvention purposes, then the cost differential between using [an unlawful service] and using a lawful service [...] will narrow still further. This is particularly true for less active users. The smaller the cost differential, the more likely it is that at least some users will be prepared to pay a little extra to obtain material from a legitimate service*

28 Justice Arnold thus sees the effectiveness of website blocking in raising transaction costs for users demanding unlawful services. A recent empirical study[39] conducted by IViR, however, suggests that the impact of website-blocking injunctions in copyright cases, and thus the overall effectiveness of injunctions that underlie its justification, might be very small. According to the study, only 5.5% of all customers (approximately 20% of all *infringing* customers) of affected Internet access providers downloaded less, or stopped downloading altogether, due to website block of The Pirate Bay in the Netherlands. It seems, however, that in Justice Arnold's view, the improvement of the situation of rights holders (the effectiveness of the measure) did not have to be particularly high. This is demonstrated by his comment that 'I agree with counsel for the Studios that the or-

der would be justified even if it only prevented access to Newzbin2 by a minority of users'.

29 It should be noted that what applies to copyright does not necessarily apply to other intellectual property rights, especially trademarks. This is because the copyright-infringing content is very often demanded by users, whereas trademark-infringing goods are demanded less often (as trademark law often protects consumers in parallel). Thus users who have to circumvent blocked websites in order to access them might have a higher incentive to overcome barriers (and pay more in transactions costs) when it comes to copyright-protected content that is being blocked, than content infringing upon trademarks.

II. Methods

30 Furthermore, it has to be noted that the technique of website blocking as such, not just the subject matter concerned, has a lot to do with the effectiveness of such measures. Currently, there are three techniques used to block access to certain websites.

- The first and most primitive is *DNS blocking,* where the Internet access provider merely black-lists certain domain names from its DNS records. This technique can be easily circumvented by both users and targeted website operators. Users need only to use a different provider as a source of DNS records, which is a trivial setting in the Internet browser, or by simply using search engines instead of direct URL entry.[40] A website operator, on the other hand, can change the name of the domain name. This type of block, for instance, was issued by a Danish court in *IFPI Denmark v Tele2* to block <allofmymp3.com>.

- The second method is *IP address blocking*, where an Internet access provider black-lists certain IP addresses used by the server where the targeted website is stored (used in *Dramatico*). This technique is relatively more difficult for users to circumvent. They would need to use a special proxy service or VPN to go around this block. The website operator can change his IP address.

- The last technique is called Deep Packet Inspection (DPI), which, unlike the previous two techniques, enables blocking certain URLs in addition to entire webpages. This method is used when the targeted service shares an IP address with other services, or if the specific part of the website is to be blocked (also used in the UK *Newzbin II* decision). The most significant disadvantage to Deep Packet Inspection is that it may be easily subverted if the packets are encrypted, e.g. using the 'https' protocol.[41]

31 Apart from these technical methods, one has to distinguish whether the website block is issued by the court as a *fixed order* or as an *open order*. The first means that only the decision-specified domain name, website or IP address will be blocked, whereas the second creates an out-of-court system enabling flexible submission of changed IP addresses or domain names by right holders, often without further judicial review. All these different techniques and types of orders raise numerous problems (see below).

III. Collateral damage

32 Assuming that the combination of different techniques and appropriate subject matter makes website blocking effective and hence improves the situation of the right holders, we should ask whether the situation for the rest of society is worsened only to a lesser extent. Plus, the cumulative effects of other website blocks originating from other right holders should also be taken into account. Website blocking especially raises the problem of respect towards the core values of the democratic society and also of public interest in innovation. This potential *collateral damage* can in fact reduce the practical societal need for injunctions against innocent third parties, like website blocking, to zero.

33 Website blocking can easily lead to a practice where the website operators whose websites are to be blocked cannot defend themselves before the block is granted and without having a remedy to challenge such blocks *ex post.* Although it might be more efficient to block the website without notifying the website operator and giving him chance to defend his case, our values embodied in a right to a fair trial shall preclude such scenarios. This is exactly the problem with most of the UK website-blocking injunctions as well. Of all three UK website blocks (*Newzbin II*, blocking Newzbin; *Dramatico Entertainment*, blocking The Pirate Bay; and *EMI Records*, blocking KAT, H33T, and Fenopy),[42] only *Newzbin II* was initiated after the court decision against the website operator was issued (*Newzbin I*) and failed to be implemented. In the other two cases, the infringing nature of a website was assessed as a preliminary question. Website operators whose websites were to be blocked were not party to the proceedings and thus could not defend themselves in court.[43] Justice Arnold relied on the following three arguments in his decision in this respect (see para 9-15 of *Dramatico Entertainment*): i) nothing in the legal bases of the injunctive provision requires a court to do so, ii) other courts did the same, and iii) it would be impracticable, or at least disproportionate, to require the website operator to be part of the proceedings. This type of reasoning is not very convincing from a human rights perspective, however.

IV. Right to a fair trail

34 Website-blocking proceedings fall within the scope of Article 6(1) of the European Human Rights Convention because their result is decisive for private rights and obligations (*see Ringeisen v Austria*, No. 2614/65). A website operator's right to engage in commercial activities as well as his property rights or other rights as a private individual can be interfered with by such a blockade. For instance, a right to conduct a business can be limited by the blocking decision, which orders other entities (here Internet access providers) to block access to the business website. The ban concerned is very serious. Unlike a tenant who cannot run his club at some particular place because his landlord was sued for nuisance, the website operator cannot simply relocate somewhere else. His website was found to be infringing *per se*, not only in the context of a certain neighbourhood. Also, a website operator, unlike a tenant against his landlord, has no proper compensation cause of action against the Internet access provider. His website is locally banned for the entire country and he has almost no possibility to challenge it. Moreover, it is only a matter of time before right holders start asking for EU-wide website blocks based either on Brussels I or unitary community rights. The court, therefore, in my opinion, has to have an obligation to provide for a fair trial to all parties that are affected in this way, including a targeted website operator.

35 A website operator's right to a fair trial can be interfered with in two of its components: i) access to the court and ii) equality of arms. The main problem of a website block is not only that the court will not hear the website operator in the proceedings, but also that the website operator has no remedy to challenge the block of his website. The court thus decides *de nobis sine nobis*, i.e. about us, without us. Equality of arms requires that each party be afforded a reasonable opportunity to present its case, including its evidence, under conditions that do not place it at a substantial disadvantage *vis-à-vis* its opponent (*Ankerl v Switzerland*, Case No. 17748/91). The website operator cannot object to evidence or present legal arguments in the assessment whether his service is complying with the law. This sharply contrasts with criminal cases in which even criminals have a right to defend themselves, regardless of how evident their case may be.

36 The Strasbourg Court also reads the set of minimal rights from criminal cases stipulated in Article 6(3) ECHR as the minimum standard in civil cases in the scope of Article 6(1) ECHR. This is known as a right to adversarial proceedings (see e.g. *J.J. v The Netherlands*, No. 21351/93). In principle, this means the opportunity for the parties to a civil trial to have knowledge of and comment on all evidence adduced or observations filed, with a view to influencing the court's decision. If a website operator's website is blocked, the operator is stopped or substantially disadvantaged (circumvented) from conducting business, sharing opinions or exploiting property (for domain names, see *Paeffgen v Germany*, No. 25379/04, No. 21688/05, No. 21722/05).

V. Abuse

37 Furthemore, this constellation of injunctions can easily lead to abuse. Instead of directly suing the website operator or domain name holder, one can without serious resistance sue only the Internet access provider for the website blocking. This happened, for instance, in a recent trademark dispute over HomelifeSpain.com in Denmark.[44]

38 The courts will need to be very sensitive to this. Probably as never before, the remedy as such was vulnerable to the abuse of a right to fair trial, as many of these injunctions are. Based on human rights principles, the courts need to recognize *existing* enforcement limits as a sort of new safe harbour. These principles can be distilled from the Strasbourg case law. For instance, we could formulate the following enforcement limitation embodying the right to fair trial as an instruction for courts:

> *If a result of an injunction is decisive for private rights or obligations of a certain person that is not party to the proceedings, the court must not issue an injunction, unless it will be assured that his right to a fair trial is fully guaranteed.*

39 This type of (external) defence can then be invoked by courts in many other cases, not only in the practice of website blocking. If, for instance, a plaintiff sues only the domain name authority for the cancellation of a certain domain name, the court must not issue any injunction against the domain name authority, unless the right to a fair trial of a domain name owner is sufficiently guaranteed.

VI. Legality

40 Moreover, as a recent ECHR case *Ahmet Yıldırım v Turkey* (Case No. 3111/10) suggests, not only the procedural right of a fair trial might be infringed upon, but also other rights such as freedom of expression. The *Ahmet Yıldırım v Turkey* case also teaches us that the courts should be very cautious about the *scope of a website ban* and *the guarantee of judicial review* to prevent possible abuses. Otherwise, website blocks can clash with a legal principle that the rights have to be proportionate and 'prescribed by the law'. This problem was illuminated in *Scarlet Extended*, where Advocate General Cruz Villalón suggested that forcing a fairly complicated filtering and blocking mechanism requiring Deep Packet Inspection onto an Internet access provider should be rejected *without*

assessing proportionality, due to the fact that the injunction provision *cannot serve as a legal bases* for a very complicated filtering measures that seriously interferes with the right to privacy and freedom of expression. The argument was as follows:

> *[B]oth the Charter and the ECHR acknowledge the possibility of a limitation on the exercise of the rights and freedoms, of an interference in the exercise of the rights or of a restriction on the exercise of the freedoms, which they guarantee on condition, inter alia, that they are 'provided for by law'. The European Court of Human Rights, principally on the basis of the supremacy of law enshrined in the preamble to the ECHR, has constructed from that expression, and essentially through the concept of 'quality of the law', an actual doctrine, according to which any limitation, interference or restriction must previously have been the subject of a legal framework, at least in the substantive sense of the term, which is sufficiently precise having regard to the objective it pursues, that is, in accordance with minimum requirements.[...]* **The 'law' must therefore be sufficiently clear and foreseeable as to the meaning and nature of the applicable measures, and must define with sufficient clarity the scope and manner of exercise of the power of interference in the exercise of the rights guaranteed by the ECHR.** *[...] From the point of view of the users of Scarlet's services and of Internet users more generally, the filtering system requested is designed, irrespective of the specific manner in which it is used, to apply systematically and universally, permanently and perpetually, but its introduction is not supported by any specific guarantee as regards in particular the protection of personal data and the confidentiality of communication.[...] The necessary conclusion is therefore that* **the national law provision at issue cannot**, *in the light of Articles 7, 8 and 11 of the Charter and in particular of the requirements relating to the 'quality of the law' and, more generally, the requirements of the supremacy of the law,* **be an adequate legal base on which to adopt an injunction imposing a filtering and blocking system such as that requested in the main proceedings.** *[emphasis mine]*

41 Despite that fact that the CJEU then ignored this issue and instead rejected blocking and filtering on the merits after carrying out a balancing exercise between the rights concerned, the issue of *quality of the law* has to be taken into account when issuing more complicated website-blocking injunctions, such as those involving Deep Packet Inspection of users' communication. Justice Arnold, for instance, who also instituted this technique of website blocking, first assessed different alternatives of website blocking and their collateral damage on others. Nevertheless, his website-blocking orders are still vulnerable to abuse, because they set up an out-of-court system of non-transparent submission of IP addresses and domain names that are not subject to any further judicial review. One may question whether all the subsequent website blocks are still 'provided for by law' as required by the ECHR. As the number of website blocks will be growing, these court-approved website blocks should have a more strict system of checks and balances, e.g. transparency obligations by Internet access providers or periodic review of the implementation. Moreover, website blocks were so far instituted only via court proceedings. In civil law countries, where injunctions are recognised as remedies exercisable also out of the court, one might ask whether the notion of 'prescribed by the law' does not also impose an obligation to exercise it only before the courts.

VII. Innovation

42 Last but not least, one may ask a question closely linked with public interest in innovation: If the court continues issuing website-blocking injunctions, how much illegality of content would actually be required? Especially disruptive innovations – such as YouTube was some time ago – can be easily prohibited in their early development stages if the bar for the legal content is set too high. In his judgment, Justice Arnold says that '[his] position might be different if Newzbin2 had a substantial proportion of non-infringing content' when discussing whether plaintiffs have to provide specific URLs instead of a full website block.

43 This furthermore opens the question of whether such a 'hard case' should not be preferably addressed in proceedings against the innovator, instead of some unrelated forum between the parties that might have no or even negative interest in defending that particular innovation. For instance, if an Internet access provider is vertically integrated in another market, such as cable TV, it might have negative interest in defending any competing innovation that uses its infrastructure to access consumers (e.g. IPTV). In such cases, an Internet access provider might be willing to block the website because it improves its position in the parallel market.

VIII. Position of the remedy

44 This entire picture of the scope of the injunctions and its human rights problems poses an important question of a *hierarchical position of such a remedy* in our enforcement systems. During the current consultation,[45] right holders strongly advocated for the following action to be taken:

> *[...] make clear that the intermediary's liability (or the violation by the intermediary of any kind of duty) is not a pre-condition to an injunction being issued against him with respect to a third party's infringement.[...] The availability of an injunction against intermediaries should not depend on whether the infringer has or has not been identified; nor should the availability of such an injunction be made subject to an obligation for the rights-holder to sue the actual infringer* **(no rule of subsidiarity)**.*[...] Under appropriate circumstances, injunctive relief against infringers and intermediaries* **should be available irrespective of whether they have received prior notice.** *[emphasis mine]*

45 In other words, injunctions against an innocent third party, in their view, shall be recognised as an independent remedy that should not require any exhaustion of tort liability, i.e. any proof that tort law remedies failed.[46] Although this is consistent with the concept of in rem actions, it can at the same time distort economic rationale behind existing tort remedies. For instance, it is questionable why innocent parties should bear the costs of cooperation, also in cases where negative externalities of technology are

efficiently enough regulated by the tort law instruments (e.g. see the example of 'HomelifeSpain.com' mentioned above).

D. Economic consequences

46 Website-blocking injunctions show several serious problems brought by the expansion of injunctive relief against innocent third parties. The most striking consequences of this paradigmatic shift, however, are concerned with the future of Internet innovation. This is because courts in this system are being turned into *standard-setting bodies*, a function they avoided when they had only secondary liability doctrines at their disposal. Take the domain name registration system as an example. If this system were created today under the current remedy landscape in the European Union, domain name authorities could be arguably theoretically forced to apply an *ex ante* screening system (before registration) instead of an ex post dispute system (after registration). This derives from the fact that secondary (tort) liability doctrines were unable to actively force domain name authorities to change their policy of first-come/first-served registrations (see the *Lockheed Martin v NSI* case[47]). With injunctions against innocent third parties in place, however, one can challenge such policy decisions of providers in times when the system is fragile because it is only being formed. When a system is already established and becomes more solid, the courts are usually more reluctant to change it.[48] This also shows that enforcement limits that were set up to prevent similar dramatic scenarios, such as a prohibition of the general monitoring obligation set by Article 15 of the E-commerce Directive, are usually very narrow rules to protect unexpected innovations.[49] For the future, this all again means that courts can substantially change the innovation in the process of its formation. It also means that courts will now move from a '*rubber-stamping' position* (assessing whether providers did enough to avoid secondary liability) to a more 'standard-setting' position (actively imposing a new conduct standards and associated costs onto providers).[50]

I. Costs

47 The most crucial element in this context is the problem of costs. Shifting the costs from one person to another was so far triggered by *some special reasons* as defined by tort law.[51] The system of in rem injunctions, however, creates a model where costs can be shifted to others only because they have the factual and legal possibility to do something to minimize infringements. Injunctions against innocent parties thus enable a shift of costs *without special reasons.* And the costs involved can often be very high. The initial cost of implementing a website-blocking injunction, for instance, is about £5,000, with another £100 for each subsequent notification.[52] According to current practice, this cost is borne by Internet access providers.

48 The growing blocking practice can hence naturally soon lead to an increased price for Internet access. So it is ultimately consumers who will be paying for this kind of enforcement technique. Similarly, in our theoretical example, if an *ex ante* screening system in respect to domain names were reality, consumers would be the ones who would have to bear the increased costs of compliance forced onto domain name authorities. Innovations can therefore become more expensive. The concerned industry, of course, understands this aspect of injunctions. For industry, the question of injunctions in Europe is becoming more important than liability in tort, especially because existing safe harbours set forth in Articles 12 to 14 of the E-commerce Directive protect them from additional costs possibly incurred by expansion of secondary liability doctrines, but do not protect them from costs resulting from these sort of injunctions.[53] We can illustrate voices of the industry on the example of Yahoo complaints during the hearing about amendment of the Enforcement Directive and debate about Article 11 injunctions:

> *[...] disproportionate injunctions are being imposed by the courts on online intermediaries. Such injunctions are very damaging for online intermediaries, even if they are not, per se, liable.[...]* **For online intermediaries, legal liability** *per se* **is not key, but rather the effect of injunctions on their business.** *Therefore, reassurances from rightholders that injunctions need not be linked to liability are of no comfort if these injunctions cause economic damage and oblige them to take decisions on the legality of content, which would damage the fundamental rights of Internet users.*

49 On the other hand, it is theoretically possible to see injunctions against innocent third parties being issued only on the promise that right holders will pay the implementation costs. Under such circumstances, the issue of special reasons for shifting costs would disappear. This scenario, however, is not explicitly envisaged by the Enforcement Directive[54] and of course is not appealing to the right holders. Justice Arnold probably views this as an exceptional circumstance when he notes, in his first blocking order against British Telecom:

> *I do not rule out the possibility that in another case the applicant may be ordered to pay some or all of the costs of implementation, but for the reasons given above I do not consider that such an order is appropriate in this case.*

50 Soon, competition between the two types of remedies might arise. If injunctions against innocent third parties become cheaper due to little resistance from the defendants, then they will be exploited more often and innocent third parties will eventually often bear costs instead of direct or secondary infringers. Moreover, the pursuit of pure right holder self-interest in enforcement might lead to results that are

not efficient from the societal point of view, i.e. it might lead to market failures.

E. Conclusion

51 As Article 8 of ACTA[55] and other initiatives (BTAs)56 show, injunctions against innocent third parties are definitely a trend of the last years, and the European Union is very active in 'exporting it' outside of the old continent. Website blocking is a manifestation of derailing injunctions from the tracks of tort law in the recent jurisprudence. This phenomenon leads to an extension of rights by extending their scope of enforcement against persons that are too far for tort law, but have resources and factual and legal means to reduce the negative externalities. In this paper I argue that the theory behind such an extension can be found in the Roman notion of 'in rem action'. Also, the justification for such an extension should not be mechanical, but subject to a thorough justification analysis. In this respect, I have tried to demonstrate rising problems in the practice of website blocking, especially tensions with the right to a fair trial, legality and costs of injunctions.

52 Although at first sight, injunctions against innocent third parties might seem to be an effective enforcement tool to supplement the deficiencies of tort law in the online environment, these injunctions are very vulnerable to abuse and have a similarly great potential to negatively influence innovation. In the context of the Internet and intellectual property rights enforcement, derailing injunctions from the tracks of tort law is literally akin to derailing the future of the Internet and its innovation into *unknown waters.* As maybe never so intensively before, this future has been left in the hands of our courts. This article suggests that if we now shift to this new paradigm of injunctions in the IP law, we should also start discussing new positive intellectual property limitations or other checks and balances, not only on the level of the scope of the right but also on the level of the scope of its enforcement.

53 If readers feel at this point that I have merely raised a lot of questions without furnishing proper answers to them on how to address these challenges, they are certainly right to conclude so. I simply don't have the answers. Yet.[57]

(Endnotes)

1 The courts of the United Kingdom (3), Netherlands (1), Belgium (1), Finland (1), Denmark (2), Greece (1), Austria (1) and Italy (2) were reported to issue such injunctions. See more at M. Husovec, European cases on ordering ISPs to block certain websites, Hu□ko Technology Law Blog at <www.husovec.eu/2011/11/european-cases-on-ordering-isps-to.html>. Also L. Feiler, Website Blocking Injunctions under EU and U.S. Copyright Law: Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law? TTLF Working Papers No 13 (concluding *inter alia* that in the US such injunctions are not possible).

2 Report from the Commission to the Council, the European Parliament and the European Social Committee on the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights COM(2010) 779 final.

3 The reference is made to the German doctrine of liability of participator, which is also shared in some other countries such as Slovakia and Austria.

4 In this paper, the term 'secondary liability' means purely tort liability of any person different from the direct infringer (actor), who has to bear the weight of any kind of non-contractual claim for acts of the direct infringer. Secondary liability could be further divided into fault-based secondary liability that requires the breach of a certain duty of care, and no-fault-based secondary liability that triggers liability regardless of such a breach.

5 In the recent Donner case, C-5/11, the CJEU read into the autonomous notion of the 'distribution right' arguably also the test for secondary infringements in para 27 of the decision. The Court states that '[a] trader in such circumstances bears responsibility for any act carried out by him [...] or on his behalf giving rise to a 'distribution to the public' in a Member State where the goods distributed are protected by copyright. [...] Any such act carried out by a third party may also be attributed to him, where he specifically targeted the public of the State of destination and must have been aware of the actions of that third party.' In a different context, Justice Arnold states that 'I can conceive that it might nevertheless be argued that the Trade Marks Directive did approximate national laws on accessory liability in the context of infringement of national trade marks to some extent. It might also be argued that the Community Trade Mark Regulation implicitly regulated the question of accessory liability in the context of infringement of Community trade marks to some extent. In the present case, however, it was common ground between counsel that there was no conflict between domestic law and Community law on this issue if domestic law was properly interpreted and applied in the manner that they respectively contended for. Accordingly, it is not necessary to enquire into the effect of Community law any further' (L'Oreal SA & Ors v EBay International AG & Ors [2009] EWHC 1094 (Ch)).

6 Maximal (standard) ceiling conditions stipulated in Art. 3 require that such injunctions are a) fair, b) equitable, c) not unnecessarily complicated, d) not costly, e) do not entail unreasonable time-limits or unwarranted delays, f) effective, g) proportionate, h) dissuasive, i) do not create barriers to legitimate trade and j) not abusive.

7 n common law, it might be a concept of equitable protective jurisdiction. See footnote 21.

8 In Ireland, the High Court of Ireland, which has the same general statutory jurisdiction to grant an injunction as the English High Court, considering a request for a blocking order (EMI v UPC), held that where there was no primary actionable wrong, the court should not intervene in an area – such as copyright – where the Irish Parliament had legislated (quoted from Davey, F. Blocking access to copyright infringing sites. What would ISP's be required to do? (not published)).

9 See M. Boháček, Actio negatoria k dějinám zápůrčí žaloby, Nákládatelství České Akadémie Věd a Umění, 1938; E. Picker, Der 'dingliche Anspruch', In: Fest Schrift Bydlinski, 2002, 269; E. Herrmann, Der Störer nach § 1004 BGB. Duncker & Humbolt, 1987; R. Wetzel, Die Zurechnung des Verhaltens Dritter bei Eigentumsstörungstatbeständen. Mohr Siebeck, 1971; P. Ch. van Es, De actio negatoria: een studie naar de rechtsvorderlijke zijde van het eigendomsrecht, Wolf Legal Publishers, 2005.

