

jipitec

2 | 2014

Volume 5 (2014)

Issue 2

ISSN 2190-3387

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

Articles

Oblivion, Erasure and Forgetting in the Digital Age
by Aurelia Tamò and Damian George

The Implementation of the Media Services Directive by National
Regulatory Authorities: National Responses to Regulatory Challenges
by Jenny Metzdorf

A Qualitative Study on the Adoption of Copyright Assignment Agreements
(CAA) and Copyright License Agreements (CLA) within Selected FOSS Projects
by Sylvia F. Jakob

Proportionality of Website Blocking: Internet
Connectivity Providers as Copyright Enforcers
by Pekka Savola

Social Networking Sites' Terms of Use Addressing Imbalances in the
User-Provider Relationship through Ex Ante and Ex Post Mechanisms
by Ellen Wauters, Eva Lievens & Peggy Valcke

Book Review

Sebastian Haunss, Conflicts in the Knowledge Society
The Contentious Politics of Intellectual Property
by Axel Metzger

Editors:
Thomas Dreier
Axel Metzger
Gerald Spindler
Lucie Guibault
Miquel Peguera

www.jipitec.eu

jipitec

Journal of Intellectual Property,
Information Technology and
Electronic Commerce
Law

Volume 5 Issue 2, September 2014
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.

Editors:

Thomas Dreier
Axel Metzger
Gerald Spindler
Lucie Guibault
Miquel Peguera

Board of Correspondents:

Graeme Dinwoodie
Christophe Geiger
Ejan Mackaay
Giovanni M. Riccio
Cyrill P. Rigamonti
Olav Torvund
Mikko Välimäki
Rolf H. Weber
Andreas Wiebe
Raquel Xalabarder

Editor-in-charge for this issue:

Axel Metzger, Hannover

Administrative Editor:

Philipp Zimbehl

Layout:

Philipp Zimbehl

ISSN 2190-3387

Funded by

DFG Deutsche
Forschungsgemeinschaft

Table Of Contents

| | Articles |
|---|----------|
| Oblivion, Erasure and Forgetting in the Digital Age by Aurelia Tamõ and Damian George | 71 |
| The Implementation of the Media Services Directive by National Regulatory Authorities: National Responses to Regulatory Challenges by Jenny Metzdorf | 88 |
| A Qualitative Study on the Adoption of Copyright Assignment Agreements (CAA) and Copyright License Agreements (CLA) within Selected FOSS Projects by Sylvia F. Jakob | 105 |
| Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers by Pekka Savola | 116 |
| Social Networking Sites' Terms of Use: Addressing Imbalances in the User-Provider Relationship through Ex Ante and Ex Post Mechanisms by Ellen Wauters, Eva Lievens & Peggy Valcke | 139 |
| Sebastian Haunss, Conflicts in the Knowledge Society The Contentious Politics of Intellectual Property by Axel Metzger | 152 |

Book Review

Oblivion, Erasure and Forgetting in the Digital Age

by Aurelia Tamò and Damian George

Aurelia Tamò is a PhD Candidate, Chair of Information and Communication Law, University of Zurich
Damian George is a junior associate at Nobel & Hug attorneys at law in Zurich

Abstract: In light of the recent European Court of Justice ruling (ECJ C-131/12, *Google Spain v. Spanish Data Protection Agency*), the “right to be forgotten” has once again gained worldwide media attention. Already in 2012, when the European Commission proposed a right to be forgotten, this proposal received broad public interest and was debated intensively. Under certain conditions, individuals should thereby be able to delete personal data concerning them. More recently – in light of the European Parliament’s approval of the LIBE Committee’s amendments on March 14, 2014 – the concept seems to be close to its final form. Although it remains, for the most part, unchanged from the previously circulated drafts, it has been re-labelled as a “right of erasure”. This article argues that, despite its catchy terminology, the right to be forgotten can

be understood as a generic term, bringing together existing legal provisions: the substantial right of oblivion and the rather procedural right to erasure derived from data protection. Hereinafter, the article presents an analysis of selected national legal frameworks and corresponding case law, accounting for data protection, privacy, and general tort law as well as defamation law. This comparative analysis grasps the practical challenges which the attempt to strengthen individual control and informational self-determination faces. Consequently, it is argued that narrowing the focus on the data protection law amendments neglects the elaborate balancing of conflicting interests in European legal tradition. It is shown that the attempt to implement oblivion, erasure and forgetting in the digital age is a complex undertaking.

Keywords: Right to be forgotten, oblivion, erasure, privacy, data protection, defamation, autocomplete suggestions, notice and take down, EU data protection directive, data protection reform, data protection regulation, ECJ C-131/12 *Google v. Spain*

© 2014 Aurelia Tamò/Damian George

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Aurelia Tamò and Damian George, *Oblivion, Erasure and Forgetting in the Digital Age*, 5 (2014) JIPITEC 71, para. 1.

A. Introduction

1 Every individual has experienced episodes in his life he enjoys remembering (and having others remember), and others that he would like to forget (or have others forget). As individuals increasingly make frequent public use of the Internet, users have become aware of the potential harm persistent information can cause when stored on the eternal

memory of the Internet. Considering that digital abstinence is not an option, users are expressing an increased fear of being haunted by their digital past.¹

2 The European Commission (EC) claims to have recognized the problem and recently proposed a “right to be forgotten and erasure” as part of the revision of the 1995 European Data Protection Directive² (Directive 95/46/EC) principles. In light of the increased online activities and opaque privacy

policies of web services, the EC wants to strengthen the control and digital rights of individuals. Therefore, users should be given the right to have their data fully removed.³

- 3 Legal scholars in Europe and the US have debated the implications of an online right to be forgotten. The first comprehensive approach in this regard was taken by Mayer-Schönberger in his *oeuvre* “Delete”.⁴ The concept of deletion has since been central to the academic debate, which focuses on the legal, philosophical and sociological foundations as well as potential implications of a policy response.
- 4 In this article we approach the topic at hand from a European legal tradition perspective, leaving aside the US-American concepts in this respect. Nevertheless it should be mentioned briefly that the US has been rather critical of the concept of the right to be forgotten.⁵ In particular the implementation of the so-called “Eraser Law” (SB 568, California Business & Professions Code Sec. 22581) in California was controversially discussed in the media.⁶
- 5 The focus of this article lies on interactions among private parties, omitting conflicts arising out of government activities. We will elaborate throughout this article that one should not restrict the debate to the legal provisions but must simultaneously draw insights from the elaborated case law. We will support this approach by showing that European Member States have dealt with questions relating to oblivion and erasure in the age of online activities and interactions by continually balancing the conflicting interests according to long-established norms and concepts.

B. Oblivion, Erasure and Forgetting – Understanding the Concepts Behind the Terminologies

I. Privacy Protection in Europe

- 6 Before discussing new approaches for protecting the individual’s privacy with data protection tools, we shall briefly put data and privacy protection into context.
- 7 The term “data protection” might be misleading since the protected good is not the data itself but the data subject’s fundamental privacy rights.⁷ While the protection of privacy, and the individual’s right to personality in particular, have long been discussed and contested in national legislations in Europe, data protection laws have been evolving only since the second half of the twentieth century.⁸ Unlike mechanisms that protect personality, which are

mostly used retroactively (*ex post*), data protection tries predominantly to guarantee the protection in advance (*ex ante*) by considering the processing of data as privacy infringing “by default” and therefore making processors adhere to data quality principles. In other words, data protection law

*has introduced the default rule that the handling of personal data is per se an intrusion unless guiding principles were followed like the purpose limitation principle, the fairness principle and other safeguards like a right of access to one’s own data.*⁹

- 8 In the European Union, the processing of personal data must not only fulfil the guiding principles of data quality as provided for in Art. 6 Directive 95/46/EC but must also be legitimate. The criteria for making data processing legitimate are listed in Art. 7 Directive 95/46/EC. One important criteria is consent. However, despite consent being regarded as a promising tool, the reliance upon consent as a basis of justification for the processing of data through private parties has not been successful in providing the intended self-control of the users.¹⁰ The EU’s data protection reform efforts strive – amongst other things – to increase the individual’s control by clarifying, and possibly strengthening, its rights.¹¹ One of these reinforced rights is currently known under its original terminology, the “right to be forgotten”. Thereby, the EU attempts to strengthen the individual’s self-determination¹² with regard to the processing of his personal data.

II. The Right of Oblivion vs. the Right to Erasure

- 9 In both the literature and political discussions, there is a lack of uniformity when it comes to defining the overall concept of “deletion” of personal data. While some use the terms “the right of oblivion”, “the right to forget”, “the right to be forgotten” or the “right to erasure” as synonyms, or at least sometimes interchangeably,¹³ others differentiate among the underlying concepts based on their legal rationale and scope.¹⁴
- 10 In particular, a distinction between the right of oblivion and the right of erasure can add value to the maze of terminologies:
- 11 First of all, the right of oblivion – or *le droit a l’oubli* resp. *il diritto al’oblio* according to its French and Italian root¹⁵ – has historically been applied in severe cases of (potential) defamation and breach of privacy of (mostly) ex-convicts.¹⁶ The right offers deletion of some public data that are no longer newsworthy, which highlights the importance of the time component, i.e. the period elapsed between the creation of the public data and the request for oblivion.¹⁷ The rationale behind the concept of

oblivion is found in the fundamental respect for privacy.¹⁸ It aims to prevent potential harm to “dignity, personality, reputation, and identity” of an individual.¹⁹

- 12 Secondly, the right of erasure provides the data subject with a right to demand the removal of personal data that is being processed by third parties.²⁰ This right is rooted in the idea that the data subjects should be able to infer in the data processing (e.g. when the processing is illegitimate) and that the data subject’s consent to the processing of his personal data should be revocable.²¹ Put in a broader context, the goal is to re-balance power between data subjects and data processors. The data subject herewith becomes a right holder over its personal data.
- 13 Thus, the aim of each right is different: While the right of oblivion, as a right derived from the fundamental respect for privacy and personality, is based on a lengthy tradition of balancing contradicting interests, the right of erasure can be seen as a way of enforcing a substantial claim, i.e. the claim that a certain way of processing personal data is a violation of data protection principles.
- 14 So while the scope of the right to oblivion is limited to outdated data, the right to erasure potentially applies to any data whose processing violates data protection laws. As it is shown in below, these two concepts can overlap.