10 H. Honsell, Römisches Recht. Springer, 2010, p. 72; U. Mattei, Basic Principles of Property Law: A Comparative Legal and Economic Introduction. Praeger, 200, p. 183.

11 Ch. K. Sliwka Herausgabeansprüche als Teil des zivilrechtlichen Eigentumsrechts? die rei vindicatio und funktionsäquivalente Ansprüche des Eigentümers gegen den Besitzer im französischen, englischen und deutschen Recht. Logos Berlin, 2012, p. 536.

12 Ibid.

13 E. Picker, Der 'dingliche Anspruch' In: Festschrift Bydlinski, 2002, 269.

14 See para 44 to 48 of the Avocate General's Opinion in ČEZ C-343/04.

15 Ibid.

16 Ibid.

17 Ibid.

18 Similar idea expressed by S. Green, J. Randall, The Tort of Conversion, 2009, Hart Publishing, p. 56 who says that whereas the common law system protects from disturbance via tort law, civil law divides this function between property law and tort law (quoted from Ch. K. Sliwka, Herausgabeansprüche als Teil des zivilrechtlichen Eigentumsrechts, p. 519 (footnote 2144)).

19 An example from IP law is 15 USC § 1125 (d)(2)(a), which reads: 'The owner of a mark may file an in rem civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located if ...'.

20 See L. Collins, The Civil Jurisdiction and Judgments Act 1982, London, Butterworths, 1983, pp. 78-79, pointing out that 'the expression "proceedings which have as their object rights in rem in or tenancies of, immovable property" does not fit with any existing concepts of property law in the United Kingdom'. On the notion of actio in rem under English Maritime Law, see also the opinion of Advocate General Tesauro in Case C-406/92 Tatry [1994] ECR I-5439, point 19 (quoted from ČEZ C-343/04). The decisive part of this decision reads: '[...] However, for the purposes of resolving the present problem, namely identification of the circumstances in which it can be said that two actions have the same cause of action under the Brussels Convention, no importance should in my view be attached to the distinction drawn by English law between actions in rem, by means of which the plaintiff seeks to satisfy his claim by proceeding against specific assets, and actions in personam intended to produce binding effects as between individuals.[...] A similar conclusion was recently arrived at by the Admiralty Court itself, in a judgment of April 1992 in proceedings which in certain respects are similar to those in the present case. Being called on to determine, specifically for the purpose of applying Articles 21 and 22 of the Brussels Convention, whether Netherlands proceedings brought by owners of goods for compensation for damage suffered by a ship's cargo involved the same subject-matter and cause of action as proceedings subsequently commenced by the same owners in the United Kingdom by arresting the vessel under the Arrest Convention, the English court concluded that the two actions involved the same subject matter, notwithstanding the differences between actions in rem and actions in personam. It arrived at that conclusion by reference to the fact that the subject-matter of the action against the ship must necessarily be the same as that of the action against the owner and that, if service of the writ of arrest is not acknowledged by the owner, the plaintiff must, in order to obtain a decision against the vessel, prove the owner's liability'.

21 See UK concept of equitable protective jurisdiction, which was mentioned in L'Oreal SA & Ors v EBay International AG & Ors [2009] EWHC 1094 (Ch) and also in Washburn and Moen Manufacturing Co. v Cunard Steamship Co. (1889) 6 R.P.C. 398 (brought to my attention by Graham Smith). Norwich Pharmacal Co. & Others v Customs and Excise Commissioners [1974] AC 133 applies similar logic in respect to information disclosure: 'UK courts allow to grant disclosure orders, known as Norwich Pharmacal orders, against innocent third parties which have been mixed up in wrongdoing. While first developed in relation to intellectual property, such as patents, Norwich Pharmacal orders are now granted in relation to other torts, as well as defamation and breach of contract, and alleged criminal offences' (quoted from Wikipedia entry on Norwich Pharma injunctions; see more on this issue at <http://en.wikipedia.org/wiki/Norwich_Pharmacal_Co._v_Customs_and_Excise_Commissioners>); The Norwich case cites among others Upmann v Elkan (1871) 7 Ch App 130, where the court allowed an injunction to be issued to restrain an (innocent) mere carrier in possession of counterfeit goods. The case also dealt with his duty as the possessor of counterfeit goods to give all proper information and offer redress.

22 Quoted from van Boom, W. Comparative notes on injunction and wrongful risk-taking, In: Maastricht Journal of European and Comparative Law 1 (2010) 10-31.

23 For the situation in Germany, England and France, see van Boom, W. Comparative notes on injunction and wrongful risk-taking.

24 H. Koziol, Basic Questions of Tort Law from a Germanic Perspective (2012) Jan Sramek Verlag, p. 21 – 26.

25 Ch. K. Sliwka, Herausgabeansprüche als Teil des zivilrechtlichen Eigentumsrechts? die rei vindicatio und funktionsäquivalente Ansprüche des Eigentümers gegen den Besitzer im französischen, englischen und deutschen Recht. Logos Berlin, 2012, p. 536.

26 W. van Boom, Comparative notes on injunction and wrongful risk-taking, p. 6.

27 See K. Lanzinger-Twardosz, Unterlassungsanspruch und Störerhaftung im Immaterialgüterrecht, 2008; Study of European Observatory on Counterfeiting and Piracy on Injunctions in Intellectual Property Rights.

28 H. Koziol, Basic Questions of Tort Law from a Germanic Perspective (2012) Jan Sramek Verlag, p. 21 – 26.

29 The court praxis since the decision of the German Federal Supreme Court, Constanze II, 06.07.1954, Case No. I ZR 38/53; see also K. Gursky, Sachenrecht §§ 985 - 1011 (Eigentum 3), C.H.Beck, Neubearb., 2013, p. 551.

30 German Federal Supreme Court, Internet-versteigerung I, 11.4.2004, Case No. I ZR 304/1.

31 Instructive examples can be found in decisions of the German Federal Supreme Court, Sommer Unseres Lebens, 12.05.2010, Case No. I ZR 121/08 and Alone in the Dark, 12.7.2012, Case No. I ZR 18/11.

32 See decision of the Austrian Supreme Court, 16.12.2008, Case No. 8 Ob 151/08a.

33 See decision of the Austrian Supreme Court, 16.11.2012, Case No. 6 Ob 126/12s.

34 See decision of the Austrian Supreme Court, 19.12.2005, Case No. 4 Ob 194/05s.

35 See the interpretation of § 81 (1a) UrhG in a referral decision of the Austrian Supreme Court, 11.05.2012, Case No. 4Ob6/12d.

36 The diagram illustrates entitlement extension. The blue field represents tort liability and the yellow field injunctions outside the tort law system. 'Actor' refers to a person who acts within the scope of the right (direct infringer). 'Non-actor' refers to person who does not act within the scope of the right (secondary infringer). The picture depicts a tort liability system in a country such as the US, which enables fault-based liability of a non-actor for an actor's conduct in some cases (contributory liability) and also non-fault-based liability of a non-actor for an actor's conduct in some cases (vicarious li-

ability). The yellow field shows the extension of the scope of the enforcement against non-actors. The arrow shows the direction of lowering causal link standards.

37 Kaldor–Hicks efficiency is a measure of economic efficiency. Under Kaldor–Hicks efficiency, an outcome is considered more efficient if a Pareto optimal outcome can be reached by arranging sufficient compensation from those that are made better off to those that are made worse off so that all would end up no worse off than before. See more at <http://en.wikipedia.org/wiki/Kaldor%E2%80%93Hicks_efficiency>.

38 The High Court of Justice, [2011] EWHC 1981 (Ch).

39 J. Poort, J. Leenheer, File sharing 2@12: Downloading from illegal sources in the Netherlands, IViR, available at <http://www.ivir.nl/publications/poort/Filesharing_2012.pdf>.

40 F. Davey, Blocking access to copyright infringing sites. What would ISP's be required to do?

41 Ibid.

42 The High Court of Justice: Newbiz II [2011] EWHC 1981 (Ch); Newbiz II [2011] EWHC 2714 (Ch), Dramatico [2012] EWHC 268 (Ch), Dramatico [2012] EWHC 1152, EMI Records [2013] EWHC 379 (Ch).

43 For the position of users, see M. Husovec, What's wrong with UK website blocking injunctions? Hu□ko's Technology Law Blog at <http://www.husovec.eu/2013/03/whats-wrong-with-uk-website-blocking.html>.

44 The Spanish-owned property site called HomelifeSpain.com was blocked in Denmark after the Danish site home.dk as an owner of a word mark 'home' applied and received the remedy of the website being blocked in Denmark. See more at <http://www.techdirt.com/articles/20121228/09275521510/danish-court-orders-spanish-site-blocked-because-it-uses-trademarked-english-word-home-as-part-its-name.shtml>.

45 See Study of European Observatory on Counterfeiting and Piracy on Injunctions in Intellectual Property Rights .

46 See such an example in a recent Dutch case, BREIN v ING, where the court ruled that the local bank is not required to hand over the information about an allegedly infringing account holder because such a court ruling can only be deployed as a last remedy and the plaintiff had not yet exhausted all other possible options. The case was reported at <http://www.futureofcopyright.com/home/blog-post/2013/05/17/dutch-court-ing-not-required-to-disclose-account-information-in-copyright-case-against-ftd-world.html> and M. Husovec, Are Banks Required to Disclose the Indentity of their Customers to Copyright Holders? Hu□ko's Technology Law Blog at <http://www.husovec.eu/2013/05/are-banks-required-to-disclose.html>.

47 NSI was at the time the sole National Science Foundation contractor in charge of registering domain-name combinations for the top-level domains .gov, .edu, .com, .org and .net. NSI did maintain a post-registration dispute-resolution procedure, but no *ex ante* procedure. NSI took no action on Lockheed's requests to cancel the domain names. NSI later permitted a new registrant to register <skunkworks.com>. Lockheed sued NSI on 22 October 1996, claiming a contributory service mark infringement, infringement, unfair competition, and service mark dilution, all in violation of the Lanham Act, and also seeking declaratory relief. The Ninth Circuit rejected all the claims (Lockheed Martin v Network Solutions, No. 97-56734, United States Court of Appeals, Ninth Circuit).

48 SSee e.g. decision of the German Federal Supreme Court, Ambiente.de, 17.05.2001, Case No. I ZR 251/99.

49 Art. 15 provides that 'Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity'. As domain name authority activity is generally not seen as mere hosting, caching or mere conduit, this provision does not apply to it.

50 Instructive examples can be found in German case law, e.g. the decision of the German Federal Supreme Court, Sommer Unseres Lebens, 12.05.2010, Case No. I ZR 121/08, which pushed for password protection of open wifis, or the Alone in the Dark decision, 12.7.2012, Case No. I ZR 18/11, which pushed for word-filtering technology for file-hosting providers and also for manual review of a small number of external links from search engines.

51 Inspired by H. Koziol, Basic Questions of Tort Law from a Germanic Perspective (2012) Jan Sramek Verlag, p. 31

52 See decision [2011] EWHC 2714 (Ch) Newzbin II, paras 32-53.

53 See the wording of Art. 12(3), Art. 13(2), Art. 14(2), Art. 18 of E-commerce Directive together with the explanation of injunctions against intermediaries. It is also, for instance, the current position of German jurisprudence and from case law that is coming to the Court of Justice of EU from other member states (Scarlet, Sabam, UPC Wien etc.), it seems that this is not an unusual position. Of course, in countries that did not implement Art. 11 of the Enforcement Directive and Art. 8(3) of the Information Society Directive properly, this questions often did not even arise. See Study of European Observatory on Counterfeiting and Piracy on Injunctions in Intellectual Property Rights.

54 Enforcement Directive in Art. 3(1) states that 'Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays'. Also Justice Arnold in Newzbin II opines '[i]t seems to me to be implicit in recital (59) of the Information Society Directive that the European legislature has chosen to impose that cost on the intermediary. Furthermore, that interpretation appears to be supported by the Court of Justice's statement in L'Oréal v eBay at [139] that such measures "must not be excessively costly".' On the other hand, there is no explicit requirement in any of the directives that such costs have to be borne fully by intermediaries.

55 'Each Party shall provide that, in civil judicial proceedings concerning the enforcement of intellectual property rights, its judicial authorities have the authority to issue an order against a party to desist from an infringement, and *inter alia*, an order to that party or, where appropriate, to a third party over whom the relevant judicial authority exercises jurisdiction, to prevent goods that involve the infringement of an intellectual property right from entering into the channels of commerce.' This provision was previously drafted in a more European-style way, when it provided that 'The Parties [may] shall ensure that right holders are in a position to apply for an injunction against [infringing] intermediaries whose services are used by a third party to infringe an intellectual property right.' See more on this development within the treaty, B. K. Baker, ACTA: Risks of Third Party Enforcement for Access to Medicines, PIJIP Research P*aper se*ries (2010).

56 The proposed text of Bilateral Trade Agreement between EU, Colombia and Peru that in Art. 236 says 'the Parties shall provide 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.' As the footnote of the document explains, 'The Parties shall ensure that the measures referred in this paragraph may also apply against those whose services have been used to infringe intellectual property rights to the extent they have been involved in the process.' See <http://www.bilaterals.org/spip.php?article17138>.

57 Hopefully, I will be able to provide these answers at the end of my ongoing PhD research.

Evaluation of the Role of Access Providers

Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time

by Arno R. Lodder and Nicole S. van der Meulen, VU UniversityAmsterdam, Department Transnational Legal Studies Center for Law and Internet, Amsterdam, The Netherlands

Abstract: Internet service providers (ISPs) play a pivotal role in contemporary society because they provide access to the Internet. The primary task of ISPs – to blindly transfer information across the network – has recently come under pressure, as has their status as neutral third parties. Both the public and the private sector have started to require ISPs to interfere with the content placed and transferred on the Internet as well as access to it for a variety of purposes, including the fight against cybercrime, digital piracy, child pornography, etc. This expanding list necessitates a critical assessment of the role of ISPs. This paper analyses the role of the access provider. Particular attention is paid to Dutch case law, in which access providers were forced to block The Pirate Bay. After analysing the position of ISPs, we will define principles that can guide the decisions of ISPs whether to take action after a request to block access based on directness, effectiveness, costs, relevance and time.

Keywords: Internet Service Providers; Pirate Bay; Access Providers, Effectiveness; Costs; Relevance

Recommended citation: Arno R. Lodder, Nicole S. van der Meulen, Evaluation of the Role of Access Providers Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time, 4 JIPITEC 2, para 130.

A. Introduction

1 Traditionally, third parties facilitating communication and information exchange were mere messengers or neutral transporters. As a popular Dutch saying goes,[1] their policy should be to not take notice of the content of messages. Postal services do not open letters, telephone companies do not eavesdrop on communication, and even classic telephone operators simply facilitated the connection. Only with some services is knowledge of the content inherent, as in the case of telegrams and telex.

2 In the early days of the Internet, ISPs still fit into the tradition of communication neutrals. From the moment Internet access was provided to the general public in the early 1990s, however, crime slowly started to take off, and copyright infringements in particular increased quite exponentially. These developments led to a changing role for Internet service providers. No longer could they maintain a completely neutral position.

3 The initial attempts to regulate ISPs, with the prominent examples of the US Digital Millennium Copyright Act (DMCA)[2] and the European Union Directive 2000/31/EC on electronic commerce (Directive on E-commerce),[3] reflected a new dual role of Internet intermediaries: they deserved protection as neutrals, but they could also be called upon to assist with norm enforcement. The underlying reason for these regulations, however, was primarily to define exceptions or safe harbours that would protect ISPs against liability claims. Nevertheless, these laws also acknowledged that, under certain circumstances, ISPs should assist in stopping copyright infringements, for example.

4 Both the DMCA and the Directive on E-commerce[4] regulated three types of ISP services: the transport, temporary storage, and hosting of information. In addition, the DMCA also regulated search engines. Presently, there is a tendency to put pressure on ISPs to co-operate in addressing norm violation, in particular in their role as access provider. For instance, courts in several countries (Netherlands, Finland,[5] UK,[6] etc.) ordered ISPs to filter Internet traffic; the French HADOPI Act has a so-called three-strike policy regarding downloading; and the controversial ACTA is infringing on human rights in a serious way.[7] The secrecy surrounding this last initiative added to the controversy regarding its content. Much media attention was also paid to the US initiatives SOPA and PIPA.[8] These initiatives were abandoned in February 2012, but by April 2012 the comparable CISPA had already passed in the House of Representatives.[9] Since the Senate did not accept the CISPA, it was re-entered and passed again in April 2013.[10]

5 Are the times changing? Are we entering a new era? This paper aims to answer this question by focusing the discussion on ISPs in their role as the access provider.[11] The paper is structured as follows: In section 2 the liability exemptions of the US DMCA and the EU Directive on E-commerce are introduced. Next, we will discuss a series of Dutch court cases concerning The Pirate Bay that ended in 2012 with court orders against several ISPs to filter out websites belonging to Pirate Bay. In the third part we will evaluate which role fits access providers best. Viewed from different angles, the access provider as the intermediary merely providing access to the Internet will be weighed against the access provider as a full-time norm enforcer, and we will provide principles that can help in striking a balance.

B. Early days: DMCA and Directive on E-commerce

6 The spirit of the mid-1990s is well reflected by Kaspersen:[12] '(...) the duties of access-providers do not embody anything else but giving access to the Net and all the information in it, just as it is'.

7 Stated simply, an access provider should just provide access to the Internet. This basically was the background of the legislation proposed during the late 1990s, although besides this main focus on creating a safe harbour it was also acknowledged that under certain circumstances ISPs should assist in combating (in particular copyright) infringements.

I. DMCA

8 Prior to the DMCA, in 1996 Section 230 of the Communications Decency Act regulated immunity for ISPs and others regarding hosted content.[13] For the present paper with its focus on access providers, this controversial and much-debated Act[14] is not directly relevant.

9 On December 1998 the DMCA entered into force. This Act included in Title II the addition of paragraph 512 to the US Code, better known as the Online Copyright Infringement Liability Limitation Act (OCILLA). OCILLA defines four categories of exemptions applicable to ISPs: services related to (1) information location tools (search engines), (2) storage of information at the direction of users (hosting), (3) system caching and (4) transitory communications.[15] The transitory communications category is relevant for the present paper since it concerns 'transmitting, routing, or providing connections'. Whereas in doctrine, access providers are normally distinguished as a special category of providers, in regulation this is not necessarily the case. Although all types of transitory communication providers are crucial to a proper functioning of the Internet, the doctrinal treatment of access providers as a single category is understandable. For anyone on the Internet, it always starts with getting access.

10 Instead of enforcing norms on the Internet – regulating behaviour in cyberspace – it is sometimes easier to control at the source: make sure that people never get to (parts) of the Internet, or that people cannot use particular applications. As such, the ISP can function as a single point of contact for all of its users, and these users are regulated at a single instance. Access providers are the gate to the virtual world, and consequently are an obvious party to appoint as norm enforcer or gate keeper. As Mann & Belzey state:[16] 'Internet intermediaries (...) are easy to identify and have permanent commercial roots inside the jurisdictions that seek to regulate the Internet.'

11 As a shelter for such claims, the DMCA/OCILLA determines that the transitory communication provider is not liable if (1) the provider does not initiate the access, (2) the process is automatic without selection of the material, (3) the provider does not determine recipients, and (4) the information is not modified. Besides these topics related to the core activity of an ISP, OCILLA sets two other conditions: (5) providers should have a policy of account termination of repeat infringers and (6) should not interfere with technical measures (e.g. Digital Rights Management software).

12 Access providers almost intrinsically satisfy all these conditions expect for the fifth. Basically, in a normal course of action, access providers cannot be held liable as long as they define and apply a policy of account termination. The above applies to monetary relief. There are some circumstances under which injunctive or other equitable relief is possible,[17] and

we will discuss them after introducing the E-commerce Directive.

II. Directive 2000/31/EC on E-commerce

13 The E-commerce Directive was drafted against a different background than the DMCA. The opening words of the proposal for the E-commerce Directive are illustrative: 'Electronic commerce offers the Community a unique opportunity for economic growth, to improve European industry's competitiveness and to stimulate investment in innovation and the creation of new jobs.'[18]

14 This Directive formed the central pillar in the regulation of e-commerce within the EU, as was outlined in a policy document from 1997.[19] As part of the same legal package, Directive 2001/29/EC on copyright in the information society is more directly related to the DMCA, but it did not cover liability:[20] 'Liability for activities in the network environment concerns not only copyright and related rights but also other areas, such as defamation, misleading advertising, or infringement of trademarks, and is addressed horizontally in Directive 2000/31/EC (...) on E-commerce.'

15 In the proposal for the E-commerce Directive, the European Commission identified five key issues, referred to as obstacles. One of them concerned the liability of intermediaries: 'To facilitate the flow of electronic commerce activities, there is a recognised need to clarify the responsibility of on-line service providers for transmitting and storing third party information (i.e. when service providers act as 'intermediaries').'[21]

16 The angle is basically economic. The aim is to stimulate e-commerce within the European Union by protecting ISPs against liability, thus preventing them from being hindered by all kinds of liability claims when providing their services. Nonetheless, the Directive on E-commerce[22] takes a similar approach, and as McEvedy correctly observes[23] 'closely resembles the DMCA in that it provides "limitations of liability" while leaving the underlying law unaffected'. The scope of the E-commerce Directive is broader, in that it covers all legal fields, not only copyright. Surprisingly, the proposal for the E-commerce Directive does not mention the DMCA, but in certain parts it follows it almost verbatim.

17 The E-commerce Directive's well-known triad of services provided by ISPs is mere conduit (Article 12), caching (Article 13) and hosting (Article 14). At first sight it may seem that the role of access providers is left unregulated. However, just as the DMCA covered access under 'transitory communications', the mere conduit of Article 12 regulates not only 'the transmission in a communication network' but also 'the provision of access to a communication network'. The proposal also clearly indicates the different scope depending on the provider's role: 'establishes a "mere conduit" exemption and limits service provider's liability for other "intermediary" activities'.[24]

18 In order to be not held liable, the access provider should not (a) initiate the transmission, (b) select the receiver of the transmission and (c) select or modify the information contained in the transmission. For an access provider, this set of conditions is even easier to comply with than the six conditions of the DMCA/OCILLA just discussed.

III. Court orders and other observations

19 The fact that mere transmission and providing access are headed under the same category can be considered an underestimation of the role of access providers, as was indicated above. However, one could also argue that now that both the DMCA and the E-commerce Directive take this approach, there must be a reason why these services should be judged similarly. If we proceed from this assumption, we could argue that intervention of access providers should be treated similarly to intervention by providers of servers that just pass IP packets through. It is hardly imaginable that such a provider that only transmits information over the Internet would ever be called upon. So, if this provider is headed under the same category as the access provider and never asked to assist with the enforcement of norms, why would the access provider be?

20 An obvious difference between the two providers is that the access provider has a contractual relationship with the user, while the provider merely passing through IP packets does not. However, the court cases discussed in this paper concern blocking access to certain sites, so the contractual relation is not relevant in that respect. Another difference has to do with the Internet infrastructure. If an access provider blocks access, this can be effective[25] for their users, and for the other provider the effect is not guaranteed. Moreover, all users worldwide could be affected by the latter measure, whereas actions from the access providers affect only their users.

21 The safe harbors created for access providers by both the DMCA and the E-commerce Directive are not absolute. The DMCA is different in that it has an explicit notice-and-take-down (NTD) procedure,[26] and providers can be forced to reveal the identity of subscribers. The E-commerce Directive has no explicit procedures. As a consequence, ISPs need to carefully

weigh the pros and cons after a complaint without the certainty of not being held liable by either the party complaining or the opposing party. For the present paper this is not directly relevant, since access providers are never confronted with NTD requests, at least not in their role as access providers. Identity requests ask difficult decisions of ISPs, and these requests go even beyond the classic roles of ISPs to include web 2.0 providers.[27] Identity requests also fall outside the scope of the present paper.

22 An importance difference between the two regulatory frameworks is the way court orders are regulated. Whereas the DMCA defines many conditions that have to be met before a court can order an access provider to block certain content,[28] the E-commerce Directive sets no specific conditions,[29] generally stating in Article 12(3): 'This Article shall not affect the possibility for a court (...) requiring the service provider to terminate or prevent an infringement'.

23 This might explain why it is relatively easy to get a court order within the EU and hard to get one in the US. It might also explain why the tendency within the EU is for the entertainment industry to go to court, and in the US they focus on the introduction of new legislation. Illustrative are the Dutch court cases concerning The Pirate Bay, which we will discuss next.

C. Dutch case law or the Pirate Bay saga

24 In 2012 the Dutch anti-piracy organization BREIN, a foundation that aims to enforce intellectual property rights for the entertainment industry, obtained several court orders that forced ISPs to block access to The Pirate Bay. The Dutch Pirate Bay cases nicely illustrate the legal grounds underlying the blocking of access by ISPs. Therefore, we will discuss the main arguments used in the various cases that started with court proceedings against The Pirate Bay in May 2009.

I. BREIN v The Pirate Bay 2009-2010

25 The case against The Pirate Bay began well before the judge handed down its verdict in the Netherlands. Early in 2009, charges were filed in Sweden against the people behind The Pirate Bay, followed by a conviction of one year of imprisonment for Fredrik Neij, Gottfrid Svartholm, Peter Sunde and Carl Lundström on 17 April 2009.[30] The criminal conviction in 2009 led to a court initiative by BREIN that sued the Pirate Bay people in the summer of 2009 for copyright violation.

26 The summons was delivered at the address as recorded in the Swedish population register but was returned. The defendants did not show up in court, but the judge allowed the proceedings to take place in absentia.[31] This is allowed in summary proceedings if the plaintiff has put sufficient effort in trying to reach the defendant. It is interesting in this case that the effort consisted, amongst others, in sending the court order via e-mail, Twitter and Facebook (the plaintiff was de-friended minutes after the court order was left on the Pirate Bay-owned Facebook page). The reaction of one of the defendants was decisive when the press confronted him with the upcoming court case: 'Having a court case in Amsterdam on July 21 does not ring a bell.'

27 In the 30 July 2009 verdict, the court ordered The Pirate Bay to

1. stop copyright infringements in the Netherlands and

2. make websites thepiratebay.org, piratebay.se, etc. inaccessible to Dutch users.

28 The verdict is somewhat ambiguous. What is probably meant by 'Dutch users' and 'copyright infringements in the Netherlands' is Dutch IP addresses. One could argue that if the websites mentioned are inaccessible in the Netherlands, copyright infringements are stopped as far as The Pirate Bay is concerned so the first order does not add anything. However, the reason for the first point might be that changing domain names will not work to undermine the second point. Clearly, if a proxy were used the second ban could be circumvented, allowing users to access The Pirate Bay and infringe copyrights.

29 After this verdict, Pirate Bay started summary proceedings against BREIN, arguing that due to the technical complexity, this case is not suited for summary proceedings. The judge indicated that despite the complexity, balancing the opposing interests of The Pirate Bay and BREIN remains possible. The result: The Pirate Bay did not violate copyrights, but the judge decided that the act of facilitating copyright infringements by others is illegal. The judge ordered the following on 22 October 2009:[32]

1. The Pirate Bay should delete all torrents that refer to material that infringes on copyright material relevant to BREIN.

2. The Pirate Bay should block access of Dutch Internet users on the various Pirate Bay websites to the torrents under 1.

30 The idea behind this court order change was to allow references to material that does not infringe on copyrights of the parties BREIN represents. This is in favour of the freedom of speech as far as non-infrin-

ging material is concerned. However, since the court orders the deletion of torrents, people not using a Dutch IP address would also no longer be able to access them. In this respect the order reaches further than the previous court order. Another problem with the verdict is how The Pirate Bay can establish whether a torrent infringes on the copyright of the parties BREIN represents.

II. Intermezzo: International hosting providers

31 The Pirate Bay did not follow the court order, so BREIN turned to the access providers. In previous court cases in other countries, The Pirate Bay hosting providers had been sued. First, the Swedish courts decided that hosting The Pirate Bay was not allowed. The Pirate Bay was offline for a couple of days but then reappeared on German servers. The German judge also ordered a cessation of hosting The Pirate Bay. The race to the bottom stopped in Ukraine, which has hosted the Pirate Bay servers since then. In addition to the fact that suing in Ukraine would not necessarily have the same results as in Sweden and Germany, it became clear that even winning in Ukraine would only mean that The Pirate Bay would seek yet another country to host their websites.

III. BREIN v the largest ISP, summary proceeding 2010

32 Based on this verdict, BREIN asked Dutch providers to filter out Pirate Bay Internet traffic. The providers did not grant this request. Therefore, in what they called a test case, BREIN decided to sue only the ISP that facilitated the most Pirate Bay traffic. This appeared to be Ziggo. On the grounds of principle, XS4ALL joined Ziggo as a defendant in this case.[33]

33 The subtlety of the 2009 verdict (not providing access to infringing material) was replaced by BREIN and became mere access. In summary proceedings, BREIN applied the Dutch implementation of Article 11 of Directive 2004/48/EC on the enforcement of intellectual property rights (see also Article 8(3) Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society): '(...) 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 (...)'.

34 The third party are the subscribers of the ISP. The judge did not grant the request, arguing that the injunction is allowed only in cases of direct infringement, and the order would apply to all users of the provider, not only those infringing copyrights after accessing The Pirate Bay. This ruling is a bit odd: people who do infringe are banned, and people who do not infringe did not go to The Pirate Bay anyway. The argument could be that those who do not use The Pirate Bay might want to go there for lawful activities as well. However, in practice most, if not all, Pirate Bay users go there to obtain copies of works violating copyright.

IV. BREIN v the largest ISP, proceedings on the merits 2010-2012

35 In the proceedings on the merits that BREIN started after they lost the summary proceedings, they basically claimed the same.[34] The judge followed the European Court of Justice (ECJ) ruling from 12 July 2011[35] (L'Oreal v eBay), and stated that Article 11 of Directive 2004/48/EC on the enforcement of intellectual property rights can also be used to prevent infringements. In a later case (Scarlet v Sabam) on 24 November 2011,[36] the ECJ indicated that active monitoring for illegal content cannot be asked from access providers.

36 This last decision is interesting, since the Dutch judge's verdict in the summary proceedings asked precisely this from the providers XS4ALL and Ziggo. If this verdict were to be translated to ISPs, it would not be allowed according to the Scarlet v Sabam case. However, since BREIN chose a different strategy, in which it requested the mere banning of domain names and IP addresses, this EU court ruling could not be applied directly. This actually means that because BREIN claimed too much (hence also blocking legal Internet traffic), the active monitoring prohibition could be circumvented. Blocking websites or IP addresses of The Pirate Bay is ordered from the ISPs.

37 On the subsidiarity question, the judge in the summary proceedings indicated that at least suing some consumers – i.a. because they could then have the opportunity to defend their position – could be asked from BREIN. Now the judge indicated that this was not necessary, and that after the lawsuits against The Pirate Bay and the hosting providers, the logical next step concerned access providers.

38 On the proportionality question, the judge indicated that given the amount of illegal opposed to legal content, the interests of the copyright holders outweigh the interests of the ordinary Internet users. Still, the blocking of access to the complete website is less proportional than what was previously ordered by the court: not providing access to illegal material. Interestingly enough, downloading music and movies is allowed in the Netherlands, but uploading

of infringing material is illegal. Most – though not all – users do both on a torrent site.

39 During the proceedings, BREIN claimed that blocking had been effective in Denmark and Italy. Still, it is easy to circumvent the blocking, and the people who really want to use The Pirate Bay can do so. Interestingly enough, research carried out by the University of Amsterdam showed no difference in Pirate Bay Internet traffic after the ban.[37]

40 The judge briefly addressed whether the current measure was necessary in a democratic society (cf. Article 10 ECHR). He referred to the proportionality and subsidiarity considerations just discussed, in particular regarding the interests of the subscribers in relation to the copyright holders. One might claim that the necessity considerations should at least include how the entertainment industry operated during the last 15 years.[38] Another point that could have been covered is what role access providers should have on the Internet. The outcome might still have been the same, but it would have been better grounded.

41 The judge ordered Ziggo and XS4ALL to block a list of 24 websites (of which several were outdated at the time of the verdict, and others later became outdated), as well as three IP addresses. It is curious that BREIN was granted the right to change the list anytime they believe it is necessary, without judiciary intervention. One could argue that the judge did not really take notice of the particular sites anyway, but in a trial opponents have the opportunity to object. Ziggo and XS4ALL now have to start a new trial if they do not agree with a particular IP address or website. If they do not comply, they have to pay a daily fine. The verdict does not pay attention to possible errors on BREIN's side.

42 Both Ziggo and XS4ALL have appealed, but a decision is not expected before the end of 2013.

V. BREIN v other ISPs 2012/5-

43 Based on the verdict, BREIN asked other ISPs to voluntarily start blocking The Pirate Bay. Since the ISPs refused, BREIN started new proceedings against other big providers, including KPN, UPC, T-Mobile and Tele2.[39] The verdict is lengthy but does not add much. A difference from the original verdict is that BREIN is not allowed to change the list of sites and IP addresses. The Pirate Bay has over 100 different IP addresses and has already announced that it might add one IP address at a time, meaning that BREIN would have to start over one hundred different procedures. Maybe, this Pirate Bay policy can change subsequent verdicts on this point.

44 One interesting observation is on the effectiveness of the blocking. The ISPs introduced the previously mentioned research by the University of Amsterdam[40] showing that the blocking did not have any effect. The judge stated: '[B]locking as such does not necessarily lead to less Pirate Bay traffic, but effectively combating infringements is possible only if this blocking is combined with other measures'.

45 This is a somewhat curious observation, in particular since one of BREIN's claims from the beginning has been that the blocking has at least some effect and as such contributes to fighting copyright infringements. Therefore, the argument is that the measures are a necessary element that works in combination with other measures. One of those other measures is to forbid proxy servers. In the course of 2012, BREIN sued a series of organizations and people that offered proxy servers, and did so ex parte.[41] One of the controversial cases was against the political Pirate Party. Although legally interesting and socially relevant, these cases are not within the scope of the present paper since it does not concern access providers.

D. What role fits access providers best?

46 The decisions discussed above are certainly not exclusive to the Netherlands. On 1 May 2012, the High Court in the United Kingdom ruled that the major ISPs in the UK must block access to The Pirate Bay. As the providers themselves noted, they do not want to be the judge and the jury of online content. Copyright-infringing material is the prime example of content ISPs are asked to intervene with and central in this paper.

47 The interest in ISPs commenced before the DMCA and Directive on E-commerce were enacted. Back in 1995, ISPs were considered to be the party most suited to control the dangers of the Internet; in fact, 'a task force created by President Clinton suggested imposing strict liability on ISPs'.[42] Moore & Clayton capture the complexity of ISP liability,[43] but recognize how '(...) ISPs are in an unrivalled position to suppress content held on their systems'.[44]

48 Before answering what role best fits the access provider, we will discuss ISP liability both related to Internet traffic (spam, cyber security) and concerning content (defamation, privacy breaches, child porn).[45] For each of these topics we will introduce a rule of thumb that can help ISPs in their decision whether to comply with a request.

I. Cyber security and spam: ISPs take initiative

49 In the field of cyber security, ISPs have realized over the years that it is in their best interest to act. The same is true for spam. If ISPs did not use spam filters, probably no one would use e-mail any longer. Can ISPs still claim to be neutral if they actively act, as in filtering spam or eliminating malware?

50 In a famous Dutch case, the Supreme Court judged on the position of an ISP in the case of spam.46 XS4ALL asked the direct marketer Ab.fab to stop sending spam to their customers. Ab.fab did not. Some argued that ISPs would lose their neutral position should they be allowed to reject messages. The Supreme Court decided that an ISP had the right to ask a party to stop sending spam.[47] The basic argument was that a provider is the owner of the mail server, and if the provider has good reason to not want to process specific mails, the provider does not have to. Ab.fab was ordered to stop sending e-mail. Ironically, before the Supreme Court ruled, Ab.fab had already gone bankrupt. The principle question still stood, however: Does the nature of the Internet and the role of ISPs in it conflict with asking a company not to send unsolicited email? As with all rules or principles, exceptions apply. To draw a parallel, if a football stadium is open to the general public, some people causing trouble might be banned from the stadium. After such a measure, the stadium is still open to the general public. In the case of ISPs, certain traffic can be banned from their servers without ISPs losing their neutrality. A similar argument applies to malware and other security measures.

51 In 2004, Lichtman and Posner called for an increased liability, and claimed that since ISPs are largely immune from liability, they have no incentive to act.[48] Harper attacked this proposal by pointing at a fundamental flaw: '[I]t places efficiency ahead of justice. The Internet is a medium, not a thing, and the supply of access to it is peculiarly unsuited to a liability rule like Lichtman proposes.'[49]

52 Nonetheless, Lichtman and Posner's position has been supported by the United Kingdom House of Lords Science and Technology Committee, for example, which stated in 2007 that '(...) although ISPs could easily disconnect infected machines from their networks, there is no incentive for them to do so'.[50]

53 Others echo similar notions. Chandler writes: 'The parties best placed to address cyber insecurity, including (...) ISPs (...) do not face the full consequences of their contributions to cyber insecurity. Accordingly, they do not invest time and money to the socially optimal level of improved security'.[51]

54 Van Eeten & Bauer challenge this assumption: ISPs may '(...) unwittingly reinforce the impression that they have few if any incentives to improve the security of their services'.[52] This occurs through the resistance of ISPs to government intervention and the hesitance to surrender self-regulation. The resistance to government intervention is interpreted by many as an unwillingness to provide more security; yet this is an incorrect conclusion according to Van Eeten & Bauer. The efforts made by ISPs to improve the security of their clients started to escalate during the last decade when ISPs began to understand how improved security turned out to be in their best interest. This is due to costs associated with the insecurity of their clients.

55 As follows from the above discussion on spam and cyber security, ISPs do take initiatives that in themselves go beyond the neutral role of mere transport because they influence their core activities. Both spam and malware directly negatively influence the (access) services. Their aim is to guarantee a properly functioning Internet, in particular access that is not hindered by unwanted (spam) and the undesired (malware) activities of others. This is what justifies their actions. The more these actions by ISPs are related to their core activities, the less influence such actions have regarding their neutral position. In the end it should be the decision of the ISP, and not one imposed by government, for example. Because the decision is up to the ISP, and what they do is objectively good for their users, they can uphold their basic neutral position.

II. Requests related to content: child porn, defamation and right to be forgotten

56 If ISPs have no incentive, external pressure could work. Access providers are in a position to influence what is communicated over the Internet.

57 One should be very cautious in asking assistance from ISPs. The fact that it is technically possible does not make it legally desirable. Let us assume that there is a public meeting room in a building that is hired by a politically motivated group of people. During this meeting, a defamatory poster is put on the wall. Some of the attendees inform the person who is defamed by the poster. He goes directly to the meeting and asks the people in the room to remove the poster. They do not. The defamed person goes to the owner of the room to ask for removal of the poster. If the owner chooses not to do so, can he be held liable? This is a very difficult decision for the third party to make. He has to balance freedom of expression against its possible defamatory nature. Whilst this situation is already difficult to navigate, what about the owner of the meeting room being asked to

block access to the room because of the poster? This is even more difficult to decide, for the impact is bigger. If entrance to the room is blocked, the people cannot have their meeting. This shows the indirectness of access blocking. The first level is asking the person who put the content there to remove it, the second level is asking the same of the hosting ISP, and the access provider only enters at the third level. When a judge orders that access be blocked to a particular website or IP address, this represents an indirectness acceptable only as a last resort. But a judge should be hesitant even then, because the nature of the Internet makes such measures both under- and over-inclusive.

58 Requests placed upon ISPs are often impractical and sometimes even illegitimate. The study carried out by Stol et al. on child pornography and Internet filtering illustrates the difficult position of ISPs and the importance of solid legal analysis.[53] As Stol et al. conclude,

> *[f]rom the point of view of constitutional law it is not acceptable that the authorities make use of instruments without sound legal basis in order to reach an otherwise legitimate goal. If the legislature's intention is to designate the blocking of child pornography as a duty of the police, then this should be provided in specific legal jurisdiction.*[54]

59 It has been argued by Dommering[55] that a sound legal defense is impossible. The Dutch Constitution does not permit control in advance (censorship), and this filtering prevents the assessing of particular content. A rebuttal here is that the filtering takes place only on the basis of lists of websites and IP addresses where child porn was already found, so in this respect the control is afterwards and not preventive. However, the Internet changes very quickly, and lists become outdated fast. One can never be sure what exactly is filtered.

60 Privacy breaches are another content-related topic often taking place on the Internet. Also, the Internet hosts various outdated personal information or information one simply does not want to be confronted with any longer. It is not always easy to get this information offline. In a recent proposal, the European Union introduced the right to be forgotten.[56] Again, ISPs are asked to co-operate, which is complicated since they find themselves in the midst of a conflict of interest between freedom of speech and the right to privacy.[57] The one who has published the information is the first point of contact, with the hosting provider coming second. One could imagine that access providers would be asked to block certain content if these first two steps do not work.

III. Copyright infringement: external and preventive actions

61 A couple of years ago the discussion focused on the necessity of increased liability for ISPs; currently ISPs are just asked to carry out certain actions. The Dutch lawsuits by BREIN discussed above are a prime example, as is the French HADOPI law.[58] The background of HADOPI's 'three strikes and you're out', introduced in 2009, is fighting copyright infringements. ISPs play a central role; for example, after a first notice the ISP is to actively monitor the suspect, and after the third 'strike' the person in question is blacklisted. The provider of the violating user as well as other ISPs are to ban the user for a fixed period of up to one year. This means that instead of blocking content, the access provider is to cut off an individual from the Internet. Besides the potential conflict with human rights,[59] this demands from the access provider the enforcement of norms that diametrically oppose their core activity: providing Internet access to people.

62 Of a different nature was the 2011 initiative involving some of the biggest American providers; without any act or verdict, they voluntary agreed to become 'copyright cops'.[60] Probably these providers had reasons to act as such, but it puts their neutral role under pressure. It is difficult for these providers to claim that they do not have to co-operate due to their neutral position if asked by private parties or government to intervene, either repressively or preventively, in cases of digital piracy.

63 There is an important distinction to be made here: on the one hand are ISPs acting voluntarily; on the other hand are ISPs being forced. Just as in cases of child porn, government should not force ISPs to block access, but ISPs may do it on their own initiative. However, once you act freely, you can no longer claim to be neutral as far as similar content is concerned. Once ISPs are more than passively involved with the communication or the flow of information, they cannot rely on the safe harbors created by law. This does not make them necessarily liable, but there is no longer an easy way out. The same is true for access providers: once you voluntary search for copyright violations, for example, third parties can ask you to do so, too.

IV. Statutes and judges

64 We discussed Dutch cases that led to various court orders forcing access providers to block The Pirate Bay. In contrast to what is currently happening within the EU, the US cannot count on the judiciary when it comes to blocking websites. The conditions as formulated in the DMCA/OCILLA, for example, are simply too difficult to meet. That is one reason

why the music industry is trying to get acts pushed through the American Congress. Basically, getting a bill passed is more difficult than convincing a judge. Judges are not elected in the Netherlands (and in most, if not all, EU countries), so judges do not have to take public opinion into account. The US legal initiatives demonstrated that public opinion can influence the decision-making process of the legislature.

65 Recall that on 18 January 2012, over 7,000 websites, including Wikipedia and Google, successfully staged a blackout as a means to protest legislative initiatives introduced in both chambers of the United States Congress. These initiatives, the Stop Online Piracy Act (SOPA) and the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA), both aimed to curb digital piracy in the United States. The primary objectives of both bills was to promote prosperity, creativity, entrepreneurship and innovation by combating the theft of US property. Or, as the Economist put it more bluntly, '[t]he bill aims to cut off Americans' access to foreign pirate websites by squeezing intermediaries'.[61]

66 Beside the general public's opportunity to influence, focus is another difference between legislation and court cases. In court cases the focus is on a single actor (e.g. The Pirate Bay), which makes it easier to decide against him. Also related to focus, proposals for legislation are necessarily abstract, and likewise feel like more of a threat to the general public (e.g. it touches the whole Internet). One additional difference we want to note is that politicians appear to feel more sympathy for the economic arguments of the entertainment industry than judges are expected to. Finally, public opinion can provide correction during the legislative process, whereas in court cases public opinion basically starts only after the decision: only then does the outcome become clear.

67 The neutral position of access providers is no different when it comes to objecting against case law or against acts; only the means of maintaining that neutrality are different.

V. How to draw the line?

68 The list of requests access providers receive is long, so we are not able to discuss them all, such as data retention[62] or online porn blocking.[63] This expanding list, both in terms of what to do and how to do it, forces the need to re-evaluate what is being asked from access providers.

69 There are two basic camps. One camp stresses the importance of Internet freedom, innovation, the neutral role of providers, protection of freedom of speech and privacy. The other camp also stresses innovation, protection of rights and fighting crime. And as with all discussions, there are intermediate positions. We do take a position in this debate, but as with all legal debates – and particularly in those concerning Internet governance topics – we emphasize that there is no obvious right or wrong; instead, it is about balancing and weighing the pros and cons. In the fire of the discussion this is sometimes forgotten, but with sensitive issues it is important to keep this in mind: arguments matter, not who is defending them.

70 In drawing the line between the circumstances under which ISPs should be asked to cooperate and when it is better to leave them alone, at least the following should be taken into account.

71 First, consider the directness of the measure. In a way this is related to but not the same as the question of subsidiarity: if other less burdensome actions are possible, they should be preferred. Directness also concerns how related the proposed action is to the activities of the ISP. The more direct, the sooner action might be asked from ISPs. For instance, if someone wants to take material down, the first response is to go to the one who put it there, next to the hosting provider, and third to the access provider.