III. The Right to Be Forgotten

1. Scope and Boundaries

- 15 Since the announcement of an EU-wide right to be forgotten by the EC, discussions have circled around the rationale and scope of such a right. In 2012, the EC stated that all data must be deleted whenever the data subjects no longer want “their data to be processed and there are no legitimate grounds for retaining it”.²² In a speech given in early 2013, Vice-President of the EC Reding clarified that “the right to be forgotten cannot be absolute just as the right to privacy is not absolute. There are other fundamental rights with which the right to be forgotten needs to be balanced – such as freedom of expression and freedom of the press.”²³
- 16 As the legislative background of the right to be forgotten (even if now re-labelled as a “traditional” right of erasure, cf. B.III.2) implies, its creation resulted from the increased concern regarding how especially the younger generation makes use of social networking platforms. These concerns have not only been raised in Europe but have also found

advocates in California, where a so-called “Erasure Bill” is been debated for teens and children using social networking sites.²⁴

- 17 Defining the scope and boundaries of the right to be forgotten has proven to be a difficult task not only at a political level but also among legal scholars. According to Koops, Reding’s speech indicates that the right to be forgotten is already part of the current data protection law in Europe, but it still needs to be reinforced. This argument is based on the Vice-President’s statement that the right to be forgotten shall “strengthen” the rights of individuals. Therefore, the right to be forgotten is seen as a mere support of the right to erasure, which is already established in the current Directive 95/46/EC.²⁵ However, according to Koops, two main dimensions, encompassing perspectives on the right to be forgotten in the literature, must be distinguished: these comprise, first, Mayer-Schönberger’s pioneering vision of expiration dates for personal data, or a right to have data deleted in due time and, second, the dimension of oblivion, granting individuals a “fresh start” when news seem no longer newsworthy, and enabling the individuals self-development and freedom to speak, write and act.²⁶
- 18 Another approach to distinguish the right to be forgotten has been taken by Weber, who outlines the difference between the active – right to forget – and passive – right to be forgotten – verb tense. Weber states that the difference lies in the time component: while the right to forget requires a past event that has occurred a long time ago, the right to be forgotten allows any data subject to claim the deletion of their data regardless of the length of time elapsed.²⁷
- 19 Less focused on the wording and grammatical distinction itself, Rouvory differentiates between the perspectives of the parties involved in the act of forgetting. While the right to be forgotten is directed at third parties and their duty to forget, the right to forget is needed for the individual itself, to be able to forget his own past.²⁸
- 20 Conceptually, we agree with Ausloos’s and Ambrose’s claim that the right of oblivion and the right to erasure are “two interpretations of the right to be forgotten”.²⁹ The authors maintain that the right to be forgotten can be interpreted as a combination of both concepts.³⁰
- 21 By reinforcing the idea that “individuals should have control of their personal data”, Art. 17 of the proposed General Data Protection Regulation³¹

(Regulation) can be seen as a step towards a more user-control-based approach in data protection and an attempt to reinforce the principle of informational self-determination in the digital age. Art. 17 (1) of the Regulation states that the “data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child” when the grounds listed in *littera* (a) to (d) apply. However, the subordinate clause “especially in relation to personal data which are made available by the data subject while he or she was a child” was deleted by the Rapporteur, Albrecht, in his Draft Report, 2012/0011(COD), 17.12.2012 as he feared that such a sub-clause would imply limitations on the applicability of the right to be forgotten with respect to adults.

- 22 On the basis of a compromised text by the Irish Presidency, on May 31 and June 21, 2013, the Council of the European Union published an amended version of its initial proposal.³² The long-awaited vote of the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) was held on October 21, 2013. These compromised amendments of the Draft Regulation were almost unanimously approved by the Parliament on March 14, 2014. The Council of the EU will negotiate the final text with the Parliament and the EC (trilog) and await the final approval by the Parliament once a text is agreed upon.
- 23 The Regulation subsumes under the term right to be forgotten the data subject’s right – on a number of grounds – to delete personal data. One of those grounds is the “withdrawal of consent by which the data controller holds the data”.³³ This right is currently enacted in Art. 17 (1b) of the Regulation. Even though already today Art. 14 Directive 95/46/EC obliges Member States to provide the data subject with a right to object to the procession of data, this does not embrace scenarios in which consent is withdrawn in retrospect.³⁴ Since the Directive 95/46/EC mainly sets the minimal standard for data protection in the EU, the national legislations of Member States can differ in this respect. In other words, the withdrawal of consent as a ground for erasure can be established by national data protection acts.
- 24 If erasure on the grounds of Art. 17 (1) of the Regulation is demanded, the data controller has to carry out the erasure without delay.³⁵ An exception is granted (*inter alia*) to the data controller in cases where retention is necessary for exercising the right of freedom of expression, reasons of public interests or for compliance with a legal obligation to retain the personal data by EU provisions or national law of a Member State to which the controller is subject.³⁶
- Furthermore, Art. 17 (1) (b) explicitly states, that “other legal grounds for the processing” can restrict the data subject’s right to erasure. Of special interest is also Art. 17 (1) (c), which, in combination with Art. 19, strengthens the individual’s rights by allowing the data subject to object at any time to the processing of personal data, unless the controller is able to demonstrate a compelling legitimate ground for such processing.³⁷
- 25 The pressing question with respect to the right to be forgotten is to what extent the intensive lobbying has altered the original scope and outreach of Art. 17 of the Regulation. One striking alteration is that the term “right to be forgotten” has been erased and replaced by the previously already used terminology “right of erasure”.³⁸ Yet, except for the change of terminology, Art. 17 remains mostly true to its draft versions of 2013. Especially the core provisions that strengthen the position of users remained unchanged. The same holds true for Art. 17 (1b), which allows individuals to withdraw consent to the data processing at any time. However, Art. 17 (2), concerning the data controller’s responsibility to take reasonable steps to inform third parties to follow the demand of erasure when data has been made public without proper justification has been slightly defused.³⁹ The major amendment concerns the deletion of the last sentence of the original paragraph, which stated that data controllers are responsible for publications by third parties when they authorized the third party to do so. Furthermore, the altered provision does not request data controllers to take *all* reasonable steps to inform the third party about the erasure request but only reasonable steps. How those amendments will affect the data controllers’ responsibilities, especially in light of the mostly unchanged Recital 54, is unclear.

C. Implementing Erasure and Oblivion – A Comparative Analysis

I. European Union

1. Relevant Legal Provisions

- 26 At the European level, privacy is an essential human right and is protected in Art. 8 (1) of the European Convention of Human Rights (ECHR)⁴⁰ and the more recent Art. 7 of the Charter of Fundamental Rights of the European Union (CFREU). Both articles provide a right to respect of one’s private life, home and communication. Art. 8 ECHR regulates the relationship between individuals and public authorities and does not establish a direct obligation for private parties.⁴¹ The recent ECJ ruling (cf. C.I.2.) gave some clarity with regards to the impact of

those rights on oblivion, erasure and forgetting in the digital age.

- 27 Those fundamental rights safeguarding privacy must be weighed against the fundamental rights to freedom of expression and information,⁴² as they are provided for inter alia in Art. 10 and Art. 11 ECHR.
- 28 Next to the protection of personal life in Art. 7 CFREU, the CFREU also explicitly protects personal data in Art. 8 (1). Already Art. 16 (1) Treaty on the Functioning of the European Union (TFEU) states that everybody has a right to protection of his personal data. With regard to the processing of personal data, the principles and conditions under which erasure can be demanded are defined in the Directive 95/46/EC. Especially relevant in this regard are Art. 12 (b) and Art. 14. The former article states that every data subject has the right to obtain from the controller – if appropriate – the erasure of processed data, which does not comply with the provisions established in the Directive, in particular if the data is incomplete or inaccurate.
- 29 A data subject’s right to erasure will depend on (1) whether the processing of the personal data was legitimate, i.e. in accordance with the requirements set forth in Art. 7 and 8; (2) whether the principles with respect to data quality of Art. 6 were adhered to; and (3) the availability of other corrective measures that would make the processing legitimate.⁴³ If these requirements are fulfilled, the data subject can have its personal data erased. Erasure in this sense equals every measure that results in making the personal data unavailable to the data controller.⁴⁴ Information can be erased by physically destroying the medium that carries the personal data, by overwriting the “to-be-erased” data with other information, or by removing the link between the information and the person and therewith altering the character of the data from personal to non-personal.⁴⁵
- 30 Further, the provisions of Directive 2002/58/EC⁴⁶ and Directive 2000/31/EC⁴⁷ apply as *lex specialis* with respect to the electronic processing of data. Art. 6 of the Directive 2002/58/EC states that “data (...) must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication”.⁴⁸ The Directive 2000/31/EC seeks to implement a differentiated system of intermediate service provider’s liability for illicit content in its Arts. 12-15. While not accounting for erasure or oblivion rights, as will be shown, the latter provisions do play an important role with regard to online privacy protection.
- 2. ECJ C-131/12, Google Spain v. Spanish Data Protection Agency**
- 31 On May 13, 2014, the ECJ brought some clarity regarding the practical impact of some of the aforementioned provisions. The Spanish Data Protection Authority (DPA) had ordered Google to de-index parts of a newspaper’s archive concerning a data subject’s attachment proceedings back in the 1990s. During appeal proceedings, the High Court of Spain (“Audiencia Nacional”) demanded that the ECJ determine whether Google can be deemed a data controller regarding the contested archives, whether Art. 12 (b) and 14 Directive 95/46/EC oblige Google to de-index third-party-generated web pages and if these provisions provide for a “right to be forgotten”.⁴⁹
- 32 As to whether search engines are to remove certain results that were provided when typing the data subject’s name according to Art. 12 and 14 Directive 95/46/EC the question was affirmed. Interestingly, the court emphasized that whenever a search is performed by typing a person’s name, the engine establishes “a more or less detailed profile” of such a person, and the interference of this occurrence is catalysed by the role search engines play in today’s society. In Recital 81 and 97, the ECJ then established the general rule that, due to the potential seriousness of such an offence, the data subject’s right to privacy as provided for in Art. 7 and 8 CFREU overrides the interest of Internet users in having access to information as well as the economic interest of the search engine. The impact of this *obiter dictum* will have to be subject to further research.
- 33 With regards to the merits of the case, the court acknowledged the duty of Google to erase such links when demanded to do so by a DPA. It argued that even if the content on the corresponding web page, to which the Google search results linked, was lawful, Google could still be forced to de-index specific results relating to a subject’s name. In particular, the court reasoned that the appearance of the contested data did violate the data relevancy principle as well as the principle of limited retention (Art. 6 (1) c and e Directive 95/45/EC) and therefore was unlawful in the meaning of Art. 12 (b) Directive 95/46/EC. Furthermore, since Google only could justify further processing by invoking Art. 7 (f) Directive 95/46/EC – overriding the interest of the controller since the data subject never consented to Google processing his personal data – the court reminded Google that a data subject has a right to object to such processing of personal data pursuant to Art. 14 Directive 95/46/EC.

II. France

1. Oblivion and the Various Provisions Protecting Privacy

- 34 The French constitution does not provide for a fundamental right to privacy or personality but rather makes a reference to the Declaration of Human and Civic Rights of August 1789 (1789 Declaration) in its preamble. Nevertheless, Art. 9 of the French Civil Code (CC), which guarantees everybody a general right to privacy, can be seen as the codification of the protective standards courts have drawn in the past from Art. 12 of the 1789 Declaration.⁵⁰ Even if some legal scholars deem Art. 29 of the Act on the Freedom of the Press⁵¹ as the establishment of the right to privacy, the latter is merely a libel action that prohibits defamation.⁵² Additionally, the scope of Art. 1382 et seq. CC (the basic provision of French tort law) has traditionally been very broad, which has led to quite an effective protection of personality rights in France.⁵³ The right of oblivion – having personal data deleted when it is no longer newsworthy – is seen as a particular right of personality.⁵⁴ However, up to today the right is not explicitly provided by statute but rather is derived from “judicial reasoning” when applying the aforementioned provisions.⁵⁵
- 35 The effectiveness of the French legislation is also reflected in the country’s extensive case law. In different instances the French jurisdiction has elaborated on the conditions under which an individual can claim his right of oblivion. The High Court of Paris (“Cour d’appel”) initiated the discussion, in 1967 in the case *Delle Segret v. Soc Rome Film*.⁵⁶ In its decision, Mme. S’s demand for damages against a movie company that had produced a docu-fiction movie on the serial killer Henri Landru, to whom she had been a mistress, was rejected, based on the argument that she had previously made the story public in her published memories.
- 36 In 1981 the High Court of Paris ruled that the disclosure of personal information relating to an individual who had been involved in a tragedy fifteen years back could not be justified because there was no necessity to disclose such information. The court thereby acknowledged a right to oblivion.⁵⁷ In 1983 in the well-known *Papon* decision,⁵⁸ the Regional Court of Paris (“Tribunal de grande instance”) defined the boundaries of the right of oblivion that had been acknowledged two years earlier. In *Papon* the court stated that it is neither the duty nor the competence of French judges to decide how a special episode of history should be remembered or characterized in history. The court argued that a historian could only be liable if he was disclosing inaccurate or twisted facts, or when the disclosure of the facts was not

justified by any historical interest when the person concerned was still alive.⁵⁹

- 37 Nevertheless, it seemed to have become the accepted *opinio juris* amongst French Regional and High Courts that “a public event, after the passing of a sufficiently long time, can become, for the person who was its protagonist, a fact of private life again, which may remain secret or forgotten”.⁶⁰ However, and somewhat surprisingly, when a woman requested the suppression of publications on her activities during the occupation of 1940-45, the Supreme Court’s first civil chamber (“Cour de Cassation”) dismissed the notion that a right of oblivion may be invoked when the information had been lawfully disclosed in the local press and therefore no longer belonged to the private sphere.⁶¹

2. Defamatory Autocomplete Suggestions

- 38 The judicial reasoning in France shows the delicate balance between the personality rights of an individual, the freedom of the press and the freedom of information depending on the specifics of the case. Today, in particular search engines – or Google as the dominant search engine in Europe – also face accusations of infringement of personality rights. In 2010, the Regional Court of Paris had to decide whether the plaintiff could, based on Art. 29 Freedom of the Press Act, demand erasure of the autocomplete suggestions “rapist”, “sentenced”, and “satanist” when inserting his name in the search box.⁶² The court qualified the autocomplete suggestions as allegations or imputations that undermine the honour or reputation of the plaintiff. The court argued that since the algorithms are based on human thought, Google must prove why the search results they provide should not be viewed as a statement from the company. Since Google failed to do so, they were ordered to delete these autocomplete suggestions.
- 39 Another decision of the High Court of Paris dealt with autocomplete suggestions and preliminary measures. The court found that the search suggestion “fraud” next to a company’s name was capable of libelling, especially because the average Internet user follows the suggestions. It concluded that the suggestion could be interpreted as Google’s opinion, in particular because it was presented as helpful input and it was not obvious that it was generated automatically. Therefore, requiring Google to take all necessary measures to eliminate those privacy-infringing results did not violate the company’s freedom of expression.⁶³ In a later decision, the same court concluded again that it is appropriate to require Google to delete suggestions that were “obvious infringements of privacy”. The respondents’ objection that the suggestion was delivered by an algorithm was dismissed because the

court ascertained that Google is able to filter racist or pornographic suggestions and therefore it should be feasible to do the same for defamatory suggestions.⁶⁴

3. Data Protection Law and Erasure

40 France was among the first countries that enacted a law on data protection.⁶⁵ The “*Loi n°78/17 du 6 janvier 1978, relative à l’informatique, aux fichiers et aux libertés*” (Act 78/17), which had considerable influence on the drafting of the Directive 95/46/EC,⁶⁶ was amended in 2004 according to EU standards.⁶⁷ The two most relevant provisions with respect to erasure are Arts. 38 and 40. While the former establishes a right to object to the personal data processing for legitimate reasons, the latter guarantees every individual, for any incomplete data, expired data or data for which processing is unlawful, a right to have it rectified, completed or deleted. Art. 40 Act 78/17 is seen as a procedural right which entitles the individual to have its data deleted whenever its right to privacy is infringed. It is interesting to note that most of the reviewed case law regarding the erasure of personal data has not been based on Art. 40 Act 78/17.⁶⁸ Nevertheless, in the 2011 *Mme. C. v. Google* decision, the Regional Court of Montpellier elaborated that Google had an obligation under Art. 38 Act 78/17 to allow subsequent withdrawal of personal data by de-indexing webpages.⁶⁹ With respect to de-indexation, the recent ruling by the Regional Court of Paris⁷⁰ elaborates on the hosting provider’s liability with respect to erasure. The decision was based on Art. 6 Law for Confidence in the Digital Economy (LCEN),⁷¹ which establishes the notice and take down obligation on hosting providers, as laid out in the Directive 2000/31/EC (cf. C.I.1).⁷² Under this provision, the hosting provider will be held liable whenever the demanding party demonstrates the hosting provider’s actual knowledge of the contested content and his wrongdoing. Such a wrongdoing is seen in the continued distribution of the unlawful content or in not having reacted to the request immediately.⁷³ Therefore, the Court of Paris held that Google had participated in the realization of the moral damage the plaintiff had suffered from having her name linked to pornographic webpages. Even though it is based on different legal norms, the case has similarities to the previously mentioned *Mme. C. v. Google* decision of the regional Court of Montpellier in 2011. In both cases, former porn actresses were demanding the de-indexation of webpages relating to their past activities.

41 The Regional Court of Paris dealt with explicit content once again when it ordered Google to block images depicting Max Mosley during a privately held Nazi-themed sex act. The British High Court of Justice as well as the Regional Court of Paris had recognized the unlawfulness of distributing such pictures and subsequently approved Mr. Mosley’s demand for

erasure.⁷⁴ Google also complied with the erasure notice and deleted several photographs from its image service. Nonetheless, the pictures reappeared, which led Mr. Mosley to demand that Google de-index the defamatory photographs from its search results. Based on Art. 6 LCEN, Mr. Mosley demanded that Google be ordered to remove and prohibit the future publication of those explicit photographs. When applying Art. 6 LCEN, such measures must be proportionate and limited in time. The illegality of the pictures confirmed by two European courts, and the fact that Google filters images automatically when uploading them to its services, led the court to affirm the proportionate nature of the request.⁷⁵

III. Germany

1. Oblivion in the System of Constitutional, Civil and Criminal Privacy Protection

42 In Germany the Constitutional Court (“*Bundesverfassungsgericht*”) has interpreted the “right to personality” in Art. 2 (1) of the German Basic Law (GG) of 1949, which guarantees to everyone a “right to free development of his personality”. The introduction of Art. 1 (1) and Art. 2 (1) GG was crucial for the evolvement of personality protection.⁷⁶ In the light of the latter two provisions, German courts interpreted § 823 (1) of the German Civil Code (BGB) – whose scope is not as wide as Art. 1382 CC in France⁷⁷ – in a way that protects the individual’s right of integrity of his physical body and belongings as well as his right to privacy.⁷⁸ However, many specific statutory provisions in private and criminal law further protect personal information – some of which were enacted long before the GG.⁷⁹

43 The German case law dealing with the right to personality – and in particular the right of oblivion – is extensive.⁸⁰ Important leading cases⁸¹ in this respect are the *Lebach I* and *Lebach II* decisions. In the German Constitutional Court’s *Lebach I* decision, the airing of the ZDF produced docu-drama on a criminal gang who had killed five soldiers in 1969 was prohibited because it showed C’s name and picture (C had been an actual member of the gang and at the time was still in prison). It was reasoned that the airing would have affected his privacy as well as public interest, in regard to putting his rehabilitation in danger.⁸² While the *Lebach I* verdict was rendered in 1973, the *Lebach II* case dates to 1999. Another TV station wanted to air a TV documentation on the gang’s deeds. This time, however, the gang members were neither named nor were pictures of them shown during the documentary. The German Constitutional Court therefore argued that the right to personality does not entitle criminals with a claim of not being confronted with their deeds in public

ever again. Such an interpretation of the *Lebach I* decision was deemed to be misleading.⁸³

- 44 The *Hooligan* decision of the High Court of Berlin (“Kammergericht”) in 2001⁸⁴ was an interesting one with respect to the digital storage of information. The decision concerned a news article reporting on the tragic incident at the FIFA World Cup 1998 when a hooligan almost killed a policeman by kicking him in the head. The article reported the story (including a picture of the hooligan), rendered a psychological analysis of the hooligan’s character and stated that he was an international drug lord (which turned out to be wrong). The hooligan demanded deletion of the article from the newspaper’s online archive by invoking the tort of privacy infringements in connection with the libel action and his right to personality. The court acknowledged that after a certain amount of time, the criminal’s interest in anonymity could outweigh the public interest in the information. Yet the court got around balancing the right to privacy with the right to information by clarifying that an online archive is a “pull service”, which is not to be confused with a publication. The archive therefore enjoys a right to store any article based on the freedom of speech (Art. 5 (1) GG).⁸⁵
- 45 In 2006 the High Court of Frankfurt (“Oberlandesgericht”) also dealt with issues resulting from online newspaper archives and balanced the right of oblivion in light of the benefits of rehabilitation. The court acknowledged a general right of oblivion, but denied it in the particular case due to the plaintiff’s lifetime imprisonment and thus a lack of interest in rehabilitation. The court stated that freedom of speech requires an unrestricted access to information and doubted whether an archive should be ordered to “change history”.⁸⁶ One year later, the High Court of Hamburg did not seem to have such reservations. In its decision, it argued that based on § 823 (1) BGB in connection with Art. 1 (1) and Art. 2 (1) GG, the interest in rehabilitation did outweigh the interest of the archive in being complete. It therefore had to delete the plaintiff’s name from its publications. Furthermore, concerning the potential harm articles on convicted persons can have on their rehabilitation, the court found that monitoring its archives in order to prevent infringements of the right of oblivion seems to be a reasonable obligation for an online archive.⁸⁷
- 46 The so-called *Sedlmayr* case has gained much attention. Two brothers had killed the famous actor Walter Seldmayr in 1990. Though they had been sentenced to lifetime imprisonment in 1993, one brother was released on probation in 2008. He filed several claims against media webpages, inter alia one against a German radio. The latter had stored an online report dating from 2000 in its web archive, in which the 10-year anniversary of the killing was remembered. While the High Court