72 Second, consider the effectiveness of the measure. Each action serves a goal, but if the goal is hardly reached, someone might take independent action anyway and therefore should not ask this from others. If a measure is merely symbolic or the effects are insignificant, access providers should not be asked to cooperate. Basically, the more effect a measure has, the sooner action might be asked from ISPs. It might be that what is asked for is so important that even the slightest effect is worth carrying out the action. If that is the case, normally the action should be carried out unless the costs (not only financially) associated with the action are disproportional.

73 Third, consider the costs of the measure. This point is related to proportionality: the action should be in proportion to the severity of what is targeted. Again, the costs are not only financial but may also include effort or side effects. The lower the costs, the sooner action might be asked from ISPs. It may not become an argument in itself, or better, not the only argument. If an action scores badly on other aspects, and the only real argument is that it is easy for the access provider to fulfil the request, the ISP should not.

74 Fourth, consider relevance as related to the history of the ISP. If an ISP has cooperated voluntarily in past requests, or has taken independent actions related to what the ISP is now being asked to do, it is harder to refuse assistance. The more related the past activities of the ISP are to what the ISP is now being asked to do, the sooner action might be asked.

75 Fifth, consider the time element. Repressive actions do not concern censorship, whereas preventive actions do.[64] If content is taken down, the action is clearly repressive and concerns only the content taken down. In the case of repressive action, blocking access to websites might even turn into censorship. This has to do with the dynamic nature of the Internet. In the case of cybercrime, for example, assistance in blocking traffic to particular websites (cf. the black-listing of servers sending spam) may also filter out legitimate e-mail. Therefore, any list of sites blocked should be evaluated regularly.

76 Finally, and this is an overreaching element, adequate safeguards should be in place. The points indicated above already imply warranties. In addition, for any action asked from ISPs, there should be a sound legal ground. It is important to rule out arbitrariness. Judiciary intervention can also be part of the safeguards. For instance, at the wrong side of this boundary are black box lists of websites so that ISPs do not know what they are filtering or lists of websites created without judicial intervention.

E. Concluding observations

77 In January 2012, a 10-year-old Dutch boy (and obviously many others) could no longer download legal software via his favourite website. This was not because the Court of The Hague had ordered two providers to block The Pirate Bay on January 11, or because SOPA, PIPA or ACTA had entered into force. Instead, it appeared that the US Department of Justice had taken the file-hosting site Megaupload offline. Ironically, or sadly, this was exactly one day after Wikipedia had staged a blackout to protest the SOPA and PIPA initiatives.

78 The Megaupload case is an interesting example of the strong – or better: long – arm of the law. People (such as Kim Dotcom) were arrested by the FBI in New Zealand, amongst others. The link between Megaupload and the US was not clear. Sure, the Internet is accessible all over the world, and information on a website basically enters all jurisdictions.[65] The reason, however, for the US action was that the people behind Megaupload were accused of running an international criminal organization, not only facilitating copyright infringements but also laundering money. This begs the question: Why ask dozens, hundreds, or maybe even thousands of access providers to filter out websites if one action against the provider of the website has the same result?

79 As the discussion of the Pirate Bay case revealed, it is not always easy to take a website offline. In the case of The Pirate Bay, successful court actions only led to shifting from hosting providers in one country to hosting providers in another country, lastly Ukraine.[66] So the call on access providers is comprehensible. Under certain circumstances they could be asked to assist. In this paper we introduced rules of thumb that could help in deciding whether an access provider should cooperate:

3. The more direct the requested action is, the sooner action might be asked from ISPs.

4. The more effect a measure has, the sooner action might be asked from ISPs.

5. The lower the costs, the sooner action might be asked from ISPs.

6. The more related the ISP's past activities are to what the ISP is asked to do, the sooner action might be asked.

7. Repressive action is preferred over preventive, and preventive action needs regular re-evaluation.

80 Notably, adequate safeguards should be in place, in particular a sound legal basis for action. From the US perspective, Lemley, Levine & Post stated:[67]

> *United States law has long allowed Internet intermediaries to focus on empowering communications by and among users, free from the need to monitor, supervise, or play any other gatekeeping or policing role with respect to those communications. Requiring Internet service providers (...) to block access to websites because of their content would constitute a dramatic retreat from that important policy.*

81 We hope that the appeal cases in the Netherlands have outcomes other than that of the first instance decisions. The US policy just described should be enforced (again) in the Netherlands as well as within other European Union countries. Access providers should not be forced to check lists of websites, IP addresses and the like, for it concerns the opposite of what their role should be: providing access. An intermediary basically helps to connect two parties. We should not shut down train stations when the actual threat is somewhere down the line; otherwise we are heading in a direction we do not want to go.[68]

Endnotes

1 The Dutch phrase is often used to emphasize the neutral position of Internet service providers with a difficult-to-translate repetition of words: 'geen boodschap aan de boodschap'.

2 112 STAT. 2860 PUBLIC LAW 105–304—OCT. 28, 1998, 105th Congress. An Act to amend title 17, United States Code, to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty, and for other purposes. The present paper covers one of the 'other purposes', limitations on liability for ISPs.

3 Directive 2000/31/EC on electronic commerce; see above, footnote 4.

4 For an extensive overview of case law ruled under both initiatives, see M. Martinet Farano (2012), Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and U.S. Approaches, TTLF Working Papers No. 14.

5 M. Norrgård (2011), Blocking Web Sites – Experiences from Finland, <http://ssrn.com/abstract=1997103>.

6 The High Court of England and Wales ruled on 30 April 2012 after claims from the British Phonographic Industry (BPI) that five ISPs (Sky, Everything Everywhere, TalkTalk, O2 and Virgin Media) should block the Pirate Bay; see e.g. Huffington Post 30 April 2012, <http://huff.to/OGhD5m>.

7 P.K. Yu (2011), Six Secret (and Now Open) Fears of ACTA. SMU Law Review, Vol. 64, pp. 975-1094, 2011.

8 M.A. Carrier (2012), Copyright and Innovation: The Untold Story. Wisconsin Law Review, Forthcoming. Available at SSRN: <http://ssrn.com/abstract=2099876>.

9 Cyber Intelligence Sharing and Protection Act, Passed the US House of Representatives on 26 April 2012. See <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3523>. It is uncertain whether the US Senate will accept the bill; if it does, President Obama has indicated he will not sign it.

10 H.R. 624: Cyber Intelligence Sharing and Protection Act, accepted on 18 April 2013, <http://www.govtrack.us/congress/votes/113-2013/h117>.

11 The access provider was not explicitly mentioned in the two main 1990s regulations; instead, it is commonly designated as a mere conduit (EU Directive) or as transitory communications (DMCA); see further below the section Early days: DMCA and Directive on E-commerce.

12 H.W.K. Kaspersen, Liability of Providers of the Electronic Highway, 12 The Computer Law and Security Report 2006: 290-293.

13 M. Schruers (2002), The History and Economics of ISP Liability for Third Party Content, Virginia Law Review, Volume 88, No. 1, pp 205-64.

14 S. Ardia (2010), Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act. Loyola of Los Angeles Law Review, Vol. 43, No. 2, 2010.

15 Reese nicely characterizes the nature of the exemptions: 'Congress has enacted, in section 512 of the Copyright Act, limitations on the liability of service providers, but conditioned those limitations on a fairly complicated set of conditions.' R.A. Reese, The Relationship between the ISP Safe Harbors and Liability for Inducement. Stanford Technology Law Review, Vol. 8, 2011.

16 R. J. Mann and S.R. Belzley, The Promise of Internet Intermediary Liability. William and Mary Law Review, Vol. 47, October 2005.

17 As defined in § 512 subsection (j).

18 Proposal for a EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE on certain legal aspects of electronic commerce in the internal market, 18.11.1998, COM(1998) 586 final, p. 3.

19 'A European Initiative on Electronic Commerce', COM(97) 157 final, 16.4.1997.

20 Recital 16 DIRECTIVE 2001/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ, 22.6.2001, L 167/10. The proposal for this Directive was published 10 December 1997, almost a year before the E-commerce Directive: 18 November 1998. The final text, however, was published one year later (June 2000 and June 2001 respectively). The Member States had far more problems agreeing on how to regulate copyright on the Internet than they had to agree on how to regulate e-commerce. For a discussion of this Directive, see M. Vivant (2002), Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, in Lodder, A.R., Kaspersen, H.W.K. (eds.), eDirectives: Guide to European Union Law on E-Commerce , Kluwer Law International, The Hague, p. 95-117.

21 Proposal for a EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE on certain legal aspects of electronic commerce in the internal market, 18.11.1998, COM(1998) 586 final, p. 4.

22 At that time some case law already existed on ISP liability. For instance, in the Netherlands a lower court had already ruled on 12 March 1996 in a lawsuit with the Scientology Church and the Dutch ISP XS4ALL (for a translated version of the summons, see <http://kspaink.home.xs4all.nl/cos/dag1eng.html>). The case law was one of the reasons why the European Union considered it necessary to regulate the exemptions to liability: 'to eliminate the existing legal uncertainty and to bring coherence to the different approaches that are emerging at Member State level'. The final ruling by the Dutch Supreme Court on 16 December 2005 (LJN: AT2056) in the abovementioned Scientology v XS4ALL case is one of the few cases where the freedom of speech prevailed over copyright law.

23 V. McEvedy (2002), The DMCA and the Ecommerce Directive, E.I.P.R. 2002, 24(2), 65-73.

24 Proposal for a EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE on certain legal aspects of electronic commerce in the internal market, 18.11.1998, COM(1998) 586 final, p. 4.

25 As is well known, these measures are not necessarily effective since circumvention is often quite easy.

26 Section 512(c)(3) of the DMCA.

27 P. Balboni et al. (2008), Liability of Web 2.0 Service Providers – A Comparative Look, Computer Law Review International Issue 3, pp. 65-71.

28 § 512 (j)(2): 'The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider—(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network; (B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement; (C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and (D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.'

29 M. Peguera (2009), The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems. Columbia Journal of Law & the Arts, Vol. 32, p. 481-512.

30 Subsequently, in February 2012, the Swedish Supreme Court decided not to grant leave on appeal, and the case is now at the European Court of Justice.

31 Court of Amsterdam, 30 July 2009, LJN BJ4298, <www.rechtspraak.nl/ljn.asp?ljn=BJ4298>.

32 Court of Amsterdam, 22 October 2009, LJN BK1067, <www.rechtspraak.nl/ljn.asp?ljn=BK1067>.

33 Court of The Hague, 19 July 2010, LJN BN1445, <www.rechtspraak.nl/ljn.asp?ljn= BN1445>.

34 Court of The Hague, 11 January 2012, LJN BV0549, <www.rechtspraak.nl/ljn.asp?ljn= BN1445>.

35 Judgment of the Court (Grand Chamber) of 12 July 2011. L'Oréal SA and Others v eBay International AG and Others. Case C-324/09.

36 Judgment of the Court (Third Chamber) of 24 November 2011. Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Case C-70/10. The filtering asked for was far-reaching; see under 40: 'filtering system would require: first, that the ISP identify, within all of the electronic communications of all its customers, the files relating

to peer-to-peer traffic; secondly, that it identify, within that traffic, the files containing works in respect of which holders of intellectual-property rights claim to hold rights; thirdly, that it determine which of those files are being shared unlawfully; and fourthly, that it block file sharing that it considers to be unlawful'.

37 A report in Dutch by the System and Network Engineering research group is available at <http://bit.ly/S9xcCZ>, J. van der Ham et al. (2012), Review en Herhaling BREIN Steekproeven, 7-9 April 2012.

38 See e.g. D.Y. Choi & A. Perez (2007), Online Piracy and the Emergence of New Business Models, Technovation, Volume: 27 Issue: 4 pp. 168-178.

39 Court of The Hague, 17 April 2012, LJN BW3596, <www.rechtspraak.nl/ljn.asp?ljn= BW3596>.

40 See note 40.

41 For a discussion of the Dutch ex parte practice, see Ex parte decision against The Pirate Bay proxy causes controversy on Future of Copyright: <http://bit.ly/UgmcVj>.

42 Mann & Belzey 2005, see note 11.

43 T. Moore & R. Clayton (2008), The Impact of Incentives on Notice and Take-down. Workshop on the Economics of Information Security (WEIS).

44 Ibidem.

45 G. Sutter (2003): 'Don't Shoot the Messenger?' The UK and Online Intermediary Liability, International Review of Law, Computers & Technology, 17:1, 73-84.

46 Dutch Supreme Court, 12 March 2004, LJN AN8483 (XS4ALL v. Ab.Fab).

47 At that time the EU Directive 2002/58 on electronic communications had been enacted, and included an Article that banned spam in the EU, at least spam sent to natural persons.

48 D.G. Lichtman & E.A. Posner, Holding Internet Service Providers Accountable (July 2004). U Chicago Law & Economics, Olin Working Paper No. 217, <http://ssrn.com/abstract=573502>.

49 J. Harper (2005), Against ISP Liability. Regulation, Vol. 28, No. 1, pp. 30-33, Spring 2005.

50 House of Lords: Science and Technology Committee (2007) Personal Internet security: 5th report of session, Vol. 1: Report: 30.

51 J.A. Chandler. Liability for Botnet Attacks. Canadian Journal of Law and Technology (2006), Vol. 5: 1.

52 M.J.G.van Eeten, & J. M. Bauer. Economics of Malware: Security Decisions, Incentives and Externalities. STI Working Paper 2008/1: 26.

53 Stol, W.PH., Kaspersen, H.W.K., Kerstens, J., Leukfeldt, E.R. & Lodder, A.R. (2009). Governmental filtering of websites: The Dutch case. Computer, Law & Security Review, 25(3), 251-262.

54 Ibidem. What happened in the Netherlands was that the police provided a list of sites to be blocked by ISPs. Only the ISPs could see the sites that were on the list. In the research by Stol et al. it appeared that this was not updated regularly, contained websites that did not distribute child porn, and of course missed many sites that did not. An additional problem with the initiative is that child pornography is hardly disseminated via public websites. The constitutional argument against this co-operation between police and ISPs was that the police asked ISPs to filter Internet traffic, which is something the police would not be legally allowed to do. After the publication of the research, the police stopped the co-operation with ISPs.

55 E. Dommering (2008), Filteren is gewoon censuur en daarmee basta (Filtering is always censoring), Tijdschrift voor Internetrecht.

56 In Section 3, Rectification and Erasure, Article 17 (Right to be forgotten and to erasure) in COM(2012) 11 final, 25 January 2012, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

57 G. Sartor (2012), Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?, <http://ssrn.com/abstract=2047428>.

58 HADOPI is also known as the Creation and Internet Law and (freely translated) stands for High authority for the dissemination of works and the protection of rights on the Internet (in French: Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet); <http://www.hadopi.fr/>.

59 Several countries acknowledge a fundamental, constitutional Internet access right.

60 <http://news.cnet.com/8301-31001_3-20077492-261/top-isps-agree-to-become-copyright-cops/>.

61 Rights and wronged: An American anti-piracy bill tries to stem the global theft of intellectual property, <http://www.economist.com/node/21540234>.

62 F. Bignami (2007), Privacy and Law Enforcement in the European Union: The Data Retention Directive, 8 Chicago Journal of International Law, Spring 2007, p. 233-255.

63 More than a third of Britons support online porn blocking, Daily Telegraph, August 19 2012, <http://bit.ly/S84SiK>.

64 For an overview of Internet filtering practices in Africa and Asia some years ago, see R. Deibert et al. (2008)(eds.), Access Denied, The MIT Press, Cambridge, Massachusetts.

65 A similar development is found in UK courts convicting people posting defamatory statements on Twitter, see e.g. Eurotech 28 March 2012 <http://bit.ly/QEvqFN>: 'Now get this clear: someone from New Zealand feels insulted by an Indian official through a statement posted on Twitter which has its shiny new headquarters in San Francisco. Why would a British judge even accept this case?'

66 Even a drastic action as in the Megaupload case would not have succeeded, since the US can shut down generic top-level domains (.com, .org) but not top-level country domains (piratebay.se).

67 M. Lemley, D.S. Levine & D.G. Post, Don't Break the Internet, 19 December 2011, 64 Stan. L. Rev. Online 34.

68 It could be the first slip on a slippery slope. See M. Schellekens, 'Liability of Internet Intermediaries: A Slippery Slope?', (2011) 8:2 SCRIPTed 154, who argues this is not the case.

Das Verhältnis zwischen Urheberrecht und Wissenschaft

Auf die Perspektive kommt es an!

by Alexander Peukert, Prof. Dr. iur., Goethe-Universität Frankfurt am Main, Fachbereich Rechtswissenschaft und Exzellenzcluster „Die Herausbildung normativer Ordnungen“

Abstract: Since the advent of digital network technologies, copyright has become a highly contentious political matter. This is also true in the area of scientific works and the scholarly communication system in general. However, whether the relationship between copyright and scholarship is considered problematic and which, if any, alternative approaches to the current system are preferred, depends upon the perspective. In that regard, the article distinguishes a copyright perspective from a perspective that takes as its starting point the philosophy and sociology of science. The article shows that only the latter, scientific perspective is capable of explaining and adequately regulating the current, fundamental change taking place in the scholarly communication system.

Keywords: Urheberrecht; Wissenschaft; Open Access; Scholarly Communication

Recommended citation: Alexander Peukert, Das Verhältnis zwischen Urheberrecht und Wissenschaft: Auf die Perspektive kommt es an!, 4 JIPITEC, 1, para 142

A. Einleitung

1 Seit dem Einzug der digitalen Netzwerktechnologie ist das Urheberrecht zu einem heftig umkämpften Politikum geworden. Dies gilt auch im Hinblick auf „Wissenschaft“ als urheberrechtlichen Schutzgegenstand.[1] Der Streit um das Wissenschaftsurheberrecht wird in verschiedenen Foren ausgetragen und ist inzwischen auch in der Sache weit verzweigt.

2 Eine Analyse dieser Auseinandersetzung ergibt, dass der Diskurs von zwei weitgehend unverbunden nebeneinander stehenden Perspektiven geprägt ist, nämlich einer urheberrechtlichen einerseits und einer wissenschaftstheoretisch/-soziologischen andererseits. Ob sich ein Sprecher die eine oder andere Betrachtungsweise zu Eigen macht, beeinflusst bereits die Haltung zur Ausgangsfrage, ob das Verhältnis zwischen Urheberrecht und Wissenschaft überhaupt als problematisch erscheint: Die urheberrechtliche Perspektive verneint (dazu II), die wissenschaftstheoretische bejaht (dazu III). Auch die jeweiligen Alternativvorschläge zur gegenwärtigen Rechtslage stehen in einem engen Zusammenhang zum gewählten Ausgangspunkt. Der urheberrechtliche Diskurs befasst sich mit Änderungen des materiellen Urheberrechts, während der wissenschaftstheoretische außerhalb des Urheberrechts ansetzt und auf die Änderung sozialer und wissenschaftsrechtlicher Normen fokussiert (dazu IV). Wie sich zeigen wird, ist nur die letztgenannte Perspektive geeignet, den gegenwärtig stattfindenden, grundlegenden Wandel des wissenschaftlichen Kommunikationssystems zu erklären und adäquate Regulierungsvorschläge zu entwickeln.

B. Urheberrechtliche Perspektive: Die Wissenschaft im Urheberrecht

3 Aus der Sicht des Urheberrechts ist „Wissenschaft“ kein besonders problematisches Rechtsobjekt. Im Gegenteil: Mit gutem Grund lässt sich sagen, dass noch nie mehr qualitätsgeprüftes, strukturiertes und

vernetztes Wissen so vielen Menschen an ihrem Arbeitsplatz verfügbar war wie in Zeiten digitaler Verlagsdatenbanken.[2] Just jenes Geschäftsmodell – die zugangskontrollierte Online-Datenbank – wird vom geltenden Urheberrecht durch eine Kombination aus rechtlicher und technischer Ausschließlichkeit ermöglicht und gefördert. Dem „Rechtsinhaber" – in der Regel der Wissenschaftsverlag und nicht der originäre Urheber – wird zu diesem Zweck „in letzter Konsequenz ... die volle Herrschaft an der Information" vermittelt,[3] die als solche zu einem als handelbaren Wirtschaftsgut wird:[4]

I. Schutzgegenstand und Schutzbereich des Wissenschaftsurheberrechts

4 Nach traditioneller Lesart verschafft das Urheberrecht eine solche Exklusivität allerdings nicht. Wissenschaftliche Sprachwerke und Darstellungen zählen zwar gem. § 2 Abs. 1 Nr. 1 und 7 UrhG zu den geschützten Werkkategorien. Schutzfähig aber ist grundsätzlich nur die „Form", also die konkrete, von der Gedankenführung geprägte Gestaltung der Sprache und das konkrete Ausdrucksmittel der grafischen oder plastischen Darstellung.[5] Die wissenschaftliche Lehre, das wissenschaftliche Ergebnis, das abstrakte Darstellungskonzept, die Rohdaten – kurz: der „Inhalt" – sind hingegen strukturell gemeinfrei.[6]

5 Die Unterscheidung zwischen „Form" und „Inhalt" ist nun freilich primär als Appell an den Rechtsanwender aufzufassen, den Schutzbereich des Urheberrechts nicht zu überdehnen. Im konkreten Fall sind die Übergänge zwischen beiden Kategorien fließend – denn Inhalt ist ohne Form nicht zu haben. So erachtet die Rechtsprechung auch die Gliederung eines Textes[7] sowie „konkrete eigenständige Verknüpfungen, Schlussfolgerungen und Auswertungen" wie zum Beispiel die Erkenntnis, dass Deutschland in der Erdbebenforschung führend wurde, obwohl es nicht zu den besonders erdbebengefährdeten Gebieten gehört, als schutzfähig.[8] Diesen „Kern rechtswissenschaftlicher Argumentationstiefe, der sich dem Laien nur schwer erschließt",[9] muss man aber gar nicht ausloten, um zu unserer eingangs formulierten Feststellung zu gelangen, dass das digitale Urheberrecht die volle Herrschaft über wissenschaftliche Informationen vermittelt.