found this case comparable to the *Lebach I* case, the Supreme Court (“Bundesgerichtshof”) came to a different interpretation of § 823 BGB, Art. 1 (1), Art. 2 (1) GG and Art. 8 ECHR when it weighed them against statutes protecting the freedom of speech and information (Art. 5 GG and Art. 10 ECHR). Even though data protection law was invoked, it was considered not applicable due to reservations resulting from international public law. The Supreme Court stated that when current events are reported, the public interest in the information generally outweighs other individual interests, but that such reports could become unjustified during time. The court subsequently weighed different factors against each other, such as the time elapsed between the event and the report, the correctness of the report and its impact. Since the contested report was found to be based on true facts and not stigmatizing as well as – unlike *Lebach I* – not of broad public impact, the Supreme Court decided in favour of the plaintiff. Further it was reasoned that an imperative of deleting identifying reports on criminal conduct would eventually lead to deleting history and the media would not be able to fulfil its purpose of informing the public – as they are ordered by the GG.⁸⁸ Note that the court had similar reservations with regard to “erasing” history as they could be seen in the Regional Court of Paris’ *Papon* decision (cf. C.II.1). It also must be mentioned that there were several *Sedlmayr* decisions, and all media companies defeated the claimant.⁸⁹

- 47 In sum, German jurisdiction has been reluctant to grant the right of oblivion on grounds of infringement of the individual’s right to personality. German courts have balanced (in different instances) the interest in having “historical news” deleted versus the freedom of the press. Especially in light of the potential endangerment of the rehabilitation into society, an interest in oblivion has been acknowledged. As illustrated by the cases presented, the right of oblivion is only granted when the benefits of rehabilitation outweigh the censorship of the press.
- 48 Furthermore, one should mention the *Kannibale von Rothenburg* ruling by the German Supreme Court in 2009, in which a known cannibal was unsuccessful in trying to stop the airing of a horror movie that was an adaption of his disturbing deeds. His case was dismissed because he himself had exposed details of his crime and his identity to the public and therefore failed to prove that his rehabilitation was endangered by the movie.⁹⁰ Similar to the above-mentioned 1967 Paris Appellate Court’s *Delle Segret v. Soc. Rome Paris Film* decision,⁹¹ the conclusion may be drawn that a right of oblivion can also be waived if the subject itself reminds the public of its deeds.

2. Data Protection Law and Erasure

- 49 The fundamental legal ground for privacy protection when personal data is being processed lies in the German Federal Data Protection Act (BDSG). This law incorporates the principles of data processing laid out in the Directive 95/46/EC.⁹²
- 50 § 35 BDSG lays out the foundation of the right of erasure of personal data when this data is being processed by non-state entities. In particular, § 35, (2) BDSG distinguishes four general situations in which personal data may be erased; these arise whenever (1) the data is unlawfully recorded, (2) the data is sensitive, (3) the purpose of the collection of the data is fulfilled or (4) further retention is unnecessary. Moreover, personal data may not be collected, processed or used if the data subject lodges an objection with the controller and an examination indicates that legitimate interests of the data subject due to its particular situation outweigh the interest of the data controller in such collection, processing or use.⁹³
- 51 One case that dealt with § 35 BDSG was decided at the dawn of the new millennium by the High Court of Hamm. The defendant, a business information agency, had stored information on the plaintiff's number of employees, business routine, mode of payment, assets and liabilities. Most data was compiled from public sources, except the assets and liabilities which had been estimated. The plaintiff filed a lawsuit against the business information agency in which it demanded erasure. The court acknowledged that § 35 BDSG guarantees a right to erasure, except when consent was given to the processing (and that this was not the case was uncontested) or the law allows the processing. § 29 BDSG allows commercial collection from public sources as long as there are no legitimate overruling interests of the data subject. Because the information was not sensitive and there was, to a certain degree, a public interest in such data, its collection was legal. Accordingly, the request for erasure was rejected. Nevertheless, the agency had to rectify that the data on assets and liabilities were only estimated.⁹⁴
- 52 With regards to the admissibility of online rating platforms the Supreme Court's 2009 *spickmich.de* ruling was expected to be a landmark decision. The issue concerned a rating platform which allowed pupils to anonymously rate their teachers with regards to several criteria by using pre-fixed attributes such as "competent" and "well prepared". These ratings were combined to an overall grade. One teacher (she had received a 4.3, which is equivalent to a barely acceptable performance) sued the platform for forbearance. The court found that the respondent's processing of data could be justified by Art. 29 BDSG (collection from public sources for commercial reasons) as far as there are no legitimate

overruling interests of the data subject. In order to assess this question, the court weighed the "right to informational self-determination as provided for in Art. 1 (1) and Art. 2 (1) GG" against the freedom of speech and information as provided for in Art. 5 (1) GG. The court qualified the data in question as belonging to the professional social sphere, meaning that they were neither private nor even intimate. On the other hand, it found the platform to be designed in a manner that prevented libelling statements (e.g. besides the possibility to rate a teacher with pre-fixed attributes, there was no possibility to leave comments) and acknowledged pupils and their parents' legitimate interests in comparing teachers. The claim was therefore dismissed.⁹⁵ Yet the Supreme Court's judgment highlights that there is no general rule regarding the admissibility of online rating platforms; rather, each case must be assessed individually.

3. Defamatory Autocomplete Suggestions

- 53 It is further interesting to note that in Germany, the "well-known" claims against the autocomplete function of Google were not based on data protection law. In 2011, the High Court of Hamburg had to decide, on the grounds of defamation and general tort law,⁹⁶ whether the claim of a real estate company was legitimate or not. The claimant demanded that Google delete the autocomplete suggestion "fraud". In addition, he demanded that various pages and snippets, in which the real estate company was accused of betraying its customers, be de-indexed from the search results. According to the claimant, the snippets were an expression of Google's opinion and therefore were capable of being a violation of personal rights. Yet the High Court of Hamburg found that an algorithm – without human intervention – had produced the search results and that these were not the opinion of Google as the search engine would only provide results that are already available on the Internet. Additionally, the court held that Google had no duty to examine and filter the source of search results beforehand, and that its participation in the alleged violation of privacy rights was neither voluntary nor of appropriate causality. The High Court of Hamburg thereby rejected the claim for forbearance.⁹⁷
- 54 Similar reasoning led to denying a right to erasure by the High Court of Munich. The claimant, an address register provider, demanded the deletion of Google's search results which accused him of fraud. Furthermore, he demanded the deletion of the search suggestions "fraud" and "rip-off" associated with his name. The court argued that Google provides results – in the form of snippets and search suggestions – which are automatically generated. Thereby, Google does not make a statement of its own but rather re-organizes pre-existing content. As

this was considered an obvious fact to the average user, Google could not be considered an offender, accomplice or assistant to any privacy-infringing action. Furthermore, the court reasoned that a notice and take down obligation would require a so-called “duty to secure fair competition”. Such an obligation would only arise when being notified of an obvious privacy infringement. Privacy infringements, however, were deemed to be far from obvious because they involve a complex balancing of interests and therefore a notice and take down obligation was denied.⁹⁸

- 55 These decisions showed that German courts highly valued the right to information and therefore were reluctant to impose any liability on a search engine for its results or autocomplete suggestions.⁹⁹ Surprisingly, the German Supreme Court overthrew this approach in its *Scientology* decision in 2013. In this case, the plaintiffs, an online drugstore and its founder and chairman R.S., sued Google for the search suggestions “Scientology” and “fraud” and demanded forbearance. By invoking the above-mentioned arguments, the High Court of Cologne dismissed the claim.¹⁰⁰ However, the Supreme Court reasoned that “Scientology” and “fraud” are both words with negative associations and since the average user expects that these suggestions are helpful inputs, they are capable of invading privacy rights. In the present case, such a privacy infringement was acknowledged, in particular because the suggestions created untrue associations. The court concluded that even if generated by an algorithm, the search engine is accountable for its suggestions. In particular, the notion that search engines could be considered as mere hosting providers was dismissed. However, in the court’s view, search engines should not be obliged to check all suggestions in advance, but should take measures to prevent their suggestions from infringing privacy rights. The significance of this is that if someone notifies the search engine that the suggestions are infringing upon his or her privacy rights, this notification creates an obligation to check whether this is the case and eventually delete the contested suggestion.¹⁰¹ Therefore, as in France, search engines face accountability for autocomplete suggestions generated by algorithms and qualify as content providers in this respect. Nevertheless – as opposed to France, where obvious privacy infringements must be taken down in advance – the German Supreme Court merely established a notice and take down obligation for a content provider based on the general privacy tort action.

IV. Italy

1. Privacy and Data Protection Provisions

- 56 According to Art. 2 of the Italian Constitution, “the Republic recognizes and guarantees the inviolable rights of a person, as individual and in the community where he expresses its personality (...)”. In combination with Art. 15, which protects the secrecy of correspondence, those constitutional norms lay out the foundation for protecting an individual’s privacy.¹⁰² Yet in civil law there is no statutory provision protecting a general right to personality or privacy; rather, only certain aspects of personality (such as name and physical integrity) enjoy protection.¹⁰³
- 57 On a base level, the protection of personal data is seen as a subjective right that strengthens the individual’s right to defence against actions that adversely affect his right of privacy.¹⁰⁴ The Italian Data Protection Act¹⁰⁵ (Legislative Decree 2003/196) incorporates in Art. 7 (3) the right of the data subject to demand erasure or anonymization of personal data if the processing is illegitimate or if the maintenance of the data is no longer necessary in relation to the purpose for which they were specifically collected. Furthermore, the data subject has the right to update, rectify or complete the data with additional data.¹⁰⁶ These tools allow the rectification of the data after its collection and mutation.¹⁰⁷ Art. 11 (1e) states that identifiable personal data shall not be processed over a certain amount of time necessary for the purposes for which they have been collected. According to Italian scholars, once the purposes are attained or no longer of interest, the data subject has the right “*ad essere dimenticato*”,¹⁰⁸ i.e. the “right to be forgotten”. Thereby, Italian law prohibits the maintenance of personal data as soon as it fulfils its purpose of collection.¹⁰⁹

2. The Right of Oblivion and Online Archives

- 58 It should first be mentioned that Italian literature distinguishes between privacy and reservation, yet states that these two concepts are overlapping and intermingled. While privacy is understood as a guaranteed freedom to determine for oneself how to shape one’s private life, reservation protects the integrity of the individual’s private sphere.¹¹⁰ Those rights were further developed by courts and include, among others, the right of reputation, the right to rectification, the right to be let alone and the right of image and name.¹¹¹ In their core, these rights protect the personality and identity of the individual.¹¹² Since the personality of an individual consists of different aspects varying over time, the

right of oblivion balances the conflict between an accurate story (at the time it occurred) and an actual person's identity at the time being. In this regard, the right of oblivion guarantees a right to reservation.¹¹³ Therefore, Italian jurisprudence and legal scholars define the right of oblivion as the individual's right to prevent the publishing of old news concerning him or her, even if the reported events had once been newsworthy and legitimately published.¹¹⁴ Special focus lies on the role of time and the balance between public and individual interests.¹¹⁵

- 59 In 1984 the Italian Court of Cassation ("Corte di Cassazione") established three criteria determining the boundaries of the freedom of the press. The dispute before the court involved different reports published in a monthly newspaper concerning the common funds of two real estate companies. The plaintiffs claimed that these reports published in 1972/1973 were denigrating and demanded, based on Art. 2043 of the Italian Civil Code, the subsequent prohibition of the reports and damages for the loss suffered. In its decision, the court debated the limits of the freedom of the press, a right guaranteed in Art. 21 of the Italian Constitution, and regulated in the Press Act.¹¹⁶ The court established three criteria limiting the freedom of the press: first, the reported information needs to be of social or public interest; second, the coverage needs to be correct (or at least the result of a serious investigation towards finding the truth); and third, the information must be presented in an objective, civilized manner. The decision balanced arguments such as the social utility of the information, newsworthiness, need for completeness of the information, intrusions in the private sphere of the individual and the potential harm to his image, honour and reputation.¹¹⁷
- 60 Later in 2012, the Court of Cassation dealt with the right of oblivion in online newspapers.¹¹⁸ A politician who had been arrested and charged with corruption in 1993 and subsequently acquitted, requested that a news article regarding his arrest be removed from the archive of the "*Corriere della Sera*", which was still indexed by search engines. Even though the event of his arrest and charges were true, the Court of Cassation acknowledged that the information in the article was incomplete, since the charge had been dropped. Balancing the freedom of the press and the individual's right to privacy and oblivion, the court ruled that the newspaper had an obligation to equip its archives with "an appropriate system designed to provide information (in the body of the text or in the margin) on whether there exists a follow-up or any development to news items and if so what the content is [...] allowing users swift and easy access to the updated information."¹¹⁹ Therefore, it is necessary to amend information¹²⁰ on the development of the case so that the users are presented with an accurate picture of the events. However, search engines were viewed as mere

intermediaries and hence not responsible for the information or obliged to de-link the contested webpages.

- 61 Prior to this ruling, the Italian data protection authority issued two decisions in 2005 and 2008 concerning online archives. The first ruling dealt with the online retrieval of a decision issued in 1996 by the Italian Antitrust Authority against a company on account of misleading advertising.¹²¹ The data protection authority stated that such an online retrieval on external search engines should be restricted. Next to the establishment of a restricted-access section to old decisions on the antitrust authority website, which must not be retrievable by standard search engines, the Italian DPA ordered the Antitrust Authority to define the time period during which the posting of free decisions seemed proportionate. Thus, access must be granted to decisions that are still relevant for fulfilling their purpose; respectively, access to decisions that have already achieved their purpose should be restricted. The Antitrust Authority complied by applying robotmeta tags¹²² to decisions that were more than five years old (sanctions against offenders were statute-barred after this time). In the second decision, *DPA v. Google Inc. and Rcs Quotidiani S.p.A* of 2008, the data protection authority balanced the individual right of oblivion with the freedom of expression, the freedom to exercise free historical research, the right to education and information as well as with the rules on protection of personal data. The DPA held that there were legitimate grounds for publishing the contested publication – at that time an undisputed depiction of facts of public interest. Nevertheless, the DPA argued that there were no legitimate grounds for personal data in online archives being retrievable through external search engines. In other words, an archive's web page that exhibits personal data must be de-linked from the external search engine function by the company that acts as the content provider.¹²³

3. Defamatory Autocomplete Suggestions

- 62 In 2011 the Regional Court of Milan ("Tribunale Ordinario di Milano") dealt with a matter concerning autocomplete suggestions by Google. The plaintiff demanded that the suggested search result "fraud" or "crook" next to his name be erased. The court ruled in the plaintiff's favour: a user seeing such a suggested search result would be suspicious and assume illicit activities by the plaintiff; the user would therewith be more likely to stop his further search enquiry. Therefore, the court stated that such an autocomplete suggestion infringes the honour and reputation of the person it relates to. Simultaneously, the court specified that the search suggestions are based on a "neutral" algorithm that does not differentiate between good and bad. The

association between the applicant's name and the words "scam" and "crook" was considered the work of the software specially developed and adopted by the claimant to optimize access to its database. While Google itself was considered a hosting provider under Directive 2000/31/EC (and its implementation into Italian law in Legislative Decree 70/2003), Google's "autocomplete function" was deemed to fulfil characteristic functions of a content provider, namely by choosing which information to provide to its users. The court found that Google was liable for autocomplete defamatory suggestions that average individual users are unable to distinguish from truthful facts.¹²⁴

- 63 Two years later, the same Regional Court of Milan decided a case in which it excluded Google from liability for defamation with respect to the autocomplete suggestions.¹²⁵ The court reasoned that notwithstanding the qualification of Google as a caching, hosting or content provider, the company would still be responsible under Art. 15 and 16 Legislative Decree No. 70/2003 to remove defamatory content from its autocomplete function on an urgent basis. The court concluded, however, that even though Google had thus no general obligation to monitor the information and *in casu* autocomplete keywords, it did have a duty to remove illicit content if required to do so by a competent judicial authority.¹²⁶

D. Putting Oblivion, Erasure and Forgetting into Context: Insights Drawn from the Comparative Case Law Analysis

- 64 Since 1995 the European Member States have set a Union-wide standard for data protection. Nevertheless, the different legal backgrounds have led to a diverse implementation of data protection principles into national legislation. Therefore, to understand the *ratio legis* of the right of oblivion and the right to erasure and the evolution of the concept of forgetting on a Union and national level, it is essential to discuss the legal provisions and case law dealing with these concepts.
- 65 The insights can be summarized in the following main points:

The right of erasure as provided for by data protection law has rarely been the only legal ground in courts.

The right of erasure as established in data protection law has served only in few instances as the only legal ground of a court decision. Instead, other civil or criminal law provisions have been called upon when an individual's personality right is infringed.

Therefore, when it comes to discussing the potential benefits of introducing a right to be forgotten in data protection law, legislators should be aware of existing laws and case law with respect to privacy protection. The current debate has failed to thoroughly analyse and benefit from existing judicial reasoning on the right of oblivion that provides for a differentiated balancing of interests. However, the recent ECJ ruling could foster the importance of data protection law, since the court based its ruling on the latter.

Oblivion may be achieved by other means than erasure.

National legal systems in Europe have taken different approaches when it comes to balancing conflicting interests and – once a violation of privacy has been assessed – rely upon different measures to end such a violation. In Germany, the national case law dealing with the traditional concept of oblivion often focuses on the question of whether or not rehabilitation of the individual will be affected. The extensive case law on this subject helps to define which criteria affect the balance between the public's interest of knowledge with the individual's interest of privacy. If the individual right outweighs other interests, German courts will order the violator to erase the illicit content. Thereby, German courts need to balance between erasing historical facts and the individual interest in having these facts forgotten. Interestingly, the Italian jurisprudence highlights that the rectification of personal data or restricting its retrievability, in comparison to its total erasure, is less radical and interferes less with the freedom of information or expression. In light of the recent ECJ ruling, future research should also focus on measures such as rectification or restricting online retrievability (e.g. ordering the application of robot-meta tags or de-indexing).

The easy access and quick retrieval of personal data via search engines is the main concern of individuals regarding their online privacy.

The reviewed case law shows that increased accessibility has catalysed online privacy concerns. In particular, Google's autocomplete software has been at the heart of various lawsuits. The question of whether or not the autocomplete function requalifies a search engine as a content provider has been discussed in depth, in particular in Italy. While the court decisions show that there have long been insecurities on how to approach the ruling against autocomplete suggestions, the establishment of a notice and take down obligation is deemed to be proportionate by German and Italian courts.

The recent ECJ ruling also shows that the role of information intermediaries should not be underestimated. An individual may object to the further processing of data by a search engine. However, the search engine has some discretion

when it balances the conflicting interest and is only forced to de-index search results when ordered to do so by a competent authority. It should be examined in further detail if this means that search engines are subject to a de facto notice and take down obligation with respect to personal data.¹²⁷

Sometimes the right to oblivion can be waived.

Courts in Germany and France have acknowledged the possibility of waiving the right of personality: in both the 1967 Paris Appellate Court *Delle Segret v. Soc. Rome Paris Film* decision as well as the *Kannibale von Rothenburg* Supreme Court ruling of 2009, a person's right of oblivion was disregarded because of prior public communication of the disputed facts. It is questionable whether or not EU regulators have given enough thought to the possibility to waive one's right of oblivion when drafting the concept of the right to be forgotten. It seems more likely that the right to be forgotten would implement a right to have information erased when the consent to its publication is withdrawn.

In this regard, one may ask whether the data subject in the latest ECJ ruling still has a legitimate interest in having certain search results deleted by claiming they have become irrelevant. After all, the subject's entire name as well as the related attachment proceedings were not only mentioned in the ruling but the subject was also recently interviewed by newspapers.¹²⁸

While oblivion and erasure are complementary legal tools, the right of erasure has the potential to neglect the thorough balancing of conflicting interests.

Finally, the legal tools of oblivion and erasure are used in a complementary way. In other words, both concepts fulfil different purposes needed in legislation: while the right of oblivion incorporates a substantial concept for balancing conflicting interests in order to determine when once-newsworthy information should become irrelevant to the broader public, the right of erasure has a more procedural character. The outlined national legislations and court practices in France, Germany and Italy show that on a national level, the right to erasure is understood and applied as one of many corrective measures to end an infringement of privacy. The Italian case law especially highlights this understanding: the discussed requests for erasure were balanced with other rights, and often the demand for erasure was replaced by a less radical enforcement measure, e.g. rectification. In addition, the case law illustrates that erasure will be granted only after the thoughtful deliberation of substantial conflicting rights.

rights that may be invoked whenever the provisions of the Directive 95/46/EC are violated, the ECJ saw no reasons to elaborate on the rights of freedom of information and expression. This contradicts the examined national case law where these rights are carefully balanced against privacy and personality rights. This may be attributed to the fact that the focus of data protection law lies on the adherence of processing principles rather than on balancing conflicting fundamental rights on a case-by-case basis. Nevertheless, Art. 12 (1) b Directive 95/46/EC gives some discretion with regards to the measures that can end a privacy infringement. Regulators should bear in mind that while erasure might be the easiest way to end a privacy infringement, it may, however, not be the most proportionate one in all cases.