6 Grund hierfür ist zum einen das Datenbankherstellerrecht gem. §§ 87a ff. UrhG. Demnach verfügt derjenige, der eine „wesentliche Investition" in die Beschaffung, Überprüfung oder Darstellung[10] von Werken, Daten oder anderen unabhängigen Elementen tätigt, für die Dauer von 15 Jahren nach der Veröffentlichung der Datenbank über das ausschließliche Recht, die Datenbank insgesamt oder einen im Hinblick auf die Gesamtinvestition quantitativ oder qualitativ[11] wesentlichen Teil der Datenbank zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben. Für diesen Rechtsschutz müssen keine wissenschaftlichen Werke gesammelt werden; vielmehr genügt jedes digitalisierte Element, insbesondere wissenschaftliche Rohdaten.[12] Zwar dürfen unwesentliche Teile einer Datenbank – etwa ein einzelner Datensatz – benutzt werden, ohne in das Recht des Datenbankherstellers einzugreifen. Zudem erklärt § 87c Abs. 1 Nr. 2 UrhG die Vervielfältigung eines nach Art oder Umfang wesentlichen Teils einer Datenbank zum eigenen wissenschaftlichen Gebrauch für zulässig, wenn und soweit die Vervielfältigung zu diesem Zweck geboten ist, der wissenschaftliche Gebrauch nicht zu gewerblichen Zwecken erfolgt und die Quelle deutlich angegeben wird. Allerdings bleiben wiederholte und systematische Abrufe stets verboten, so dass das Datenbankherstellerrecht etwa einem *data mining* zu Forschungszwecken entgegensteht.[13] Schon hiermit wird Wissenschaftsverlagen bzw. Investoren ein Rechtstitel gewährt, auf dessen Basis der Zugriff auf wissenschaftliche Information als solche (der „Inhalt") urheberrechtsrelevant werden kann.

7 Diese rechtliche Exklusivität lässt sich bis zu einem Pay-per-use-Geschäftsmodell ausweiten, indem technische Zugangs- und Kopierkontrollen eingesetzt werden, deren Umgehung gem. §§ 95a ff. UrhG verboten ist und die zudem in den Endnutzer-Lizenzverträgen abgebildet werden. Auf diesem Wege kann bereits der isolierte Zugriff auf einen einzelnen Datensatz und damit die einzelne wissenschaftliche Information vom Erwerb einer entgeltlichen Lizenz abhängig gemacht werden. Wer technische Zugangsbarrieren ausschaltet, begeht eine Vertrags- sowie eine ggf. strafbare Urheberrechtsverletzung.[14]

8 In dieser „himmlischen Jukebox"[15] haben die Schranken des Urheberrechts keinen Platz mehr. Denn jeder noch so geringfügige Eingriff in die technisch vermittelte Herrschaft über den Datenbankinhalt untergräbt die Wirtschaftlichkeit des Geschäftsmodells, das auf vollständiger Computerisierung der Zugriffsrechte und Zahlungspflichten beruht. Sähe sich ein Datenbankhersteller mit massenhaften Anfragen von Personen konfrontiert, die keine Lizenz erworben haben, aber unter Berufung auf § 87c Abs. 1 Nr. 2 UrhG bzw. die §§ 44a ff. UrhG dennoch Datenbankinhalte vervielfältigen wollen, würden sich schnell – so die kaum je ausgesprochene Befürchtung – prohibitive Kosten einstellen, die das Geschäftsmodell der zugangskontrollierten Online-Datenbank wirtschaftlich gefährden oder unverhältnismäßig erschweren würden.[16] Deshalb wird solchen Begehren die rechtliche Grundlage entzogen. Die ohnehin eingeschränkte und praktisch irrelevante Durchsetzung von Schrankenbestimmungen gegen technische Schutzmaßnahmen gilt im Online-Bereich gem. § 95b Abs. 3 UrhG nicht.

9 Und selbst wenn gesetzlich zulässige, digitale Nutzungen von Werken zu wissenschaftlichen Zwecken vorgenommen werden können, ohne dass hierfür Digital Rights Management (DRM)-Systeme ausgeschaltet werden müssen, räumt das geltende Urheberrecht dem zugangskontrollierten Datenbankmodell systematisch Vorrang ein. Der zustimmungsfreie elektronische Kopienversand durch Bibliotheken steht unter dem ausdrücklichen Vorbehalt, dass der Online-Zugang zu den betreffenden Werk(teil)en nicht offensichtlich zu angemessenen Bedingungen vom Rechtsinhaber ermöglicht (*angeboten*) wird.[17] Die Schranke für elektronische Leseplätze kann von den Rechtsinhabern jedenfalls im Rahmen von Lizenzverträgen mit den privilegierten Bibliotheken abbedungen werden; der Bundesgerichtshof tendiert dazu, die Regelung bereits dann für nicht einschlägig zu erachten, wenn der Verlag das betreffende Werk als E-Book *anbietet*.[18] Die zulässige öffentliche Zugänglichmachung für Forschungszwecke gem. § 52a UrhG ist nicht nur eine prekäre, weil lediglich befristete Nutzungsfreiheit innerhalb kleinerer Forschungsteams;[19] sie steht zudem wiederum unter dem Vorbehalt, dass das betreffende Werk oder der benötigte Werkteil vom jeweiligen Rechtsinhaber nicht zu angemessenen Bedingungen über das Internet *angeboten* wird. Eine gleichwohl stattfindende Nutzung sei mit Rücksicht auf die Vorgaben des Dreistufentests nicht geboten.[20] Selbiges müsste nach dem „Grundsatz des Vorrangs vertraglicher Beziehungen“[21] schließlich für die Zulässigkeit digitaler Kopien für eigene wissenschaftliche Zwecke (§ 53 Abs. 2 Nr. 1 UrhG) gelten. Diese Nutzungsfreiheit stünde somit ebenfalls unter dem Vorbehalt, dass das individuell kopierte Werk nicht offensichtlich von einem Verlag in elektronischer Form zu angemessenen Bedingungen über eine Online-Datenbank *angeboten* wird.[22]

10 Nach dieser Lesart bliebe aus dem Kreis der wissenschaftsrelevanten Schranken im digitalen Zeitalter nur noch das Zitatrecht vorbehaltlos und vergütungsfrei gewährleistet. Im Übrigen geht das EU-Urheberrecht ersichtlich davon aus, dass sich wissenschaftliche Kommunikation primär mithilfe digitaler, zugangskontrollierter Verlagsdatenbanken vollzieht. An die Stelle gesetzlicher Nutzungsbefugnisse sind vertragliche Lizenzen getreten. Jene legen abschließend fest, was der interessierte und zahlungsfähige Nutzer mit den Inhalten wissenschaftlicher Verlagsdatenbanken tun darf.

11 Insgesamt zeigt sich, dass die Schranken des Wissenschaftsurheberrechts im digitalen Zeitalter auch ohne Rücksicht auf den Vorrang von DRM-Systemen eher symbolischen Charakter haben.[23] Zur effizienten Digitalisierung der wissenschaftlichen Kommunikation tragen sie nicht in relevanter Weise bei. Vielmehr flankieren selbst die Schranken des Urheberrechts das zugangskontrollierte Datenbankmodell der Wissenschaftsverlage.[24]

II. Kompatibilität mit dem Zweck des Urheberrechts

12 Doch entspricht all dies nur der inneren Logik und der primären, historisch gewachsenen Zwecksetzung des Urheberrechts. Es stellt in Gestalt der kommerziellen Verwertungsrechte[25] Instrumente bereit, um die dezentral-marktmäßige Produktion und Verbreitung von Werken und anderen immateriellen Schutzgegenständen zu ermöglichen. Jene Rechtsobjekte werden durch die ausschließlichen, fungiblen Rechte zu handelbaren Wirtschaftsgütern. Der ganze Sinn und Zweck des Urheberrechts besteht mit anderen Worten darin, für die Bereiche der Literatur, der Wissenschaft und der Kunst private, eigentumsbasierte Geschäftsmodelle zu institutionalisieren und damit diese gesellschaftlichen Sphären der marktmäßigen Organisation zu erschließen.[26]

13 Hingegen ist es nicht Zweck des Urheberrechts, die Kommunikationsbedingungen und -normen zu stabilisieren, die außerhalb dieser Geschäftsmodelle im Literatur-, Wissenschafts- und Kunstbetrieb sonst noch vorkommen mögen. Das lässt sich gerade am Beispiel des Wissenschaftsurheberrechts nachweisen. Jenes macht sich von der Wissenschaft nämlich einen eigenständigen Begriff, der von den Selbstbeschreibungen der Wissenschaft und dem verfassungsrechtlichen Begriff der Wissenschaftsfreiheit gem. Art. 5 Abs. 3 S. 1 GG grundlegend abweicht.

14 Dort wird Wissenschaft verstanden als der nach Inhalt und Form ernsthafte und planmäßige Versuch zur Ermittlung der Wahrheit, als „die geistige Tätigkeit mit dem Ziele, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen“.[27] Nicht zur Wissenschaft in diesem Sinne zählt, was den Anspruch von Wissenschaftlichkeit systematisch verfehlt, weil die Äußerung nicht auf Wahrheitserkenntnis gerichtet ist, sondern vorgefassten Meinungen oder Ergebnissen lediglich der Anschein wissenschaftlicher Gewinnung oder Nachweisbarkeit verliehen wird.[28] Ferner umfasst die Wissenschaftsfreiheit „nicht den Schutz eines Erwerbs- oder Gewinnstrebens“.[29]

15 Der urheberrechtliche Begriff der Wissenschaft hat mit methodengerechter Wahrheitssuche und intrinsischer Wahrheitsliebe nichts zu tun. Lehrpläne werden als wissenschaftliches Sprachwerk gem. § 2 Abs. 1 Nr. 1 UrhG eingeordnet, weil sich „der [urheberrechtliche, A.P.] Bereich der Wissenschaft … nicht nur auf Forschung und Lehre im engeren verfassungsrechtlichen Sinne [beschränkt].“[30] Eine wissenschaftliche Darstellung gem. § 2 Abs. 1 Nr. 7 UrhG zeichnet sich dadurch aus, dass sie der Vermittlung von belehrenden oder unterrichtenden Informationen über den dargestellten Gegenstand dient. Dabei lässt die Rechtsprechung die Vermittlung „einfachster wissenschaftlicher Erkenntnisse“ genügen

und subsumiert Kreuzwort- und Silbenrätsel sowie Lernspiele für Kleinkinder.[31] Solche Produkte haben zweifellos einen ökonomischen Wert, um dessen Zuordnung gestritten wird. Auch mögen sie Gegenstand der Forschung sein. Lehrpläne, Kreuzworträtsel und Lernspiele dürften indes noch nie als wissenschaftliche Beiträge Eingang in eine Fachzeitschrift gefunden haben.[32]

C. Wissenschaftstheoretische Perspektive: Das Urheberrecht in der Wissenschaft

16 Die erste, nämlich die urheberrechtliche Perspektive auf das Verhältnis von Urheberrecht und Wissenschaft hat kein besonderes Problem ergeben. Das Urheberrecht macht wissenschaftlichen Output ebenso zum handelbaren Wirtschaftsgut wie Romane, Happenings und Pornographie. Wenn Wissenschaftsverlage zugangskontrollierte Datenbanken zu hohen Preisen offerieren, tun sie nichts anderes, als ein gesetzgeberisches Angebot in die praktische Tat umzusetzen.

17 Erst aus umgekehrter Perspektive wird das Wissenschaftsurheberrecht zum Problem. Betrachtet man nämlich das Urheberrecht *aus der Warte der Wissenschaft*, meinen jedenfalls manche Beobachter, dass „das Urheberrecht ... seine Funktion mit Bezug auf das wissenschaftliche Werkschaffen in wachsendem Maße [verfehlt].“[33] Mehr noch: „Nimmt man diesen Blickwinkel ein, ist der Weg zu der Erkenntnis, dass – jedenfalls im Bereich der Forschung – die ‚guten Gründe‘ für ein proprietäres Urheberrechtssystem eigentlich fehlen, nicht mehr weit.“

I. Divergente Kommunikationsbedingungen und Grundannahmen

18 Dass selbst Urheberrechtler zu einer solch irritierenden Schlussfolgerung gelangen können, beruht im Kern darauf, dass das Urheberrecht als Instrument zur Kommodifizierung von Wissenschaft (ergo sein kommerzieller Zweig) auf Annahmen basiert, die dem Selbstverständnis der Wissenschaft geradezu diametral entgegengesetzt sind:[34]

19 Spezifisch wissenschaftliche Kommunikation orientiert sich an der Leitdifferenz zwischen wahren und unwahren Aussagen.[35] Ob ein Beitrag oder ein Kommunikationsteilnehmer dem Wissenschaftssystem zuzuordnen ist, hängt davon ab, ob die Äußerung auf Wahrheitserkenntnis gerichtet ist bzw. ob der Sprecher über die erforderliche Sachkompetenz verfügt.[36] Ziel des wissenschaftlichen Gesamtunternehmens ist die Ausweitung des gesicherten Wissens.[37] Das Urheberrecht hingegen operiert mit der Leitdifferenz Recht/Unrecht und exkludiert im Hinblick auf die Frage, wer über eine ausreichende Nutzungsbefugnis verfügt, was wiederum primär von der individuellen Zahlungsbereitschaft und -fähigkeit abhängt.[38] Freilich verweist diese Gegenüberstellung zunächst nur auf das generelle Problem, dass im Rechtssystem nach rechtlichen Gesichtspunkten über nicht rechtliche Kommunikation kommuniziert wird, was zwangsläufig Engführungen und Verzerrungen mit sich bringt. Wichtiger noch ist, dass die spezifischen Grundannahmen der urheberrechtlichen und der wissenschaftlichen Kommunikation divergieren:

20 Dies betrifft zunächst die Frage nach den Anreizen, wissenschaftlich tätig zu sein. Die urheberrechtlichen Verwertungsrechte werden zum Teil damit gerechtfertigt, dass die Aussicht auf Tantiemen/Lizenzeinnahmen dazu ansporne, Werke zu schaffen. Im überwiegend staatlich grundfinanzierten Wissenschaftssystem kommt diesen Umsätzen aber eine zu vernachlässigende Bedeutung zu. Der angestellte oder verbeamtete Wissenschaftler bestreitet seinen Lebensunterhalt aus dem dauerhaften Arbeitseinkommen. In den meisten Fällen erhalten die Wissenschaftsurheber für ihre Aufsätze und Bücher keine Vergütung – man denke nur an Sammelbandbeiträge. Und selbst wenn Autorenhonorare gezahlt werden, stellen sie – abgesehen von ganz besonderen Ausnahmefällen wie etwa der ständigen Mitarbeit an einem juristischen Standardkommentar wie dem *Palandt*™ – nicht mehr als ein gelegentliches Zubrot dar, das der Einzelne gern verbucht, das aber nicht ausreichen würde, um dauerhaft wissenschaftlich – und das heißt prinzipiell nicht kommerziell – tätig sein zu können.[39] Vorrangige Bedeutung besitzen vielmehr intrinsische Motivationsquellen wie insbesondere die Freude an einsamer und freier Wahrheitssuche[40] sowie das extrinsische Motiv, wissenschaftliche Reputation zu erlangen, die sich später ggf. versilbern lässt.[41] Der Reputationserwerb setzt lediglich voraus, dass Wissenschaftler geltend machen können, Autor bestimmter Äußerungen zu sein. Dieses ideelle Interesse gewährleistet das Urheberpersönlichkeitsrecht in Gestalt des Integritätsschutzes und des Namensnennungsrechts. Im Gegensatz zu den Verwertungsrechten verhält sich das Urheberpersönlichkeitsrecht folglich komplementär zu den Anforderungen des wissenschaftlichen Kommunikationssystems, in dem die Selektion lesenswerter Texte häufig anhand des Namens und der hiermit verknüpften Reputation einzelner Wissenschaftler erfolgt.[42] Eine kritische Analyse des Wissenschaftsurheberrechts hat daher stets sorgfältig zwischen den Verwertungs- und den Urheberpersönlichkeitsrechten zu unterscheiden.

21 Auch im Hinblick auf die je eigenen Kommunikationsstrukturen, -bedingungen und -normen weichen das kommerzielle Urheberrecht und die Wissenschaft durchweg voneinander ab. Wissenschaft wird als prinzipiell unabgeschlossener[43] Zusammenhang, als prozesshaftes Netzwerk individueller Versuche zur Ermittlung von Wahrheit beschrieben.[44] Die einzelnen Anläufe müssen publiziert werden und zugänglich bleiben, damit über Zitate Verknüpfungen hergestellt, Aussagen kritisch überprüft und ggf. falsifiziert werden können.[45] Als wissenschaftlich relevant und originell gilt die Leistung, neue Wahrheiten auszusprechen, also etwas zu entdecken oder zu erfinden;[46] in den Geisteswissenschaften findet auch die Art und Weise (die „Form"), wie Wahrheit erklärt und vermittelt wird, Anerkennung.[47] Unveröffentlichte Manuskripte entziehen sich diesem Wettbewerb der Ideen von vornherein und zählen daher schon gar nicht zum wissenschaftlichen Diskurs.[48] Ferner zeichnet sich wissenschaftliche Kommunikation dadurch aus, dass sie universell, also unabhängig von personalen oder sozialen Eigenschaften des Sprechers sowie unabhängig vom Ort und der Zeit ihrer Äußerung entweder wahr oder aber unwahr ist,[49] dass der Kommunikationszusammenhang deshalb eine globale Einheit darstellt,[50] und dass zunehmend kollaborativ geforscht wird.[51] Je näher die praktischen Kommunikationsbedingungen diesen Beschreibungen kommen, und das heißt, je offener und vollständiger wissenschaftliche Ergebnisse verfügbar sind, desto intensiver und schneller kann die weitere Erzeugung vorläufig akzeptierten Wissens ablaufen.[52]

22 Die Strukturmerkmale des Urheberrechts besagen in all diesen Hinsichten etwas Anderes und zum Teil das glatte Gegenteil: Rechtsobjekt des Urheberrechts ist nicht ein dynamischer Prozess, sondern eine genau zu identifizierende, für immer feststehende Einzelheit: das Werk.[53] Jenes wird auch und sogar besonders intensiv geschützt, solange es unveröffentlicht ist. Schutzfähig ist nicht die neue Entdeckung oder Theorie als solche („Inhalt"), sondern die konkrete „Form" der Versprachlichung oder der grafischen/plastischen Darstellung. Demzufolge ist begünstigter Urheber nicht zwangsläufig der wissenschaftliche Pionier, der mit einer Entdeckung oder Theorie wissenschaftliche Reputation gewinnt, sondern derjenige, der die neue Information in eine konkrete Sprach- oder sonstige Darstellungsform bringt.[54] Hierbei ist stets eine individuelle Zuordnung der geistigen Leistung zu einem bestimmten Autor vorzunehmen; Kollektive können nicht „Schöpfer" sein. Schließlich existiert kein Welturheberrecht. Der globalen Kommunikation unterliegt ein Flickenteppich von mehr als 180 nationalen Urheberrechten, die einer Fragmentierung des Internets entlang längst überwunden geglaubter Staatsgrenzen Vorschub leisten.[55]

23 All diese Unterschiede kulminieren in grundlegend abweichenden Charakterisierungen wissenschaftlichen Outputs durch die globale Gelehrtenrepublik einerseits und das Urheberrecht andererseits. Die Wissenschaft betrachtet ihre Ergebnisse, zumindest die Rohdaten, Theorien, Entdeckungen und Erfindungen, als öffentliches Gut,[56] das allen[57] oder niemandem[58] gehört. Das digitale Urheberrecht hingegen macht wie erläutert selbst diese „Inhalte" zu privat-exklusiven, handelbaren Wirtschaftsgütern.

	24 Wissenschaft	25 Urheberrecht
Leitdifferenz	wahr/unwahr	Recht/Unrecht zahlen/nicht zahlen
Inklusion/Exklusion	Sachkompetenz	Berechtigung und Zahlung
Anreizmechanismen	intrinsisch, Reputation	extrinsisch: Vergütung
Strukturmerkmale	Prozess, Netzwerk Offenheit Vollständigkeit Kollaboration Universalität/Globalität	Objekt Exklusivität Einzelheit individuelle Autorschaft Territorialität (national)
Relevanzkriterien	Veröffentlichung neues Wissen (Information)	Schöpfung, auch unveröff. Kreativität („Form")
Relevantes Ergebnis	primär Information („Inhalt")	„Form", aber mittelbar auch Information (DRM)
Zuordnung des Ergebnisses	nein: öffentliches Gut	ja: Privateigentum

II. Auswirkungen der Unterschiede im digitalen Zeitalter

26 Im analogen Zeitalter mussten die dargestellten, strukturellen Unterschiede zwischen Wissenschaft und Urheberrecht hingenommen werden, da die technisch-organisatorisch anspruchsvolle Aufgabe der Wissensvermittlung nur mithilfe von Verlagen bewältigt werden konnte. Hinzu traten praktisch bedeutsame Freiheiten zur Nutzung des wissenschaftlichen „Inhalts", zur Herstellung von Kopien für den eigenen wissenschaftlichen Gebrauch sowie flankierend zum Kopienversand durch Bibliotheken.[60]

27 Die Digitalisierung und das Internet haben diese Ausgangsbedingungen des klassischen wissenschaftlichen Publikationssystems grundlegend verändert. Nunmehr sind die Wissenschaftler in der Lage, die

Darstellung und die globale Verbreitung ihrer Ergebnisse ohne Weiteres selbst zu übernehmen; eines klassischen Wissensvermittlers bedürfen sie hierfür im Prinzip nicht mehr.[61]

28 Gleichwohl wurde das Urheberrecht und mit ihm das exklusive Vermarktungsmodell in den 1990er Jahren auf digitale Netzwerke erstreckt. Hier besteht das vom Urheberrecht ermöglichte Geschäftsmodell in der zugangskontrollierten Online-Datenbank, die wie erläutert die volle Herrschaft über die wissenschaftliche Information vermittelt. Damit realisiert sich auch im Wissenschaftsurheberrecht das digitale Dilemma: Die Digitalisierung erlaubt maximalen Zugang und zugleich maximale Kontrolle.[62]

29 Dieser fundamentale Konflikt äußerte sich um die Jahrtausendwende in der sog. Zeitschriften(preis)krise.[63] Eine immer kleiner werdende Zahl namentlich in den Natur- und Lebenswissenschaften tätiger Wissenschaftsverlage verlangte für immer umfangreicher werdende Datenbankpakete immer höhere Preise, deren Steigerungsraten systematisch über dem allgemeinen Preisindex lagen. Die betreffenden Entgelte und Gewinne können realisiert werden, weil die in den Datenbanken verfügbaren wissenschaftlichen Informationen praktisch nicht substituierbar sind, so dass sich die Nachfrage der Wissenschaftler und der für sie verhandelnden Bibliotheken ausgesprochen unelastisch verhält.[64]

30 Als aber die Bibliotheksetats mit dieser Entwicklung nicht mehr Schritt halten konnten und Zeitschriften, Bücher und Datenbanken abbestellt werden mussten, wurde offenbar, dass sich das Versprechen des Netzes, allumfassenden, globalen Zugang zu gewähren, in sein Gegenteil zu verkehren drohte. Es zeichnete sich eine wachsende digitale Kluft zwischen denjenigen ab, die von einer (schrumpfenden) Campus- oder Nationallizenz profitieren können, und denjenigen, die außerhalb der Wissenschaftsorganisationen[65] und generell im globalen Süden ohne Zugang auskommen müssen. Zwar vollzogen die Verlage nur die innere Logik des vom Urheberrecht ermöglichten Datenbankmodells, wonach gilt, dass mehr Inhalt größere Nachfrage erzeugt, die zu höheren Preisen befriedigt werden kann, was zu weiteren Investitionen in größere und bessere Datenbanken Anlass gibt, wodurch wiederum mehr Inhalte verfügbar werden usw.

31 Je mehr aber an dieser Exklusivitäts- und Preisschraube gedreht wurde, desto schärfer trat die auch aus urheberrechtlicher Sicht atypische Wertschöpfungskette im Wissenschaftsbereich hervor: Die Herstellung, die Darstellung und die Qualitätskontrolle (peer review) wissenschaftlicher Ergebnisse werden ganz überwiegend aus Steuermitteln finanziert. Zugeordnet aber werden diese Ergebnisse dem einzelnen Wissenschaftler, der seine Urheberrechte in der Regel unentgeltlich einem Verlag einräumt, welcher schließlich den Output des steuerfinanzierten Systems als privates Wirtschaftsgut an die öffentliche Hand gegen Entgelt rücklizenziert.[66]

32 Jetzt erst erschien das Urheberrecht den öffentlichen Forschungsfinanziers und vielen Wissenschaftlern nicht mehr als der wissenschaftlichen Kommunikation förderlich oder zumindest als notwendiges Übel, sondern als geradezu überflüssiges Hindernis.[67] Allein mit dem Hinweis darauf, dass das urheberrechtlich ermöglichte Datenbankmodell doch funktioniere, können sich die Rechtsinhaber nicht mehr aus der Affäre ziehen, da dieses Geschäftsmodell als solches zur Disposition steht.

33 Und in der Tat genügt eine selbstreferentielle Eigentumslogik nicht, um das Urheberrecht zu legitimieren. Vielmehr muss sich das Eigentum immer wieder die Frage gefallen lassen, inwieweit es seine akzessorischen Zwecke erfüllt.[68] Aus verfassungsrechtlicher Sicht gewährleistet das Eigentum ein eigenverantwortliches Leben im vermögensrechtlichen Bereich.[69] Diese Rechtfertigung läuft für das Urheberrecht im öffentlich geförderten Wissenschaftsbereich wie erläutert allerdings weithin leer.

34 Die Verfechter des Status quo argumentieren denn auch anders, nämlich im Hinblick auf die Kommunikationsbedingungen der Wissenschaft. Demnach stelle nur das urheberrechtsbasierte Verlagssystem wissenschaftsadäquate Kommunikationsstrukturen bereit. Allein das qualitätsgeprüfte, lektorierte und gedruckte Werk erlaube ein vertieft-entschleunigtes,[70] sorgfältiges und kreatives Lesen und Schreiben, während die Open-Access-Ideologie zu einer Verflachung, ja zu einer Zerstörung des wissenschaftlichen Diskurses führe.[71]

35 So berechtigt diese kulturpessimistischen Bedenken im Hinblick auf die Folgen der Digitalisierung zum Teil sein mögen[72] – das gegenwärtige Verlagsgebaren vermögen sie nicht zu legitimieren. Nicht nur, dass Klagen über zu viele, kaum wahrgenommene und qualitativ schlechte wissenschaftliche Veröffentlichungen schon zu Zeiten des Buchdrucks weit verbreitet waren.[73] Entscheidend ist, dass das geltende Urheberrecht die Digitalisierung des Wissens fördern soll, wenngleich in einer bestimmten, nämlich zugangskontrollierten Weise. Dementsprechend gehen viele Verlage auf der Basis ihrer digitalen Ausschließlichkeitsrechte dazu über, Zeitschriften und andere Inhalte auch oder sogar nur noch elektronisch anzubieten und ihre Produkte auch sonst auf die Bedürfnisse des digitalen Lesers zuzuschneiden. Das Urheberrechts- und Verlagssystem sind der „Digitalisierungsideologie“ mit all ihren durchaus problematischen Effekten im Hinblick auf permanente Aktualisierung und möglichst schnelle Verfügbarkeit[74] nicht minder anheimgefallen als die Open-Access-Bewegung und ihre Nutznießer – zu denen im Übrigen auch ihre Kritiker zählen.[75] Es ist da-

her verfehlt, das digitale Urheberrecht unter Hinweis auf die Vorzüge der klassischen Buchkultur zu verteidigen.

D. Urheberrechtliche und wissenschaftstheoretische Alternativen zum Status quo

36 Das digitale Dilemma im wissenschaftlichen Kommunikationssystem hat eine Vielzahl alternativer Regulierungsvorschläge hervorgerufen. Auch insoweit kann die Unterscheidung zwischen einer urheberrechtlichen und einer wissenschaftstheoretischen/-soziologischen Perspektive fruchtbar gemacht werden.

I. Urheberrechtsperspektive: Reform des materiellen Urheberrechts

37 In der urheberrechtlichen Diskussion steht naturgemäß der Änderungsbedarf des materiellen Wissenschaftsurheberrechts im Vordergrund. Der radikalste Ansatz in dieser Richtung findet sich in einem US-amerikanischen Gesetzentwurf aus dem Jahr 2003, wonach der US Copyright Act dahingehend geändert werden sollte, dass „copyright protection ... is not available for any work produced pursuant to scientific research substantially funded by the Federal Government ...".[76] Freilich ist dieser „Public Access to Science Act" bereits an den ersten Hürden des US-amerikanischen Gesetzgebungsverfahrens gescheitert und seitdem nicht wieder aufgegriffen worden. Ein Grund hierfür ist rechtlicher Natur. Die Aufhebung des Urheberrechts für wissenschaftliche Werke ist mit den völkerrechtlichen Konventionen zum Urheberrecht unvereinbar.[77]

38 Die Diskussion um das Wissenschaftsurheberrecht konzentriert sich daher auf eine Erweiterung der wissenschaftsrelevanten Schranken. So diskutiert man bei der WIPO über ein völkerrechtliches Abkommen im Interesse von Bildung und Wissenschaft, ohne bisher auch nur in die Nähe eines internationalen Konsenses gekommen zu sein.[78] Auf nationaler Ebene haben verschiedene Gremien des Bundestages und zuletzt der Bundesrat die Einführung einer „breiter und allgemeiner gefasste[n] Bildungs- und Wissenschaftsschranke" gefordert.[79] Ein konkreter Formulierungsvorschlag geht dahin, dass Schriftwerke, „die im Rahmen einer überwiegend mit öffentlichen Mitteln finanzierten Lehr- und Forschungstätigkeit entstanden sind und in Periodika erscheinen, sechs Monate nach ihrer Erstveröffentlichung zur Informationsteilhabe der Allgemeinheit öffentlich zugänglich" gemacht werden dürfen, „soweit dies zur Verfolgung nicht kommerzieller Zwecke gerechtfertigt ist".[80] Der Vorbehalt zugunsten nicht kommerzieller, wissenschaftlicher Nutzungszwecke nimmt auf Art. 5 Abs. 3 lit. a UrhRL 2001/29 Rücksicht. Auch diese Restriktion wird als problematisch empfunden, weil kommerzielle Forschung in Unternehmen ebenfalls auf umfassenden Zugang angewiesen sei.[81] Gefordert wird daher eine entsprechende Änderung des europäischen Urheberrechts, und zwar auch im Hinblick auf eine Neuregelung des Rechtsschutzes technischer Schutzmaßnahmen, die keinen Vorrang mehr vor den Schranken des Urheberrechts genießen sollen.[82] Noch weiter geht die Anregung, in die UrhRL 2001/29 eine Regelung aufzunehmen, wonach der Urheber eines Werks verpflichtet wäre, ein elektronisches Pflichtexemplar an die jeweilige Nationalbibliothek abzuliefern, die es anschließend in dieser Form öffentlich zugänglich machen darf.[83]

39 Den Vorschlägen zur Erweiterung der urheberrechtlichen Schranken ist gemeinsam, dass das ausschließliche Recht an wissenschaftlichen Werken im Hinblick auf bestimmte Nutzungen auf einen Vergütungsanspruch des Urhebers reduziert wird. Nutzungsberechtigt und zugleich zahlungsverpflichtet wären öffentliche Forschungs- und Bildungseinrichtungen. Obwohl sie zu nicht kommerziellen Zwecken agieren, träte ihr Informationsangebot praktisch doch in Konkurrenz zu den zugangskontrollierten Datenbanken der Verlage.

40 Einen anderen Ansatz verfolgen Modelle zu Zwangslizenzen[84] bzw. zu einem Kontrahierungszwang.[85] Mit diesen Instrumenten sollen die Verlage verpflichtet werden, den Inhalt ihrer Datenbanken für Mitbewerber zu öffnen, die diese wissenschaftlichen Informationen sodann in anders aufbereiteter Form anbieten dürften, so dass sich ein Preiswettbewerb zwischen mehreren kommerziellen Datenbankanbietern einstellen würde, die im Prinzip substituierbare Produkte offerieren. Der erwünschte Effekt bestünde zum einen in fallenden Preisen für wissenschaftliche Datenbanken, zum anderen in einem verstärkten Ansporn für die Verlage, die wissenschaftlichen Inhalte optimal aufzubereiten und zu vernetzen.

41 Sowohl die Vorschläge für eine große Wissenschaftsschranke als auch die zuletzt genannten Ansätze laufen darauf hinaus, dass wissenschaftliche Werke nicht mehr exklusiv in einer zugangsbeschränkten Verlagsdatenbank vorhanden wären, sondern dass eine weitere Informationsquelle zur Verfügung stünde. Die Konzepte unterscheiden sich allerdings hinsichtlich der Frage, ob diese weitere Quelle ein frei zugänglicher Server öffentlicher Bildungs- und Forschungseinrichtungen (Schrankenlösung) oder aber eine ebenfalls DRM-geschützte Datenbank eines oder mehrerer weiterer, kommerzieller „Informationsbroker" (Zwangslizenzmodell) sein soll. Wäh-

rend die Verfechter einer großen Wissenschaftsschranke vor allem den ungehinderten Zugang zu wissenschaftlicher Information gewährleisten wollen, sorgen sich die Vertreter eines Zwangslizenz- bzw. eines Kontrahierungszwangsmodells vorrangig um die Strukturierung und Aufbereitung einer sonst überbordenden Datenflut.

42 Freilich sehen sich insbesondere Vorschläge zugunsten einer weiten Wissenschaftsschranke dem Einwand ausgesetzt, sie seien mit dem internationalen und europäischen Urheberrecht unvereinbar, weil ein solch gesetzgeberischer Eingriff die „normale Verwertung" wissenschaftlicher Schutzgegenstände in Gestalt des exklusiven Datenbankmodells beeinträchtige. Derartige Bedenken sind jedenfalls insofern berechtigt, als das digitale Urheberrecht gerade den Zweck hat, Urhebern und ihren Vertragspartnern volle Ausschließlichkeit bis hin zu einer Pay-per-use-Gestaltung zu verschaffen. Vorschläge, die dieses Geschäftsmodell im Kern aushöhlen, sind deshalb mit dem geltenden internationalen und europäischen Urheberrecht in der Tat unvereinbar.[86] Hieraus folgt: „Für die Wissensorganisation scheidet ... eine Option aus: die völlige Neugestaltung eines allein an der digitalen Wirklichkeit ausgerichteten Urheberrechtssystems."[87]

43 Hingewiesen sei schließlich auf eine strukturelle Schwäche aller am Urheberrecht ansetzenden Lösungsvorschläge. So wie das Urheberrecht selbst, gelten auch Schranken, Zwangslizenzen und Kontrahierungszwänge nur auf dem Territorium desjenigen Gesetzgebers, der diese Regelungen erlassen hat.[88] Eine auf Deutschland oder die EU begrenzte und deshalb auch nur hier implementierbare Regelung im Interesse der digitalen Wissenschaft verfehlt aber von vornherein den inhärent globalen Charakter wissenschaftlicher Kommunikation. Namentlich die digitale Kluft zwischen Nord und Süd bliebe bestehen.[89]

44 Diese Defizite genuin urheberrechtlicher Reformvorschläge sind unvermeidlich, da sie in der Logik des Urheberrechts und seinen international festgeschriebenen Grundsätzen gefangen sind. Die ökonomischen Argumente („Marktversagen") der Kritiker reflektieren zwar zutreffend den Charakter des Urheberrechts als Instrument zur Ermöglichung bestimmter Geschäftsmodelle.[90] Die Bedingungen spezifisch wissenschaftlicher Kommunikation aber lassen sich mit diesen juristisch-wirtschaftlichen Erwägungen gerade nicht adressieren.[91] Wenn sich die Kommunikationslogiken des Urheberrechts und der Wissenschaft so fundamental unterscheiden wie oben dargestellt, dann kann eine Angleichung beider Sphären nicht über eine Reform des Urheberrechts erreicht werden, das seinen Namen noch verdient.

II. Wissenschaftsperspektive: Open Access

45 Solche inhärenten Limitierungen vermeidet eine wissenschaftstheoretische-/-soziologische Perspektive, die wissenschaftsadäquate, digitale Kommunikationsstrukturen ohne Änderung des Urheberrechts zu etablieren sucht. Genau dies nimmt die Open-Access (OA)-Bewegung für sich in Anspruch. Sie propagiert die freie Zugänglichkeit wissenschaftlicher Ergebnisse im Internet, die von allen interessierten Nutzern weltweit zu jedem legalen Zweck verwendbar sein sollen.[92]

1. Open Access und Urheberrecht

46 Dieses Ideal lässt sich in der Tat ohne Änderung des Urheberrechts erreichen. Originäre Inhaber des Urheberrechts an wissenschaftlichen Werken sind in aller Regel die Wissenschaftler.[93] Halten sie einen Text etc. für publikationsreif – eine sehr sensible Entscheidung, die in allen OA-Modellen unberührt bleibt[94] –, obliegt es ihnen, ob sie Verlagen ausschließliche Nutzungsrechte einräumen und damit das zugangskontrollierte Datenbankmodell bestücken oder ob sie ihre Ergebnisse ohne rechtliche und technische Barrieren im Internet verfügbar machen.[95] Das Urheberrecht zwingt die Wissenschaftler also keineswegs in eine möglichst exklusive Verwertungsform. Vielmehr können sie sich auch dazu entscheiden, das Werk vollständig oder unter bestimmten Bedingungen zur Nutzung freizugeben. Die meisten Urheberrechtsgesetze der Welt erlauben einen endgültigen Verzicht auf die Verwertungsrechte, mit der Folge, dass das Werk gemeinfrei wird.[96] Und selbst das insofern restriktive deutsche Urheberrecht sieht ausdrücklich vor, dass der Urheber jedermann ein einfaches, unentgeltliches Nutzungsrecht einzuräumen vermag;[97] hinzu tritt die Gestaltungsvariante, formlos und konkludent in übliche Nutzungshandlungen einzuwilligen.[98] Jeweils kann sich der Urheber bestimmte Rechte vorbehalten, insbesondere im Hinblick auf unmittelbare kommerzielle Nutzungen und das Urheberpersönlichkeitsrecht.[99] Das Urheberrecht steht somit selbst einer sofortigen, vollständigen und weltweiten Umstellung der wissenschaftlichen Kommunikation auf Open-Access-Erstveröffentlichungen nicht entgegen – wenn die entscheidungsbefugten Wissenschaftler dies denn wünschen.

47 Zudem kann das Urheberrecht auch dergestalt flexibel ausgeübt werden, dass einem Verlag ggf. für eine bestimmte Zeit ein ausschließliches Nutzungsrecht eingeräumt wird, der Urheber sich aber vorbehält, das Werk selbst oder durch Dritte zeitgleich, zeitverzögert, in derselben oder einer abweichenden Formatierung zu nicht kommerziellen Zwecken öffentlich zugänglich zu machen.[100] Mit anderen Worten

ermöglicht das Urheberrecht auch ein Nebeneinander des Verlags- und des OA-Modells.[101] Das Urheberrecht gewährleistet aus dieser Perspektive vor allem eine Entscheidungsbefugnis des Wissenschaftler-Urhebers für die eine und/oder eine andere Form der wissenschaftlichen Publikation.

48 Mit dem Fokus auf diese Weichenstellung verlagert sich das Interesse weg vom stets vorausgesetzten Urheberrecht hin zu den wissenschaftsinternen Publikationsnormen, die für die Entscheidung für das eine oder das andere System maßgeblich sind. Dementsprechend setzen regulatorische Maßnahmen zur Förderung von Open Access nicht im Urheberrecht, sondern im Wissenschaftsrecht an.[102] Freilich ergeben sich auch dann Wechselwirkungen. Würde Open Access auf wissenschaftsrechtlicher Grundlage gefördert oder gar flächendeckend eingeführt, schwächte sich der urheberrechtliche Standard des wissenschaftlichen Publikationswesens von „alle Rechte vorbehalten" auf „einige Rechte vorbehalten" ab.

2. Vorzüge von Open Access

49 Ein solcher Paradigmenwechsel wird in der Wissenschaftstheorie, der Ökonomik und der Wissenschaftspolitik mit Blick auf die oben geschilderten, wissenschaftsinternen Kommunikationsbedingungen ganz überwiegend als wünschenswert erachtet.[103] Erstens verbessert Open Access die Voraussetzungen, damit die Wissenschaft ihre Funktion, neues gesichertes Wissen zu generieren, erfüllen kann:

- Da das vorhandene Wissen umfassender verfügbar und über interaktive Elemente intensiver vernetzt ist,[104] lassen sich doppelte, ggf. bereits falsifizierte Anstrengungen vermeiden;
- wissenschaftliche Ergebnisse können schneller veröffentlicht werden;[105]
- die Kommunikation verläuft global und nicht mehr entlang von Campus- oder systemfremden Staatsgrenzen;[106]
- Erkenntnisse anderer Disziplinen können leichter gefunden und rezipiert werden;
- die Zugangshürden für noch nicht etablierte Wissenschaftler werden gesenkt, so dass zugleich eine leistungsgerechtere Verteilung von Reputationsgewinnen möglich erscheint.[107]

50 Zweitens verspricht Open Access eine verbesserte Kommunikation über die Grenzen des engeren, öffentlich finanzierten Wissenschaftsbetriebs hinaus. Die freie Verfügbarkeit wissenschaftlicher Ergebnisse versetzt die Politik und die Gesellschaft (die Medien) in die Lage, die Entwicklung der Wissenschaft nachzuverfolgen und die Verwendung von Steuergeldern zu prüfen.[108] Außerdem erleichtert und intensiviert Open Access die Vermittlung von Forschungsergebnissen an die übrige Wissensgesellschaft, namentlich an die ihrerseits forschende Wirtschaft, die bisher nicht von Nationallizenzen profitiert, sondern häufig gezwungen ist, im inhärent limitierten Pay-per-use-Modus zu operieren.[109] Die positiven Externalitäten dieses Transfers werden im ökonomischen Modell für so erheblich erachtet, dass sie die Nettomehrkosten einer Umstellung auf Open Access selbst dann übersteigen sollen, wenn Deutschland sich in einem nationalen Alleingang für einen solchen Systemwechsel entschiede:[110]

51 Die genannten Vorzüge schlagen sich in Umfrageergebnissen nieder, wonach 80 bis 90 % der Wissenschaftler über Disziplin- und Ländergrenzen hinweg Open Access für einen positiven und förderungswürdigen Ansatz halten.[111] Die Zahl der frei verfügbaren Beiträge, der institutionellen und fachlichen Repositorien sowie der OA-Zeitschriften steigt seit Jahren kontinuierlich und überproportional zur Steigerung des gesamten Veröffentlichungsaufkommens an.[112] In manchen Disziplinen wie etwa bestimmten Bereichen der Physik, aber auch der englischsprachigen Rechtswissenschaft wird es bereits schwierig, Reputation aufzubauen, ohne in den zentralen OA-Fachrepositorien wie ArXiv bzw. dem Social Science Research Network (SSRN) vertreten zu sein.

52 Zugleich jedoch stellt auch mehr als 20 Jahre nach der Entstehung der ersten OA-Repositorien und -Zeitschriften das verlagsseitig produzierte *peer reviewed journal* den Goldstandard der wissenschaftlichen Publikation dar. In Umfragen bekunden 80 % der Wissenschaftler, dieses Medium sei das erste ihrer Wahl.[113] Dem entspricht der Befund, dass der Anteil der OA-Publikationen am Gesamtumfang wissenschaftlicher Veröffentlichungen bei erheblichen Unterschieden zwischen den Disziplinen auf lediglich 5 bis 30 % geschätzt wird.[114] Ohne Verlage, so scheint es, kommt die Wissenschaft auch im 21. Jahrhundert nicht aus.[115] Selbst die eigenen Grundbegriffe der OA-Bewegung, nämlich der „goldene" bzw. „grüne" OA, werden noch häufig unter Referenz auf den Normalfall der ggf. vorgeschalteten Veröffentlichung in einer Verlagszeitschrift definiert.[116]

53 Eine Ursache für die vordergründig langsame Etablierung dieses alternativen Modells ist tatsächlich urheberrechtlicher Natur. Hat nämlich ein Wissenschaftler einem Verlag uneingeschränkte ausschließliche Rechte an seinem Werk eingeräumt, hat er sich in Ausübung seiner Privatautonomie seines Rechts begeben, für offenen Zugang zu optieren. Dieses Szenario wird als relevantes Hindernis für eine größere Verbreitung des grünen OA eingeschätzt, da keineswegs alle Verlagsverträge von vornherein eine parallele OA-Publikation des Manuskripts gestatten.[117]

54 Der sich ergebende Lock-in-Effekt soll durch ein zwingendes Zweitverwertungsrecht des Urhebers durchbrochen werden. Nach einem Regierungsentwurf für einen neuen § 38 Abs. 4 UrhG hat der Urheber

55 „eines wissenschaftlichen Beitrags, der im Rahmen einer mindestens zur Hälfte mit öffentlichen Mitteln geförderten Forschungstätigkeit entstanden und in einer periodisch mindestens zweimal jährlich erscheinenden Sammlung erschienen ist, ... auch dann, wenn er dem Verleger oder Herausgeber ein ausschließliches Nutzungsrecht eingeräumt hat, das Recht, den Beitrag nach Ablauf von zwölf Monaten seit der Erstveröffentlichung in der akzeptierten Manuskriptversion öffentlich zugänglich zu machen, soweit dies keinem gewerblichen Zweck dient. Die Quelle der Erstveröffentlichung ist anzugeben. Eine zum Nachteil des Urhebers abweichende Vereinbarung ist unwirksam.“.[118]

56 Das *zwingende* Zweitverwertungs*recht* stellt den Grundsatz der Freiwilligkeit von Open Access nicht in Frage.[119] Eingeschränkt wird die Verfügungsbefugnis des Urhebers im Verhältnis zu verhandlungsstärker eingeschätzten Verlagen, nicht hingegen der Schutzbereich des Urheberrechts. Zutreffend wird der Vorschlag deshalb als völker-, unions- und verfassungsrechtlich unbedenklich eingestuft. Das Risiko, dass ausländische Verlage aufgrund der nicht abdingbaren OA-Option keine Verlagsverträge mehr mit in Deutschland ansässigen Wissenschaftlern[120] abschließen, erscheint relativ gering und in Anbetracht des gestärkten Wahlrechts der inländischen Urheber hinnehmbar.[121]