E. Conclusion

67 EU policy makers are legitimately concerned with users' online privacy. It is questionable whether or not the right to be forgotten might address users' fear of being haunted by their digital past. First of all, the terminology has led to controversial reactions among scholars as well as industry leaders. Second, the fact that the right was re-labelled as the right of erasure reflects policy makers' ambiguity towards the terminology used. In fact, we argue that the right to be forgotten is a generic term, bringing together the existing rights of oblivion and erasure. Therefore, it is important to understand the rationale and concepts of those rights as well as their practical implementation.

68 Policy makers were awaiting the *Google Spain v. Spanish Data Protection Agency* ECJ ruling in order to glean some insights on the right to be forgotten. Correctly, the ECJ highlights that in the online context, the retrievability of data is a major issue – a finding supported by the fact that search engines are involved in many legal disputes before courts in Germany, France and Italy. Nevertheless, we think that, while the Directive 95/46/EC was interpreted in the light of the fundamental rights to privacy, the fundamental rights of expression and information would have deserved more consideration. Seemingly, it seems problematic to establish general rules on the weighing of interests. Rather, such weighing must be done on a case-by-case basis. Therefore, an in-depth analysis of case law established in the EU member states could provide policy makers with a more nuanced picture of the current implementation of oblivion and erasure – a picture which yields that no right to erasure, oblivion or forgetting can be absolute, but rather that they have to be carefully weighed against the freedom of speech and information. Since the latter is justifiably a cornerstone of any democratic

66 By understanding the rights provided for in Art. 12 (1) b and Art. 14 (1) Directive 95/46/EC as procedural

society, policy makers are well advised to pursue this challenge candidly.

* Aurelia Tamò is a PhD candidate at Chair of Information and Communication Law, University of Zurich. Damian George is a junior associate at Nobel & Hug attorneys at law in Zurich. The authors would like to thank Prof. Dr. Urs Gasser, Executive Director at Berkman Center for Internet & Society, Harvard University; Prof. Dr. Florent Thouvenin, Chair of Information and Communication Law, University of Zurich; J.D. Cynthia Anderfuhren-Wayne, attorney at law at Nobel & Hug attorneys at law Zurich; Zach Lerner, Legal Research Assistant with Youth and Media Project at Berkman Center for Internet & Society, Harvard University; and the JIPITEC Review Committee, for their helpful inputs and discussions. The views expressed in this publication are the sole responsibility of the authors.

- 1 Cf. e.g. Special Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union, June 2011, p. 56 on the perceived risk of disclosing personal information.
- 2 Cf. Official Journal L 281, 23/11/1995 P. 0031 – 0050.
- 3 Cf. EC sets out strategy to strengthen EU data protection rules, IP/10/1462, Brussels, 10.11.2010; EC Frequently asked Questions on the Data Protection Reform, MEMO/10/542, Brussels, 10.11.2010.
- 4 Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press 2009.
- 5 Alessandro Mantelero, U.S. Concern about the Right to Be Forgotten and Free Speech: Much Ado about Nothing?, *Contratto e Impresa*. Europa Vol. 17 (2012) No. 2, pp. 727-740; Meg Leta Ambrose/Jef Ausloos, The Right to Be Forgotten Across the Pond, *Journal of Information Policy*, Vol. 3, 2013, pp. 1-23; Franz Werro, The Right to Inform vs. The Right to Be Forgotten: A Transatlantic Clash, in: Aurelia Colombi Ciacchi/Christine Godt/Peter Rott/Leslie Jane Simth (eds.), *Haftungsrecht im Dritten Millennium*, Baden-Baden 2009, pp. 285-300; Laura Lagone, The Right to Be Forgotten: A Comparative Analysis, Working Paper Series, December 7th, 2012.
- 6 Cf. e.g. Adam Thierer, California Eraser Button Passes, *The Technology Liberation Front*, September 26, 2013; Eric Goldman, California's New 'Online Eraser' Law Should Be Erased, *Forbes*, September 24, 2014.
- 7 Herbert Burkert, Privacy – Data Protection: A German/European Perspective, in: Engel Christoph/Keller Kenneth H. (eds.): *Governance of Global Networks in the Light of Differing Local Values*. Baden-Baden 2000, p. 46.
- 8 Cf. also Huw Beverley-Smith/Ansgar Ohly/Agnes Lucas-Schloetter, *Privacy, Property and Personality: Civil Law Perspectives on Commercial Appropriation*, Cambridge 2005, p. 207.
- 9 Herbert Burkert, *Changing Patterns – Supplementary Approaches to Improving Data Protection. A European Perspective*, Presentation at CIAJ 2005 Annual Conference on Technology, Privacy and Justice, Toronto September 29-30, 2005, p. 4.
- 10 Cf. Fred Cate/Viktor Mayer-Schönberger, Notice and consent in a world of Big Data, *International Data Privacy Law* 3 (2), 2013, pp. 67-73; Niko Härting/Jochen Schneider, Impulses for an Effective and Modern Data Protection System, *JIPITEC* 2011 (3), p. 197.
- 11 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010, COM(2010) 609 final, p. 7.
- 12 The concept of informational self-determination was developed by the German Federal Constitutional Court ("Bundesverfassungsgericht") in 1983. In its famous *Volkszählungsurteil* the court declared some provisions of the revised Census Act as unconstitutional. It articulated the right to informational self-determination as the "authority of the individual to decide himself, on the basis of self-determination, when and within what limits information about his private life should be communicated to others." Cf. *Antoinette Rouvroy/Yves Poullet*, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, in: Serge Gutwirth et al. (eds.), *Reinventing Data Protection?*, Springer 2009., pp. 45 et seqq.
- 13 Cf. e.g. *Napoleon Xanthoulis*, *Conceptualizing a Right to Oblivion in the Digital World: A human rights-based approach*, research essay at University College London, May 2012, pp. 16 et seq., who argues that the right to be forgotten of the Draft Data Protection Regulation dated 25.1.2012, COM(2012) 11 final constitutes – with the exception of the extension in Art. 17 (2) – a tautology of the right to erasure of the Directive 95/46/EC; Interchangeably using the term "right of oblivion" and "right to be forgotten": *Ovidiu Vermesa/Peter Friess*, *Internet of Things – Global Technological and Social Trends*, 2011 River Publisher, p. 79; *Cécile de Terwangne*, *Internet Privacy and the Right to Be Forgotten/Right to Oblivion*, *Revista de Internet, Derecheo Y Política (IDP)*, (13), February 2012, pp. 109 et seq., *Norberto Nuno Gomes de Andrade*, *Oblivion: The Right to Be Different... from Oneself – Reproposing the Right to Be Forgotten*, *IDP*, (13), February 2012, pp. 122 et seq., *Giusella Finocchiaro/Annarita Ricci*, *Quality of Information, the Right to Oblivion and Digital Reputation*, in: B. Custers et. al. (eds.), *Discrimination and Privacy in the Information Society*, Berlin 2013, pp. 289-299; *Cédric Burton/Christopher Kuner/Anna Pateraki*, *The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report*, *Bloomberg Privacy and Security Law Report*, January 21, 2013 state that the right to be forgotten is viewed by the Albrecht Report (cf. chapter B.III.2) as an extension of the right to erasure.
- 14 Cf. e.g. *Ambrose/Ausloos*, *supra* note 5, pp. 1-23, who distinguish between full deletion of public data (oblivion) and the removal of data processed by third parties (erasure); *Rolf H. Weber*, *The Right to Be Forgotten: More Than a Pandora's Box?*, *JIPITEC* 2011 (2), pp. 120-130, who distinguishes between the active and passive verb tense; see also *Antoinette Rouvroy*, *Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?*, in: *Stéphanie Lacour* (Ed.), *La sécurité de l'individu numérisé. Réflexions prospectives et internationales.*, Paris 2008, pp. 249-278.
- 15 *Paul Bernal*, *A Right to Delete*, *European Journal of Law and Technology (EJLT)* 2011 (2) No. 2, p. 2.
- 16 Cf. chapter C.III.1.
- 17 *Ambrose/Ausloos*, *supra* note 5; p. 2; *Mantelero*, *supra* note 5, p. 728.
- 18 The terminology "respect for privacy" is understood in this article as the overall idea of protecting an individual's privacy (private life, private sphere, private communication, etc.). Some jurisdictions – as will be discussed throughout this article – have codified the "respect" into a right of privacy.
- 19 *Ambrose/Ausloos*, *supra* note 5, p. 14.
- 20 *Ambrose/Ausloos*, *supra* note 5, p. 14.
- 21 *Ambrose/Ausloos*, *supra* note 5, p. 15.

- 22 European Commission, Why do we need an EU data protection reform?, Factsheet 2012.
- 23 Press Release, Speech Viviane Reding, Justice for Growth makes headway at today's Justice Council, SPEECH/13/29, 18.01.2013.
- 24 Cf. e.g. Katy Steinmetz, Lucky Kids: California Gives Minors the Right to Delete Things They Put Online, Time, September 23, 2013; Thierer, *supra* note 6.
- 25 Bert-Jaap Koops, Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice, SCRIPTed, Vol. 8, No. 3, 2011, pp. 229-256, p. 232 et seq.
- 26 Koops, *supra* note 25, pp. 233 et seq. as well as pp. 250 et seqq.
- 27 Weber, *supra* note 14, pp. 120 et seq.
- 28 Rouvroy, *supra* note 14, pp. 249-278.
- 29 Ambrose/Ausloos, *supra* note 5, p. 14.
- 30 Ambrose/Ausloos, *supra* note 5, p. 2.
- 31 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), Brussels, 25.1.2012, COM(2012) 11 final; in combination with recital 6, 53 and 54.
- 32 Council of the European Union, 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) – Key issues of Chapters I-IV, 2012/0011 (COD), n. 10227/13, Brussels, May 31, 2013, <http://register.consilium.europa.eu/pdf/en/13/st10/st10227.en13.pdf>. The version of June 21, 2013 is available at: <http://www.statewatch.org/news/2013/jun/eu-council-dp-regulation-revised-11013-13.pdf>.
- 33 European Parliament, Policy Department Economic and Scientific Policy, Reforming the Data Protection Package, Study 2012, p. 60.
- 34 The right to object as provided for in Art. 14 Directive 95/46 is limited to scenarios in which the procession was lawful only due to outweighing interests of the public or the controller (Art. 7 (e) and (f) Directive 95/46/EC); cf. Damian George/Aurelia Tamò, Ein Europäisches Recht auf Vergessen – eine Schweizer Pflicht zum Löschen?, in: Sandra Brändli/Roman Schister/Aurelia Tamò (eds.), Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft, Bern 2013, p. 49.
- 35 Cf. 17, (3) Regulation.
- 36 Cf. 17, (3), (a) (b) and (d) Regulation.
- 37 This provision is of special interest because Art. 14 of the Directive 95/46/EC – which already obliges Member States to introduce a right to object to the processing of personal data– goes less far: The scope of Art. 14 in combination with Art. 7 (e) and (f) were not applicable in cases in which the data subject wanted to withdraw his previously given consent. Ulrich Dammann/Spiros Simitis, EG-Datenschutzrichtlinie Kommentar, Baden-Baden 1997, Art. 14 N 2.
- 38 The compromise amendments are available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf (Compromise amendments 1-29) and http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf (Compromise amendments 30-91).
- 39 Compare Regulation, *supra* note 31, with the draft version of June 21, 2013, *supra* note 32.
- 40 Despite the European Union not being a member of the ECHR, it accedes its provisions according to Art. 6 par. 2 Treaty on the European Union.
- 41 Rolf H. Weber/Markus Sommerhalder, Das Recht der personenbezogenen Information, Zurich 2007, p. 97.
- 42 Cf. ECJ, Case 101/01, Lindqvist, [2003] para. 86.
- 43 Dammann/Simitis, *supra* note 37, Art. 12 N 16; Eugen Ehmann/Marcus Helfrich, EG-Datenschutzrichtlinie Kurzkomentar, Köln 1999, Art. 12 N 52 et seqq.
- 44 Dammann/Simitis, *supra* note 37, Art. 12 N 16.
- 45 Dammann/Simitis, *supra* note 37, Art. 12 N 16.
- 46 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 , 31/07/2002 P. 0037 – 0047.
- 47 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Official Journal L 178 , 17/07/2000 P. 0001 – 0016.
- 48 Cf. also Recital 22, 23, 26, 27, 28 of the Directive 2002/58/EC.
- 49 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ECJ, C-131/12, Reference to a preliminary ruling from the Audiencia Nacional 9.3.2012; the term "right to be forgotten" is understood as a right according to which "information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties".
- 50 Georgios Gounalakis, Privacy and the Media – A comparative perspective, Munich 2000, p. 74.
- 51 Official French title: Loi du 29 juillet 1881 sur la liberté de la presse.
- 52 Beverley-Smith/Ohly/Lucas-Schloetter, *supra* note 8, p. 149.
- 53 Beverley-Smith/Ohly/Lucas-Schloetter, *supra* note 8, p. 150; Mara Chromik, Die Entscheidungskriterien des Zivilrechts bei der Abwägung von Privatsphärenschutz und öffentlichem Informationsinteresse: Eine rechtsvergleichende Untersuchung zum deutschen, französischen und spanischen Recht, Munich 2011, pp. 3-4.
- 54 Roseline Letteron, Droit à l'oubli, Revue de droit public de la science politique en France et à l'étranger, 1996 n° 2, p. 385-424, p. 415, 419.
- 55 Letteron, *supra* note 54, p. 423.
- 56 Cour d'Appel de Paris, 15.3.1967, Delle Segret, c. Soc. Rome Paris Film, JCP 1967, 15107; cf. François Rigaux, La protection de la vie privée et des autres biens de la personnalité, Bruxelles/Paris 1990, p. 462 N. 403.
- 57 Court d'Appel de Paris, 13.10.1981, D. 1983, jur., 421.
- 58 Tribunal de grande instance de Paris, 6.5.1983, D. 1984, jur., 14, Papon.
- 59 Beverley-Smith/Ohly/Lucas-Schloetter, *supra* note 8, p. 174.
- 60 Beverley-Smith/Ohly/Lucas-Schloetter, *supra* note 8, p. 178, with reference to case law in Fn. 130.
- 61 Cass.civ. 1°, 20.11.1990, Mme. Monanges c. Kern, JCP II, 21908; decision available in French at: <http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007025328&fastReqId=1356475608&fastPos=1>; For an in-depth analysis, cf: Letteron, *supra* note 54, pp. 385 et seqq.; Beverley-Smith/Ohly/Lucas-Schloetter, *supra* note 8, p. 179.
- 62 Tribunal de grande instance de Paris, 8.9.2010, M.X. vs. Google and Eric Schmidt, decision available in French at: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2985.

- 63 Court d'appel de Paris, 9.12.2009, Direct Energie vs. Google, decision available in French at: http://www.legalis.net/spip.php?page=brevs-article&id_article=2804.
- 64 Court d'appel Paris 14.12.2011, Lyonnaise de Garantie vs. Google and Eric Schmidt, decision in French available at: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3303.
- 65 Weber, *supra* note 14, p. 123.
- 66 Christiane Féral-Schuhl, *Cyberdroit – Le droit à l'épreuve de l'Internet*, 6th Edition., Paris 2010, p. 35.
- 67 Cf. Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel physiques et modifiant la loi n°78/17 du 6 janvier 1978.
- 68 Cf. e.g. case Court d'appel de Paris, 9.12.2009, Direct Energie v. Google, based on Arts. 1382-1384 French Civil Code.
- 69 Tribunal de grande instance de Montpellier, 28.10.2010, Mme. C. v. Google, decision in French available at: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3121.
- 70 Tribunal de grande instance de Paris 15.2.2012, Diana Z. v. Google, decision in French available at: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3357.
- 71 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique; Art. 6 is the implementation of Art. 14 of the Directive 2000/31/EC into French law; Federica Casarosa, Wikipedia: Exemption from Liability in Case of Immediate Removal of Unlawful Materials, SCRIPTed Vol. 6, Issue 3, 2009, pp. 670-676, pp. 671 et seqq.
- 72 Casarosa, *supra* note 71, pp. 671 et seqq.
- 73 Féral-Schuhl, *supra* note 66, p. 801.
- 74 High Court of Justice, *Mosley v. News Group Newspapers* [2008] EWHC 1777 (QB), available at: http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/24_07_08moslevnewsgroup.pdf; Ordonnance de Tribunal de grande instance de Paris, 29.4.2008, unpublished.
- 75 Tribunal de grande instance de Paris, 6.11.2013, RG 11/07970, Max M. v. Google Inc. and Google France, decision in French available at: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3909.
- 76 Beverley-Smith/Ohly/Lucas-Schloetter, *supra* note 8, pp. 100 et seqq; The existence of this general personality right was contested for a very long time. It was claimed that only certain aspects of the right to personality such as the right to one's name or image could enjoy legal protection; cf. Ansgar Staudinger, in: Hk-BGB, 7th Edition, § 823 N 90, Baden-Baden 2012.
- 77 Chromik, *supra* note 53, p. 4 et seq.
- 78 Emanuel H. Burkhardt, Chapter 5, in: Wenzel et al. (eds.), *Das Recht der Wort- und Bildberichterstattung*, 5th Edition, Köln 2003, pp. 135 et seqq.
- 79 Cf. e.g. § 12 German Civil Code, which protects a right to one's name; §§ 22, 23 of the (Artistic Copyright Act), which guarantee a right to one's image are such specific provisions; §§ 185, 186 of the Criminal Code which is called upon when defamatory actions have occurred.
- 80 This article does not account for an exhaustive discussion of all the case law but restricts its focus on selected court rulings.
- 81 Cf. e.g. Bundesverfassungsgericht, 30, 173, 24.3.1971, Mephisto, decision available in German at: <http://openjur.de/u/31670.html>. In this decision, the right of oblivion of a deceased "public figure" was demanded by a family member. The publication of the book in which the fictional story was told was prohibited based on the argument that the family member's privacy was infringed upon by such a publication. Moreover, the court refused to assess the freedom of expression since "arts and expression are two different things".
- 82 Cf. Bundesverfassungsgericht, 35, 202, 5.6.1973, Lebach I, decision available in German at: <http://www.servat.unibe.ch/dfr/bv035202.html>.
- 83 Bundesverfassungsgericht, 1 BvR 348/98, 25.11.1999, Lebach II, decision in German available at: <https://openjur.de/u/182101.html>.
- 84 Kammergericht Berlin, 9 W 132/01, 19.10.2001, AfP 2001, 561, Hooligan, decision in German available at: <http://www.jurpc.de/jurpc/show?id=20030022>.
- 85 Kammergericht Berlin, 9 W 132/01, 19.10.2001, AfP 2001, 561, Hooligan, decision in German available at: <http://www.jurpc.de/jurpc/show?id=20030022>.
- 86 Oberlandesgericht Frankfurt am Main, 16 W 54/06, 20.9.2006, decision in German available at: <http://openjur.de/u/194303.html>
- 87 Oberlandesgericht Hamburg, 28.03.2007, Az. 7 W 9/07, <http://www.telemedicus.info/urteile/Allgemeines-Persoeneichkeitsrecht/Personen-der-Zeitgeschichte/Straftaeter/448-OLG-Hamburg-Az-7-W-907-Identifizierende-Berichterstattung-in-Online-Zeitungsarchiven.html>.
- 88 Bundesgerichtshof, VI ZR 227/08, 15.12.2009, Sedlmayr, (www.dradio.de), decision in German available at: <https://openjur.de/u/70781.html>.
- 89 Bundesgerichtshof, VI ZR 245/08, 20.4.2010 (www.morgenweb.de); Bundesgerichtshof, VI ZR 346/09, 22.2.2011 (www.faz.net); Bundesgerichtshof, VI ZR 243/08, 9.2.2010 (www.spiegel.de); Bundesgerichtshof, VI 217/08, 8.5.2012 (www.rainbow.at).
- 90 Bundesgerichtshof, VI ZR 191/08, 26.5.2009, Kannibale von Rothenburg, decision in German available at: <http://openjur.de/u/72210.html>.
- 91 Court d'Appel de Paris, 15.3.1967, Delle Segret, c. Soc. Rome Paris Film, JCP 1967, 15107.
- 92 Negotiated from 1970 until 1977, the BDSG was later revised in 1990 and again in 2001, incorporating the Union provisions of the Directive 95/46/EC; cf. Spiros Simitis, *Einleitung: Geschichte – Ziele – Prinzipien*, in: Spiros Simitis (ed.), *Bundesdatenschutzgesetz – Kommentar*, 7th Edition, Baden-Baden 2011, pp. 77 et seqq.
- 93 Cf. § 35 (5) BDSG.
- 94 Oberlandesgericht Hamm, Az.: 6 U 238/99, 19.6.2000, NVwZ 2001, 235-236, decision in German available at: http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/Rechtsprechung/WirtschaftUndFinanzenVerkehr/Artikel/190600_AuskunfteienGeschaetzteDatenKenntlichMachen.html?nn=408918.
- 95 Bundesgerichtshof, VI ZR 196/08, 23.6.2009, decision in German available at: <https://openjur.de/u/31109.html>.
- 96 Based on §§ 823 par. 1, 1004 par. 1 S. 2 BGB analogous in connection with Art. 1, 2 par. 1 GG, resp. §§ 1004 par. 1, 823 par. 2 BGB in connection with § 186 StGB.
- 97 Oberlandesgericht Hamburg, 3 U 67/11, 26.5.2011, decision in German available at: <http://openjur.de/u/167816.html>.
- 98 Oberlandesgericht München, 29 U 1747/11, 29.9.2011, decision in German available at: <http://openjur.de/u/442290.html>.
- 99 Cf. Niko Härting, Bettina Wulff klagt gegen Google - Aus der Einbahnstrasse in die Sackgasse, Legal Tribune Online, 10.9.2012, available at: <http://www.lto.de/recht/hintergruende/h/bettina-wulff-klagt-gegen-google/>.
- 100 Oberlandesgericht Köln, 15 U 199/11, 10.5.2012, decision in German available at: <http://openjur.de/u/462365.html>.
- 101 Bundesgerichtshof, VI ZR 269/12, 14.5.2013, Scientology, decision in German available at: <http://openjur.de/u/627117.html>; the High Court of Cologne subsequently applied the legal reasoning. While the suggestions were deemed to be privacy infringing, the claim for damages was denied. Cf. Oberlandesgericht Köln, Az. 15 U 199/11, 08.04.2014, decision