57 Doch selbst wenn ein solches Zweitverwertungsrecht Eingang in das Urheberrecht fände, würde dies an den vielfältigen wissenschaftsinternen Vorbehalten und Hemmnissen im Hinblick auf Open Access nichts ändern. Die Wissenschaftler verfolgen insoweit durchaus andere Interessen als die öffentlichen Wissenschaftsfinanziers und die Bibliotheken.[122] Während offener Zugang in der Recherche- und Herstellungsphase hoch geschätzt wird, sieht man sein fertiges Produkt unverändert am liebsten in der Verlagsdatenbank, die weiterhin die reputationsförderlichste Sichtbarkeit garantiert.[123]

58 Diese Beharrungseffekte beruhen auf einer konservativen Grundhaltung der wissenschaftlichen Community im Hinblick auf ein funktionierendes, auch Elite signalisierendes Publikationswesen[124] sowie auf Pfad- bzw. Strukturabhängigkeiten, die sich maßgeblich an der Frage orientieren, wie wissenschaftliche Macht erworben und erhalten wird.[125] So fungieren Herausgeberschaften als Reputationssignale, die ihr Träger unter Einbindung abhängiger Nachwuchswissenschaftler pflegt und nicht gern aufgibt.[126] Generell lässt sich die These aufstellen, dass es um so schwieriger ist, Open Access über neue Publikationsmedien zu etablieren, je stärker Reputation in einem Fach konzentriert ist.[127]

3. Open Access als neuer Standard wissenschaftlicher Kommunikation

59 Bisher hat man sich namentlich in Deutschland darauf beschränkt, an die Wissenschaftler zu appellieren, diese Vorbehalte aufzugeben und ihre Ergebnisse frei verfügbar zu machen.[128] Wo sich – wie etwa im Forschungsförderungsrecht der Schweiz und der EU – bereits grundsätzliche Verpflichtungen zu OA-Publikationen finden, stehen diese stets unter dem Vorbehalt, dass der Autor keinem Verlag ausschließliche Rechte eingeräumt hat, so dass Open Access letztlich auch hier eine freiwillige Veranstaltung bleibt.[129]

60 Einen erheblichen Schritt weiter gehen jüngste Bestrebungen im Wissenschaftsrecht des Vereinigten Königreichs und der USA, die sich die EU offenbar zum Vorbild nehmen möchte. Sie beruhen auf dem Gedanken, dass sich das wissenschaftliche Publikationswesen derzeit im Übergang vom Verlags- zum OA-System befindet und dass dieser Wandel intelligent zu gestalten und zu fördern ist.[130] Zu diesem Zweck werden die öffentlich finanzierten Wissenschaftler einerseits auf OA-Publikationen verpflichtet. Andererseits ist diese Pflicht so ausgestaltet, dass es zu einer Koexistenz von Open Access und Verlagsangeboten kommt, deren Geschäftsmodell nicht in Frage gestellt wird, da sie (gegenwärtig noch) einen wichtigen Beitrag für das Funktionieren der wissenschaftlichen Kommunikation leisteten. Insbesondere werden Mittel für Autorengebühren bereitgestellt, mit denen sich die Wissenschaftler die freie Zugänglichkeit ihrer Beiträge erkaufen können (goldener OA). Die Erstveröffentlichung in proprietären Formaten bleibt ebenfalls erlaubt, soweit der Aufsatz nach einem maximalen Embargo von bis zu 12 Monaten frei zugänglich gemacht wird (grüner OA).[131]

61 Eine Umsetzung dieser Vorgaben würde bewirken, dass zumindest nach einer gewissen Zeit sämtliche von den Regularien erfassten Beiträge/Ergebnisse ohne rechtliche oder technische Hürden im Internet verfügbar wären. Zugleich würden sich diese Inhalte z.T. auch noch in zugangskontrollierten Verlagsdatenbanken finden. Freilich ist zu erwarten und wohl auch erwünscht, dass das OA-System zunehmend von seiner Vollständigkeit profitiert, so dass sich Netzwerkeffekte einstellen, die an einem bestimmten *tipping point* dazu führen, dass von vornherein in diesem Modus erstveröffentlicht wird. Verlagsdatenbanken würden graduell und ab dem Umkipppunkt rasant an Bedeutung verlieren und könnten schließlich als Archivbestände von den öffentlichen Bibliotheken übernommen werden.

62 Spätestens dann stünde die Frage im Raum, ob und wie das in verschiedener Hinsicht kostenträchtige Nebeneinander von OA- und Verlagspublikationen beendet, wie mit anderen Worten der Übergang vom Verlags- auf das OA-System regulativ vollzogen werden kann. Hierzu müsste sichergestellt werden, dass jedenfalls die überwiegend öffentlich finanzierten Forschungsergebnisse *nach OA-Prinzipien erstveröffentlicht* werden und diese Fassung in der Folge zu zitieren ist.[132] Das Geschäftsmodell zugangskontrollierter Verlagsdatenbanken würde hiermit zumindest für die fernere Zukunft obsolet.[133] Die Kosten des OA-Systems müssten von den öffentlichen Forschungsförderern finanziert werden, so dass die wissenschaftliche Wertschöpfungskette ohne Umweg über die Verlage aus Steuergeldern gespeist würde.[134]

63 Ob der Zeitpunkt zur rechtlichen Umstellung des wissenschaftlichen Publikationswesens auf Open Access als primären Standard allerdings bereits in zehn Jahren[135] oder wie bei früheren medialen Revolutionen erst nach 200 Jahren[136] gekommen sein wird, ist ungewiss. Abgesehen von politischen Widerständen bedarf es noch erheblicher infrastruktureller und wissenschaftsinstitutioneller Vorleistungen, um einen solchen Paradigmenwechsel überhaupt als wissenschaftsadäquat und damit verfassungsrechtlich zulässig erscheinen zu lassen.[137] Auch insoweit richtet sich das Augenmerk auf die Wissenschaft, deren Perspektive sich im Verhältnis zum Urheberrecht als die allein weiterführende erwiesen hat.

(Endnotes)

1 Siehe z.B. Deutscher Bundestag, Sechster Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft" - Bildung und Forschung, 8.1.2013, BT-Drucks. 17/12029, 39 ff.

2 Siehe Brintzinger, Piraterie oder Allmende der Wissenschaften?, Leviathan 38 (2010), 331, 336 (die Universitätsbibliothek der LMU München biete Zugang zu mehr als 50.000 Zeitschriften an; dies sei etwa das Zehnfache dessen, was die Bibliothek in Zeiten gedruckter Abonnements zur Verfügung stellen konnte); Finch Group Report, Accessibility, sustainability, excellence: how to expand access to research publications, 2012, http://www.researchinfonet.org/wp-content/uploads/2012/06/Finch-Group-report-FINAL-VERSION.pdf, 4.

3 Hilty, Das Urheberrecht und der Wissenschaftler, GRUR Int. 2006, 179, 181; Reichman/Okediji, When Copyright Law and Science Collide: Empowering Digitally Integrated Research Methods on a Global Scale, Minnesota Law Review 96 (2012), 1362, 1418.

4 Zu dieser Tendenz Weingart, Die Stunde der Wahrheit, 2001, 329 f.

5 Für Sprachwerke EuGH Rs. C-5/08, 16.07.2009, Slg. 2009, I-6569 Rn. 35 ff. – Infopaq I; BGH I ZR 9/95, 16.01.1997, ZUM-RD 1997, 329, 331 f. – CB-Infobank I; BGH I ZR 12/08, 1.12.2010, ZUM 2011, 151, 155 – Perlentaucher; für wissenschaftliche Darstellungen BGH I ZR 140/09, 1.6.2011, GRUR 2011, 803 Rn. 39 m.w.N. – Lernspiele.

6 BGH I ZR 106/78, 21.11.1980, GRUR 1981, 352, 353 – Staatsexamensarbeit; BGH I ZR 16/89, 12.7.1990, GRUR 1991, 130, 132 f. – Themenkatalog; BGH I ZR 140/09, 1.6.2011, GRUR 2011, 803 Rn. 49 f. – Lernspiele; OLG Frankfurt a. M. 11 U 66/11, 27.3.2012, ZUM 2012, 574, 577; a. A. Rehbinder, Urheberrecht, 16. Aufl. 2010, Rn. 58, 145; Haberstumpf, Das Urheberrecht – Feind des Wissenschaftlers und des wissenschaftlichen Fortschritts, ZUM 2012, 529, 536. Zur strukturellen Gemeinfreiheit Peukert, Die Gemeinfreiheit, 2012, 19 ff.

7 BGH I ZR 157/77, 7.12.1979, GRUR 1980, 227, 231 – Monumenta Germaniae Historica; BGH I ZR 29/79, 27.2.1981, GRUR 1981, 520, 521 f. – Fragensammlung; BGH I ZR 16/89, 12.7.1990, GRUR 1991, 130, 132 f. – Themenkatalog.

8 OLG Frankfurt a.M. 11 U 66/11, 27.03.2012, ZUM 2012, 574, 579; Loewenheim, in: Schricker/Loewenheim, Urheberrecht, 4. Aufl. 2010, § 2 Rn. 64.

9 Rieble, Autorenfreiheit und Publikationszwang, in: Reuß/Rieble, Autorschaft als Werkherrschaft in digitaler Zeit, 2009, 29, 44.

10 Nicht aber in die ursprüngliche Erzeugung der Daten etc., siehe EuGH Rs. C-203/02, 9.11.2004, Slg. 2004, I-10415 Rn. 28 ff. – British Horseracing.

11 Damit ist nicht der Wert des einzelnen Datensatzes gemeint, sondern die Relevanz des entnommenen Teils im Hinblick auf die geschützten Investitionen; siehe EuGH Rs. C-203/02, 9.11.2004, Slg. 2004, I-10415 Rn. 28 ff. – British Horseracing.

12 EuGH Rs. C-545/07, 5.3.2009, Slg. I-1627 Rn. 73 – Apis/Lakorda.

13 Reichman/Okediji (Fn. 3), Minnesota Law Review 96 (2012), 1362, 1423.

14 Dazu Peukert, Der Schutzbereich des Urheberrechts und das Werk als öffentliches Gut, in: Hilty/Peukert, Interessenausgleich im Urheberrecht, 2004, 11, 24 ff. m.w.N.

15 Goldstein, Copyright's Highway: From Gutenberg to the Celestial Jukebox, 2003.

16 In diesem Sinne die Rechtsprechung zur Begrenzung der Störerhaftung der Anbieter legaler Internetdienste; vgl. zuletzt BGH I ZR 18/11, 12.7.2012, Rn. 28 m.w.N. - Alone in the Dark.

17 § 53a Abs. 1 S. 2 UrhG und obiter LG Frankfurt a.M. 2-06 O 378/10, 16.3.2011, ZUM 2011, 582, 584 f.

18 So in der Tendenz der Vorlagebeschluss BGH I ZR 69/11, 20.9.2012, BeckRS 2012, 04411 Rn. 18 – Elektronische Leseplätze.

19 Vgl. § 137k UrhG und kritisch hierzu Bundesrat, 5.12.2012, BR-Drucks. 737/1/12, 2; zum Anwendungsbereich von § 52 Abs. 1 Nr. 2 UrhG Bundestag, 9.4.2012, BT-Drucks. 15/837, 34.

20 BGH I ZR 84/11, 20.3.2013 - Gesamtvertrag Hochschul-Intranet; Vorinstanz OLG München 6 WG 12/09, 24.3.2011, ZUM-RD 2011, 603, 614 f. (die Angemessenheit könne zu verneinen sein, wenn bei beabsichtigter Verwertung eines Zeitschriftenartikels nur ein digitales Abonnement oder wenn nur die Lizenzierung eines ganzen Lehrbuchs angeboten werde, von dem nur ein kleiner Teil verwertet werden soll).

21 BGH I ZR 69/11, 20.9.2012, Rn. 18 - Elektronische Leseplätze unter Hinweis auf ErwGrd. 45 UrhRL 2001/29.

22 In diesem Sinne Berger, Die öffentliche Zugänglichmachung urheberrechtlicher Werke für Zwecke der akademischen Lehre - Zur Reichweite des § 52a I Nr. 1 UrhG, GRUR 2010, 1058, 1064.

23 Hilty (Fn. 3), GRUR Int. 2006, 179; Sandberger, Behindert das Urheberrecht den Zugang zu wissenschaftlichen Publikationen?, ZUM 2006, 818, 828; Pflüger, Positionen der Kultusministerkonferenz zum Dritten Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft – „Dritter Korb", ZUM 2010, 938, 940 („grenzwertig marginal").

24 Peifer, Wissenschaftsmarkt und Urheberrecht: Schranken, Vertragsrecht, Wettbewerbsrecht, GRUR 2009, 22, 25.

25 Peifer (Fn. 24), GRUR 2009, 22 ff. („Eigentumsfunktion" im Gegensatz zur urheberpersönlichkeitsrechtlichen „Authentizitätsfunktion").

26 Eigentum verkoppelt das Rechtssystem strukturell mit dem Wirtschaftssystem; Luhmann, Das Recht der Gesellschaft, 1993, 446.

27 BVerfG 1 BvR 424/71 u. 1 BvR 325/72, 29.5.1973, BVerfGE 35, 79, 112 ff. – Hochschulurteil; BVerfG 1 BvR 333/75 u.a., 1.3.1978, BVerfGE 47, 327, 367 – Hessisches Universitätsgesetz.

28 BVerfG 1 BvR 434/87, 11.1.1994, NJW 1994, 1781, 1782.

29 BVerfG 2 BvR 1121/06 u.a., 28.9.2007, juris Rn. 26 m.w.N.; Bäuerle, Open Access zu hochschulischen Forschungsergebnissen? Wissenschaftsfreiheit in der Informationsgesellschaft, in: Britz, Forschung in Freiheit und Risiko, 2012, 1, 10.

30 BGH I ZR 16/89, 12.7.1990, GRUR 1991, 130, 132 f. – Themenkatalog.

31 BGH I ZR 140/09, 1.6.2011, GRUR 2011, 803 Rn. 43 m.w.N. – Lernspiele; OLG München 6 U 2093/88, 19.9.1991, GRUR 1992, 510, 510 ff. – Rätsel.

32 Zum wissenschaftlichen Aufsatz als wissenschaftliche Kommunikation kennzeichnendes Format siehe Stichweh, Einheit und Differenz im Wissenschaftssystem der Moderne, in: Halfmann/Rohbeck, Zwei Kulturen der Wissenschaft – revisited, 2007, 213, 218.

33 Hilty (Fn. 3), GRUR Int. 2006, 179.

34 Hilty (Fn. 3), GRUR Int. 2006, 179, 185.

35 Weingart (Fn. 4), 330; Peifer (Fn. 24), GRUR 2009, 22 („Urheberrecht und Wissenschaftsfreiheit befinden sich miteinander in einem tiefen Konflikt."); Reichman/Okediji (Fn. 3), Minnesota Law Review 96 (2012), 1362, 1425.

36 Luhmann, Die Wissenschaft der Gesellschaft, 1990, 9.

37 Merton, Wissenschaft und demokratische Sozialstruktur, in: Weingart, Wissenschaftssoziologie I, Wissenschaftliche Entwicklung als sozialer Prozess, 1973, 45, 49; Taubert/Weingart, ‚Open Access' - Wandel des wissenschaftlichen Publikationssystems, in: Sutter/Mehler, Medienwandel als Wandel von Interaktionsformen, 2010, 159, 164.

38 Merton, in: Weingart (Fn. 37), 45, 47.

39 Vgl. Luhmann (Fn. 36), 446.

40 Suber, Open Access, 2012, 5 ff.; Brintzinger (Fn. 2), Leviathan 38 (2010), 331, 344 f. m.w.N.

41 W. v. Humboldt, Ueber die innere und äussere Organisation der höheren wissenschaftlichen Anstalten in Berlin, in: Flitner/Giel, Wilhelm von Humboldt, Werke, Band IV, 1960, 255, 256; Merton, in: Weingart (Fn. 37), 45, 53 ff.

42 Dazu etwa Taubert/Weingart, in: Sutter/Mehler (Fn. 37), 159, 169.

43 Peifer (Fn. 24), GRUR 2009, 22, 23; siehe ferner unten IV.

44 W. v. Humboldt in: Flitner/Giel (Fn. 41), 255, 256 (Wissenschaft als ein „immer ... noch nicht ganz aufgelöstes Problem"); BVerfG 1 BvR 424/71 u. 1 BvR 325/72, 29.5.1973, BVerfGE 35, 79, 112 ff. - Hochschulurteil; BVerfG 1 BvR 434/87, 11.1.1994, NJW 1994, 1781 f.

45 M. Polanyi, The Republic of Science: Its Political and Economic Theory, Minerva 38 (2000), 1, 7 („The network is the seat of scientific opinion."); Popper, Die offene Gesellschaft und ihre Feinde, Band II, 2003, 254; Schmidt-Assmann, Die Wissenschaftsfreiheit nach Art. 5 Abs. 3 GG als Organisationsgrundrecht, FS Thieme 1993, 697, 698; Stichweh, in: Halfmann/Rohbeck (Fn. 32), 213, 219; Fitzpatrick, Planned Obsolescence, 2011, 66 ff. (prozesshafter Vorgang).

46 Popper (Fn. 45), 254 (öffentlicher Charakter der wissenschaftlichen Methode).

47 M. Polanyi (Fn. 45), Minerva 38 (2000), 1, 6.

48 Zu diesem Unterschied Theisohn, Literarisches Eigentum, 2012, 98, 116.

49 Aus soziologischer Sicht Brintzinger (Fn. 2), Leviathan 38 (2010), 331, 343; Weingart (Fn. 4), 100; aus juristischer Sicht Rehbinder, Zu den Nutzungsrechten an Werken von Hochschulangehörigen, FS Hubmann, 1985, 359, 365; Schmidt-Assmann, Wissenschaft – Öffentlichkeit – Recht, in: Dreier, Rechts und staatstheoretische Schlüsselbegriffe: Legitimität – Repräsentation – Freiheit, 2005, 67, 71; Bäuerle, in: Britz (Fn. 29), 1, 11 m.w.N. Ausnahme ist die unveröffentlichte Habilitationsschrift, die aber von der habilitierenden Fakultät als ausreichender wissenschaftlicher Ausweis geprüft und insoweit der Fachöffentlichkeit zur Kenntnis gebracht wurde.

50 Merton, in: Weingart (Fn. 37), 45, 48 ff.; Stichweh, Genese des globalen Wissenschaftssystems, Soziale Systeme 9 (2003), 3, 4 f.

51 Merton, in: Weingart (Fn. 37), 45, 49; Stichweh (Fn. 50), Soziale Systeme 9 (2003), 3 ff., 11 ff.

52 Stichweh, in: Halfmann/Rohbeck (Fn. 32), 213, 220 m.w.N.

53 Siehe mit Blick auf den Buchdruck Luhmann (Fn. 36), 603; zur Frage, ob die Computerisierung hier einen „entscheidenden Wandel" auslöse offen a.a.O., 607.

54 Reichman/Okediji (Fn. 3), Minnesota Law Review 96 (2012), 1362, 1473.

55 Hier können sich ernsthafte Friktionen zwischen dem urheberrechtlichen Namensnennungsrecht, das nur demjenigen zusteht, der einen Beitrag formuliert bzw. die Darstellungen erzeugt hat, und der wissenschaftlichen Namensnennungspraxis ergeben, wonach auch diejenigen als „Autoren" genannt werden, die „nur" Rohdaten oder Wissen beigesteuert haben.

56 Dazu Trimble, The Future of Cybertravel: Legal Implication of the Evasion of Geolocation, Fordham Intellectual Property, Media & Entertainment Law Journal 22 (2012), 567 ff.

57 Schmidt-Assmann, in: Dreier (Fn. 49), 67, 90; Krujatz, Open Access, 2012, 27.

58 Merton, in: Weingart (Fn. 37), 45, 51 („Die materiellen Ergebnisse der Wissenschaft sind ein Produkt sozialer Zusammenarbeit und werden der Gemeinschaft zugeschrieben."); dazu auch Stichweh, in: Halfmann/Rohbeck (Fn. 32), 213, 216 ff.

59 So für gemeinfreie Wissensgüter Peukert (Fn. 6), 42.

60 Vgl. Katzenberger, Zugang zu wissenschaftlichem Schrifttum für Forschungszwecke, GRUR Int. 1984, 391, 395; Krujatz (Fn. 57), 61 („Institutionalisierung wissenschaftlicher Kommunikation").

61 Hilty (Fn. 3), GRUR Int. 2006, 179, 182 f.

62 Dazu National Research Council, The Digital Dilemma, Intellectual Property in the Information Age, 2000.

63 Siehe m.w.N. etwa Hilty (Fn. 3), GRUR Int. 2006, 179, 183 f.; Woll, Bibliotheken als Dienstleister im Publikationsprozess, 2006, 13 ff.; Brintzinger (Fn. 2), Leviathan 38 (2010), 331, 332 ff. m.w.N.; EU-Kommission, Verbesserung des Zugangs zu wissenschaftlichen Informationen: Steigerung der Wirkung öffentlicher Investitionen in die Forschung, 17.7.2012, KOM(2012) 401 endg., 4; Bundesregierung, Entwurf eines Gesetzes zur Nutzung verwaister und vergriffener Werke und einer weiteren Änderung des Urheberrechtsgesetzes, 5.4.2013, 13 ff. Zu Konzentrationsprozessen in der Verlagsbranche etwa Dallmeier-Tiessen u.a., Open Access Publishing – Models and Attributes, 2010, http://www.iuwis.de/sites/default/files/SOAP_OAP_models_attr_long.pdf (10 % der Verlage veröffentlichen 2/3 der publizierten Beiträge und 14 Großverlage veröffentlichen 30 % der publizierten Beiträge).

64 Hilty, Renaissance der Zwangslizenzen im Urheberrecht? – Gedanken zu Ungereimtheiten auf der urheberrechtlichen Wertschöpfungskette, GRUR 2009, 633, 635. Zur institutionellen Dimension des Umstands, dass Literaturbeschaffer (Bibliotheken) und Leser (Wissenschaftler) auseinanderfallen, siehe Brintzinger (Fn. 2), Leviathan 38 (2010), 331, 334.

65 Dazu Finch Group Report (Fn. 2), 5 f.

66 Pflüger/Ertmann, E-Publishing und Open Access – Konsequenzen für das Urheberrecht im Hochschulbereich, ZUM 2004, 436, 440; EU-Kommission (Fn. 63), KOM(2012) 401 endg., 4.

67 Hilty (Fn. 64), GRUR 2009, 633, 635.

68 Steinhauer, Das Recht auf Sichtbarkeit, 2010, 46; allgemein Peukert, Güterzuordnung als Rechtsprinzip, 2008, 660 ff.

69 BVerfG 1 BvL 77/78, 15.7.1981, BVerfGE 58, 300, 349 f. - Nassauskiesung; BVerfG 1 BvR 868/90, 29.7.1991, NJW 1992, 36 f. m.w.N.

70 Zum Umstand, dass wissenschaftliche Kommunikation viel Zeit braucht, siehe Luhmann (Fn. 36), 365.

71 Lanier, You are not a gadget, 2011; Rieble in: Reuß/Rieble (Fn. 9), 29, 32; Theisohn (Fn. 48), 115 ff.

72 Zu institutionellen Voraussetzungen einer wissenschaftsadäquaten Umstellung der wissenschaftlichen Kommunikation auf Open Access näher Peukert, Ein wissenschaftliches Kommunikationssystem ohne Verlage – zur rechtlichen Implementierung von Open Access als Goldstandard wissenschaftlichen Publizierens, i.E.

73 M. Polanyi (Fn. 45), Minerva 38 (2000), 1, 9 (Nachdruck eines Beitrags von 1962: „Journals are made unreadable by including much trash."); Taubert/Weingart in: Sutter/Mehler (Fn. 37), 159, 166 (für einen Großteil der Peer-review-Publikationen gelte, „dass die Zahl der zitierenden Leser die Zahl der Gutachter häufig erst nach Jahren überschreitet"), 167 f. m.w.N. (peer review „kein besonders wirkungsvolles Instrument für die Selektion von Neuigkeit"); ferner Fröhlich, Die Wissenschaftstheorie fordert Open Access, Information Wissenschaft & Praxis 2009, 253, 255 m.w.N.

74 Verwiesen sei etwa auf die immer kürzer werdenden Aktualisierungstakte bei juristischen Online-Kommentaren. Die Logik des Mediums läuft auf tägliche (stündliche?, automatisierte?) Aktualisierungen hinaus. Zur Notwendigkeit, wissenschaftliche Projekte endgültig abschließen zu können, siehe demgegenüber Luhmann (Fn. 36), 604.

75 Zu dieser Inkonsequenz offen Theisohn (Fn. 48), 118 f.; siehe auch Rieble in: Reuß/Rieble (Fn. 9), 29, 30 (die Absenkung der Zugangsschwellen zur wissenschaftlichen Veröffentlichung und zu veröffentlichten Texten sei „rundweg zu begrüßen").

76 Public Access to Science Act, 108th Congress (2003-2004), http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.2613:; hierfür aus ökonomischer Sicht Shavell, Should Copyright of Academic Works Be Abolished?, Harvard Law School Public Law & Legal Theory Working Paper Series, Paper No. 10-10, http://ssrn.com/abstract=1459028; zur anschließenden Diskussion siehe Müller-Langer/Scheufen, Academic Publishing and Open Access, Max Planck Institute for Intellectual Property and Competition Law Research Paper No. 13-03, http://ssrn.com/abstract=2198400, 6 ff. m.w.N.

77 Hansen, Zugang zu wissenschaftlicher Information - alternative urheberrechtliche Ansätze, GRUR Int. 2005, 378, 382; irritierend ignorant im Verhältnis zu dieser Umwelt seines ökonomischen Modells Shavell (Fn. 76), 53 mit Fn. 88 a.E. („However, Paul Goldstein has suggested to me that elimination of copyright for academic works could lead to conflict with the obligations of the United States under the TRIPS Agreement.").

78 Siehe http://www.wipo.int/copyright/en/limitations/index.html.

79 Siehe Bundesrat, 5.12.2012, BR-Drucks. 737/1/12, 2; ferner Beschlussempfehlung und Bericht des Rechtsausschusses des Deutschen Bundestages, 4.7.2007, BT-Drucks. 16/5939, 26 f.; Deutscher Bundestag, Dritter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft" – Urheberrecht, 23.11.2011, BT-Drucks. 17/7899, 21.

80 Hansen (Fn. 77), GRUR Int. 2005, 378, 383 f. Siehe ferner Pflüger (Fn. 23), ZUM 2010, 938, 944 (zulässig sei die Nutzung eines „veröffentlichten Werkes durch öffentliche Einrichtungen, denen Aufgaben in Bildung, Wissenschaft und Kultur übertragen sind, ... soweit dies im Rahmen ihrer Aufgabenstellung gerechtfertigt und zur Verfolgung nichtkommerzieller Zwecke ... im Rahmen von 1. Unterricht und Forschung, 2. Fort- und Weiterbildung, 3. Dokumentation, Bestandssicherung und Bestandserhaltung" geboten sei).

81 Hilty (Fn. 3), GRUR Int. 2006, 179, 187 ff.; Pflüger (Fn. 23), ZUM 2010, 938, 940.

82 Reichman/Okediji (Fn. 3), 1432 ff., 1440 ff. (auch für wissenschaftliche Nutzungen zu kommerziellem Folgegebrauch).

83 Hirschfelder, Anforderungen an eine rechtliche Verankerung des Open Access Prinzips, 2008, 154 f.

84 Hilty (Fn. 64), GRUR 2009, 633, 641 ff. Mit Hinweis auf medienrechtliche Zugangsrechte auch Peifer (Fn. 24), GRUR 2009, 22, 28.

85 Krujatz (Fn. 57), 279 ff., 280 (Urheber bzw. Verleger als Inhaber eines ausschließlichen Nutzungsrechts an einem wissenschaftlichen Sprachwerk seien zu verpflichten, „jedem anderen Intermediär zu angemessenen Bedingungen ein Recht der Vervielfältigung, öffentlichen Zugänglichmachung und Verbreitung zu Zwecken der weiteren Veröffentlichung in anderer Weise als der Erstveröffentlichung einzuräumen", wenn hierbei der Ort der Erstveröffentlichung deutlich angegeben werde).

86 Siehe Art. 9 Abs. 2 RBÜ, 13 TRIPS, 10 WCT, 16 Abs. 2 WPPT, 5 Abs. 5 UrhRL 2001/29; insoweit zutreffend Peifer (Fn. 24), GRUR 2009, 22, 25; eingehend Peukert, A Bipolar Copyright System for the Digital Network Environment, Hastings Communications & Entertainment Law Journal (Comm/Ent) 28 (2005), 1-80; a.A. etwa Hansen (Fn. 77), GRUR Int. 2005, 378, 384 ff.

87 Peifer (Fn. 24), GRUR 2009, 22, 23.

88 Näher Peukert, Territoriality and Extraterritoriality in Intellectual Property Law, in: Handl/Zekoll/Zumbansen, Beyond Territoriality: Transnational Legal Authority in an Age of Globalization, 2012, 189-228.

89 Gerade umgekehrt Hilty (Fn. 64), GRUR 2009, 633, 638 (Open Access nur territoriale Lösung).

90 Insbesondere Hilty (Fn. 64), GRUR 2009, 633, 635, 636 ff. („Markt wissenschaftlicher Informationsversorgung"); Peifer (Fn. 24), GRUR 2009, 22 ff.; Spindler, Urheberrecht in der Wissensgesellschaft – Überlegungen zum Grünbuch der EU-Kommission, FS Loewenheim, 2009, 287, 299 (sorgfältige Analyse des Marktes); Krujatz (Fn. 57), 5 (ökonomische Ziele), 152 ff.

91 Zum Unterschied zwischen Wirtschaft und Wissenschaft etwa M. Polanyi (Fn. 45), Minerva 38 (2000), 1, 19; Weingart (Fn. 4), 330.

92 Siehe dazu, mit Unterschieden im Detail, Budapest Open Access Initiative, 17.1.2002, http://www.opensocietyfoundations.org/openaccess/translations/german-translation; Bethesda Statement on Open Access Publishing, 20.6.2003, http://www.earlham.edu/~peters/fos/bethesda.htm; Berliner Erklärung über den offenen Zugang zu wissenschaftlichem Wissen, 22.10.2003, http://oa.mpg.de/files/2010/04/Berliner_Erklaerung_dt_Version_07-2006.pdf. Weitere Erklärungen bei Bailey, Open Access Bibliography, 2005, 20 ff.; ferner Deutsche UNESCO-Kommission, Open Access – Chancen und Herausforderungen, 2007; Krujatz (Fn. 57), 33 ff.

93 Zu Ausnahmen nach deutschem Urhebervertrags- und Arbeitsrecht siehe BGH I ZR 244/88, 27.9.1990, NJW 1991, 1480, 1483 – Grabungsmaterialien; KG 5 U 2189/93, 6.9.1994, NJW-RR 1996, 1066 – Poldok; LG Köln 28 O 161/99, 1.9.1999, NJW-RR 2000, 1294, 1295; zu Computerprogrammen Dreier, in: Dreier/Schulze, Urheberrechtsgesetz, Kommentar, 4. Aufl. 2013, § 69b Rn. 7.

94 Herb, Open Access - Ein Wundermittel?, in: Lison, Information und Ethik, 2007, 78 ff.

95 Suber (Fn. 40), 125 ff.; Budapest Open Access Initiative 2002 (Fn. 92).

96 Dazu Peukert (Fn. 6), 205 ff.

97 Siehe §§ 31a Abs. 1 S. 2, 32 Abs. 3 S. 3, 32a Abs.3 S. 3, 32c Abs. 3 S. 2 UrhG sowie BT-Drucks. 14/6433, 15; BT-Drucks. 14/8058, 19; BT-Drucks. 16/1828, 37; BT-Drucks. 16/5939, 44.

98 BGH I ZR 94/05, 6.12.2007, NJW 2008, 751 Rn. 27 – Drucker und Plotter I; BGH I ZR 69/08, 29.4.2010, NJW 2010, 2731 Rn. 28 ff., 33 ff. – Vorschaubilder I; BGH I ZR 140/10, 19.10.2011, NJW 2012, 1886 Rn. 16 ff. – Vorschaubilder II; Peukert, Der digitale Urheber, in: Bullinger u.a., FS Wandtke, 2013, 455 ff. m.w.N. zur überwiegend ablehnenden Literatur.

99 Zur Reichweite der legalisierten Nutzungen siehe Peukert (Fn. 72).

100 Vgl. § 32 Abs. 3 S. 2 UrhG.

101 Sog. grüner OA.

102 Bethesda Statement on Open Access Publishing (Fn. 92) („Community standards, rather than copyright law, will continue to provide the mechanism for enforcement of proper attribution and responsible use of the published work, as they do now."). Zum urheberrechtlichen Zweitverwertungsrecht sogleich bei Fn. 118.

103 Vgl. für Deutschland RegE verwaiste Werke (Fn. 63), 14; für das vereinigte Königreich Finch Group Report (Fn. 2), 2012, 5 f.; für die USA Executive Office of the President, Office of Science and Technology Policy, Expanding Public Access to the Results of Federally Funded Research, 22.2.2013, http://www.whitehouse.gov/blog/2013/02/22/expanding-public-access-results-federally-funded-research; zu Effizienzgesichtspunkten EU-Kommission (Fn. 63), KOM(2012) 401 endg., 3; Suber (Fn. 40), 29 ff., 43 ff., 133 ff.; Fröhlich (Fn. 73), Information Wissenschaft & Praxis 2009, 253-258; kritisch Theisohn (Fn. 48), 115 ff. („gescannte Ideologie").

104 Fröhlich (Fn. 73), Information Wissenschaft & Praxis 2009, 253, 255. Zur höheren Zitierrate von OA-Publikationen im Vergleich zu Verlagspublikationen siehe m.w.N. Mueller-Langer/Scheufen (Fn. 76), 9 f.

105 Fröhlich (Fn. 73), Information Wissenschaft & Praxis 2009, 253, 256; kritisch Theisohn (Fn. 48), 119 (Entschleunigungsbedürfnis der Wissenschaft).

106 Budapest Open Access Initiative 2002 (Fn. 92); skeptisch Herb, in: Lison (Fn. 94), 78; zynische Ressentiments bei Rieble, in: Reuß/Rieble (Fn. 9), 29, 51 („Ob in Ouagadougou oder anderswo deutsche Netzveröffentlichungen zur Soteriologie... verstanden werden, bleibt fraglich."; Hervorh. im Original). Zur Überwindung von Sprachgrenzen durch Open Access siehe Fröhlich (Fn. 73), Information Wissenschaft & Praxis 2009, 253, 257 f.

107 Taubert/Weingart, in: Sutter/Mehler (Fn. 37), 159, 166.

108 Schmidt-Assmann, in: Dreier (Fn. 49), 67, 86; Royal Society, Science as an open enterprise, 2012, http://royalsociety.org/uploadedFiles/Royal_Society_Content/policy/projects/sape/2012-06-20-SAOE.pdf, 7 f.

109 Weingart (Fn. 4), 333 m.w.N.

110 Siehe Houghton u.a., General Cost Analysis for Scholarly Communication in Germany, 2012, urn:nbn:de:hebis:30:3-275309; auf der Basis dieser Annahme auch EU-Kommission (Fn. 63), KOM(2012) 401 endg., 2; RegE verwaiste Werke (Fn. 63), 14. Zu den Nettokosten eines OA-Modells siehe auch Finch Group Report (Fn. 2), 6; Brintzinger (Fn. 2), Leviathan 38 (2010), 331, 338 f. m.w.N.

111 Weishaupt, Der freie Zugang zum Wissen: auf dem Weg, aber noch nicht am Ziel! Erste Ergebnisse einer Studie zur Akzeptanz von Open-Access-Zeitschriften, Forschung Aktuell Nr. 08/2008, urn:nbn:de:0176-200808014 m.w.N.; Dallmeier-Tiessen u.a., Highlights from the SOAP project survey. What Scientists Think about Open Access Publishing, 2011, arXiv:1101.5260 (knapp 18.000 Befragte).

112 Siehe Fry u.a., Peer Behavioural Research: Authors and Users vis-à-vis Journals and Repositories, Final Report, August 2011, http://hal.inria.fr/docs/00/73/61/68/PDF/PEER_D4_final_report_29SEPT11.pdf, 9, 43; Dallmeier-Tiessen u.a. (Fn. 63) (jährlich 200-300 neue OA-Journals); Laakso u.a., The Development of Open Access Journal Publishing from 1993 to 2009, PLoS ONE 6(6) (2011), doi:10.1371/journal.pone.0020961, 7 (auch relatives Größenwachstum von OA im Verhältnis zum gesamten Publikationsaufkommen).

113 Fry u.a. (Fn. 112), 30.

114 EU-Kommission (Fn. 63), KOM(2012) 401 endg., 5 (20 %); Enquete-Kommission „Internet und digitale Gesellschaft" – Bildung und Forschung (Fn. 1), BT-Drucks. 17/12029, 39 (5-30 %); Fry u.a. (Fn. 112), 74 (geringe Steigerungsraten); anders Laakso u.a. (Fn. 112), PLoS ONE 6(6) (2011), doi:10.1371/journal.pone.0020961, 7 (relatives Größenwachstum von OA im Verhältnis zum gesamten Publikationsaufkommen).

115 Siehe Weishaupt (Fn. 111); skeptisch insbesondere Hilty (Fn. 64), GRUR 2009, 633, 638; Krujatz (Fn. 57), 62.

116 Zum grünen OA als „self-archiving" von Zeitschriftenbeiträgen Budapest Open Access Initiative 2002 (Fn. 92). Offener die Definition von grünem OA in: Zehn Jahre nach der Open-Access-Initiative von Budapest: Den Standard auf „Offen" setzen, 12.9.2012, http://www.opensocietyfoundations.org/openaccess/boai-10-translations/german-translation (OA über Repositorien). Zum goldenen OA in hybriden Verlagszeitschriften siehe EU-Kommission (Fn. 63), KOM(2012) 401 endg., 5; Dallmeier-Tiessen u.a. (Fn. 63). Zu den Autorengebühren solcher Verlagsangebote siehe Brintzinger (Fn. 2), Leviathan 38 (2010), 331, 338; Dallmeier-Tiessen u.a. (Fn. 111), 9. Offene Definition des goldenen OA in: Enquete-Kommission „Internet und digitale Gesellschaft" – Bildung und Forschung (Fn. 1), BT-Drucks. 17/12029, 40.

117 Zur diesbezüglichen Vertragspraxis siehe http://www.sherpa.ac.uk/romeo/index.php?la=en&fIDnum=|&mode=simple.

118 RegE verwaiste Werke (Fn. 63), 5 f. Ähnliche Vorschläge sehen eine Frist von sechs Monaten bei Periodika und von zwölf Monaten bei Sammelwerken und zusätzlich die (Zweit-)Veröffentlichung in der Formatierung der Erstpublikation vor; siehe Gesetzentwurf der Fraktion der SPD, Entwurf eines ... Gesetzes zur Änderung des Urheberrechtsgesetzes, 16.3.2011, BT-Drucks. 17/5053; zuerst in diesem Sinne Hansen (Fn. 77), GRUR Int. 2005, 378, 382; ferner Pflüger (Fn. 23), ZUM 2010, 938, 941.

119 RegE verwaiste Werke (Fn. 63), 14 f.; vgl. Hansen (Fn. 77), GRUR Int. 2005, 378, 382.

120 Die von jenen abgeschlossenen Verlagsverträge unterliegen gem. Art. 4 Abs. 2, 19 Abs. 1 der Verordnung Nr. 593/2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I), Abl. Nr. L 177 04.07.2008, 6, deutschem (Urheber-)Vertragsrecht als dem Recht des Ortes ihres gewöhnlichen Aufenthalts und damit auch dem künftigen Zweitverwertungsrecht.

121 RegE verwaiste Werke (Fn. 63), 14 f.; Heckmann/Weber, Open Access in der Informationsgesellschaft, GRUR Int. 2006, 995, 997 ff.; Peifer (Fn. 24), GRUR 2009, 22, 27; a.A. noch Bundesregierung, BT-Drucks. 16/1828, 47; Hirschfelder, Open Access – Zweitveröffentlichungsrecht und Anbietungspflicht als europarechtlich unzulässige Schrankenregelungen?, MMR 2009, 444, 447 (Umgehung der Richtlinie).

122 Finch Group Report (Fn. 2), 6.

123 Zu diesem Netzwerkeffekt Spindler, FS Loewenheim (Fn. 90), 287, 300; Shavell (Fn. 76), 48; Mueller-Langer/Scheufen (Fn. 76), 11 m.w.N.

124 Fry u.a. (Fn. 112), iv („Academic researchers have a conservative set of attitudes, perceptions and behaviours towards the scholarly communication system and do not desire fundamental changes in the way research is currently disseminated and published.“).

125 Bäuerle, in: Britz (Fn. 29), 1, 7; oder in den Worten von Rieble, in: Reuß/Rieble (Fn. 9), 29, 41: „Das hat ästhetische Gründe, wurzelt auch in der Eitelkeit und dient der Karriere.“.

126 Herb, in: Lison (Fn. 94), 78.

127 Taubert/Weingart, in: Sutter/Mehler (Fn. 37), 159, 177; Spindler, FS Loewenheim (Fn. 90), 287, 301 f.; Bäuerle, in: Britz (Fn. 29), 1, 7.

128 Siehe Berliner Erklärung über den offenen Zugang zu wissenschaftlichem Wissen (Fn. 92); Enquete-Kommission „Internet und digitale Gesellschaft“ – Urheberrecht (Fn. 79), BT-Drucks. 17/7899, 81; für eine empirische Bestätigung siehe Weishaupt (Fn. 111). Weitergehend aber Enquete-Kommission „Internet und digitale Gesellschaft“ – Bildung und Forschung (Fn. 1), BT-Drucks. 17/12029, 95 (Verpflichtung auf nachgeschalteten, grünen OA).

129 Schweizerischer Nationalfonds zur Förderung der Wissenschaftlichen Forschung, Nationaler Forschungsrat, Weisung betreffend Open Access zu Forschungspublikationen aus vom SNF geförderten Forschungsprojekten, 04.07.2007, http://www.unibas.ch/doc/doc_download.cfm?uuid=2EF93B5E3005C8DEA3D13694B33B10AD&&IRACER_AUTOLINK&& (OA-Befugnisse „soweit möglich“ vorbehalten); EU-Kommission (Fn. 63), KOM(2012) 401 endg., 8.

130 Royal Society (Fn. 108), 7; tendenziell auch EU-Kommission (Fn. 63), KOM(2012) 401 endg., 6 f. (Hindernisse für einen raschen Wandel).

131 Siehe für das Vereinigte Königreich Finch Group Report (Fn. 2). Reaktion der Regierung: Letter to Dame Janet Finch on the Government Response to the Finch Group Report, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/32493/12-975-letter-government-response-to-finch-report-research-publications.pdf. Reaktion der öffentlichen Forschungsförderer: Higher Education Funding Council for England, HEFCE statement on implementing open access, 16.7.2012, http://www.hefce.ac.uk/news/newsarchive/2012/statementonimplementingopenaccess/; Research Councils UK Policy on Access to Research Outputs, 17.7.2012, http://roarmap.eprints.org/671/1/RCUK%20_Policy_on_Access_to_Research_Outputs.pdf. Für die USA Executive Office of the President (Fn. 103). Ferner EU-Kommission (Fn. 63), KOM(2012) 401 endg., 9.

132 Siehe mit Vorbehalten 10 Jahre BOAI, (Fn. 116); deutlicher Kuhlen, Erfolgreiches Scheitern – eine Götterdämmerung des Urheberrechts?, 2008, 551; wohl auch Reichman/Okediji (Fn. 3), Minnesota Law Review 96 (2012), 1362, 1467; Steinhauer (Fn. 68), 44; Enquete-Kommission „Internet und digitale Gesellschaft“ – Urheberrecht (Fn. 79), BT-Drucks. 17/7899, 37; Bäuerle, in: Britz (Fn. 29), 1, 9.

133 Siehe Peifer (Fn. 24), GRUR 2009, 22, 23 („Die entscheidende Frage, vor der man in der Onlinewelt steht, ist die, ob der klassische Verleger als Informationsbroker noch gebraucht wird.“).

134 Bethesda Statement on Open Access Publishing (Fn. 92); Research Councils UK (Fn. 131).

135 So 10 Jahre BOAI 2012 (Fn. 116).

136 Vgl. Luhmann (Fn. 36), 600 (es habe jeweils etwa 200 oder mehr Jahre gedauert, bis die Gesellschaft sich auf das Alphabet bzw. den Buchdruck eingestellt habe – eine „ungeheuer“ schnelle Veränderung); Finch Group Report (Fn. 2), 10 („likely to be a lengthy transition“); Suber (Fn. 40), 167.

137 Hingewiesen sei nur auf die Erfordernisse, den Journal Impact Factor durch autor- oder artikelbezogene Bewertungskriterien zu ersetzen; Zitierregeln auf OA-Publikationen umzustellen; weitere OA-Zeitschriften und fachspezifische Repositorien, etwa für die deutschsprachige Rechtswissenschaft, zu etablieren; im OA-System ausreichenden Peer Review zu gewährleisten; die wissenschaftlichen Gepflogenheiten dahingehend zu ändern, dass die öffentliche Zugänglichmachung eines Beitrags auf einem Repositorium dem endgültigen „Gut zum Druck“ entspricht; und wohl nicht zuletzt vom Gedanken Abschied zu nehmen, dass wissenschaftliche Aufsätze in einer „Zeitschrift“ – und nicht etwa in einer institutionellen Reihe einer Fakultät – publiziert werden müssen. Zu alldem näher Peukert (Fn. 72).

JIPITEC

Journal of
Intellectual Property,
Information Technology,
and Electronic Commerce
Law