- in German available at: http://www.justiz.nrw.de/nrwe/olgs/koeln/j2014/15_U_199_11_Urteil_20140408.html.
- 102 Cf. *Alessio Zaccaria/Mirko Faccioli*, The Protection of Personality Rights against Invasions by Mass Media in Italy, in: Helmut Koziol/Alexander Warzilek (eds.), *Tort and Insurance Law Vol. 13 on the Protection of Personality Rights against Invasions by Mass Media*, Vienna 2005, p. 184. They state that “the right to privacy is one of the personality rights that (albeit not expressly governed by law) has been envisaged by legal authors and case law”; *Massimo Farina/Fabrizio Voltan*, La nuova privacy, *Fori* 2011, pp. 6 et seqq.; *Gerolamo Pellicanò/Giovanna Boschetti*, Italy, in: *Monika Kuschewsky/ Van Bael & Bellis*, *Data Protection and Privacy*, London 2012, p. 261.
- 103 Cf. *Christian von Bar/Ulrich Döbng*, *The Interaction of Contract Law and Tort and Property Law in Europe: A Comparative Study*, Munich 2004, pp. 33 et seqq.; cf. also: *Comparative Study on the Situation in 27 Member States as Regards the Law Applicable to Non-contractual Obligations Arising out of Violations of Privacy and Rights Relating to Personality*, Annex III, pp. 87 et seqq., available at: http://ec.europa.eu/justice/civil/files/study_privacy_annexe_3_en.pdf.
- 104 *Guisella Finocchiaro*, *Privacy e protezione dei dati personali – Disciplina e strumenti operative*, Bologna 2012, p. 6.
- 105 Codice in materia di protezione dei dati personali, Decreto legislativo 30 giugno 2003, n. 196. This code replaced the previous Legislative Decree n. 675, 1996; cf. also *Farina/Voltan*, *supra* note 102, pp. 6 et seqq.
- 106 Cf. also Art. 11, (1c) of the Legislative Decree 2003/196.
- 107 Cf. *Elena Bassoli*, Art. 7 – Diritto di accesso ai dati personali ed altri diritti, in: *Giuseppe Cassano/Stefano Fadda* (eds.), *Codice in materia di protezione dei dati personali*, Commento articolo per articolo al testo unico sulla privacy D.legs. 30 giugno 2003, n. 196, Milano 2004, p. 67.
- 108 Cf. *Stefano Farra*, Art. 11 – Regole generali per il trattamento dei dati, in: *Giuseppe Cassano/Stefano Fadda* (eds.), *Codice in materia di protezione dei dati personali*, Commento articolo per articolo al testo unico sulla privacy D.legs. 30 giugno 2003, n. 196, Milano 2004, p. 92 citing *Giulio Napolitano*, Il diritto all’oblio esiste (ma non si dice), in *Dir. inf.*, 1996, pp. 427 et seqq.; cf. also *Giuseppe Cassano*, Il Diritto All’Oblio Nella Era Digitale, in: *Giuseppe Cassano/Guido Scorza/Giuseppe Vacago* (eds.), *Diritto Dell’Internet: Manuale Operativo*, Wolters Kluwer Italia 2013, pp. 45 et seqq.
- 109 Cf. *Stefano Farra*, *supra* note 108, p. 92.
- 110 *Elena Falletti*, L’Evoluzione Del Concetto Di Privacy E Della Sua Tutela Giuridica, in: *Giuseppe Cassano/Guido Scorza/Giuseppe Vacago* (eds.), *Diritto Dell’Internet: Manuale Operativo*, Wolters Kluwer Italia 2013, pp. 22 et seqq.; *Farina/Voltan*, *supra* note 102, pp. 6 et seqq.; cf. also *GianLuca Pedrazzini*, *Privacy*, in *Alberto Clerici* (ed.), *Manuale di Informatica Giuridica*, Milano 2013, pp. 297 et seqq.
- 111 Cf. with respect to rectification the Legislative Decree n. 47, 1948 (“*Legge 8 febbraio 1948, n. 47, Disposizioni sulla stampa*”); cf. also below the rectification right in the data protection act of Italy; cf. *Finocchiaro*, *supra* note 104, pp. 8 et seqq. stating, among others, that the Italian Supreme Court has established a right to be left alone in 1975 and that the right of reputation not only has close ties with the penal norms dealing with defamation but is also interlinked with the civil right of honor.
- 112 Cf. *Finocchiaro*, *supra* note 104, pp. 16 et seqq.
- 113 *Giuseppe Cassano*, *supra* note 108, pp. 45 et seqq.
- 114 Cf. *Finocchiaro*, *supra* note 104, p. 18; cf. also *Cassano*, *supra* note 108, pp. 45 et seqq., stating that the normative fundament of the right of oblivion in data protection law is found today in Art. 11 Legislative Decree 2003/196 (cf. paragraph below); *Falletti*, *supra* note 110, pp. 30 et seqq.
- 115 Cf. *Finocchiaro*, *supra* note 104, pp. 18 et seqq.
- 116 Legislative Decree n. 47, 1948 (*Legge 8 febbraio 1948, n. 47, Disposizioni sulla stampa*).
- 117 Corte di Cassazione, I. Civ., n. 5259, 18.10.1984, http://www.dirittoedellainformazione.it/materiale%20di%20ricerca/sentenza_decalogo.htm.
- 118 Corte di Cassazione, III Civ., n. 5525, 5.4.2012, decision available in Italian at: http://www.ilsole24ore.com/pdf2010/SoleOnLine5/_Oggetti_Correlati/Documenti/Norme%20e%20Tributi/2012/04/corte-cassazione-sentenza-5525-2012.pdf?uuid=11fb990c-7fc2-11e1-a8f6-20908e87732a.
- 119 *Supra* note 107; Translation by *Giusella Finocchiaro*, Italian Supreme Court: the right to oblivion to be protected with newspaper archive updates, April 23, 2012, <http://www.blogstudiolegalefinocchiaro.com/wordpress/2012/04/italian-supreme-court-the-right-to-oblivion-to-be-protected-with-newspaper-archive-updates/>
- 120 Cf. Art. 11 (1c) Legislative Decree 2003/196.
- 121 Cf. Italian Data Protection Authority, Oblivion Rights, <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1336892;Finocchiaro/Ricci>, *supra* note 11, pp. 289 et seqq.
- 122 Robot Meta Tags allow programmers to control how a webpage should be indexed and served to users in the search engine’s results. An explanation for how programmers may use Robot-Meta Tags to control page indexation is provided by Google, February 17, 2012, https://developers.google.com/webmasters/control-crawl-index/docs/robots_meta_tag?hl=de.
- 123 Italian Data Protection Authority, Decision December 11, 2008, Archivi storici on line dei quotidiani: accoglimento dell’opposizione dell’interessato alla reperibilità delle proprie generalità attraverso i motori di ricerca, Doc. 1583162, online: [http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1583162; cf. also *Finocchiaro*, *supra* note 90, p. 21.](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1583162;cf.alsoFinocchiaro)
- 124 Tribunale Ordinario di Milano, 31.3.2011, 10847/2011, *Padova Maria Louisa, Google Inc v. Monanaro Romolo*, <http://www.piana.eu/files/Ordinanza.pdf>.
- 125 Tribunale Ordinario di Milano, 25.3.2013, 68306/2012, http://www.oppic.it/index.php?option=com_docman&task=doc_details&gid=490&Itemid=60.
- 126 This decision is in line with similar cases handled in other jurisdictions to which the Court expressly referred; among others, the Swiss Jura Cantonal Court, 12.02.2011 available in French at http://www.jura.ch/Htdocs/Files/v/11625.pdf/Justice/1_Instances_judiciaires/2_TC/Documents/pdf/CC2010117.pdf?download=1; cf. *Marco Bellezza/Federica De Santis*, Google not liable for Autocomplete and Related Searches results, Italian court rules, EU Regulatory, April 5, 2013, <http://www.portolano.it/wp-content/uploads/2013/04/Google-not-liable-for-Autocomplete-and-Related-Searches-results-Italian-court-rules-Rapid-TV-News.pdf>.
- 127 Cf. Is the EU compelling Google to become about me?, *Jonathan Zittrain*, available at: <http://blogs.law.harvard.edu/futureoftheinternet/2014/05/13/is-the-eu-compelling-google-to-become-about-me/>.
- 128 *Jonathan Zittrain*, Don’t Force Google to Forget, available at: [http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0; Spain’s everyday internet warrior who cut free from Google’s tentacles, The Guardian, May 13, 2014 available at: <http://www.theguardian.com/technology/2014/may/13/spain-everyman-google-mario-costeja-gonzalez>.](http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0;Spain’s everyday internet warrior who cut free from Google’s tentacles, The Guardian, May 13, 2014 available at: http://www.theguardian.com/technology/2014/may/13/spain-everyman-google-mario-costeja-gonzalez)

The Implementation of the Audiovisual Media Services Directive by National Regulatory Authorities

National Responses to Regulatory Challenges

by **Jenny Metzdorf**,* PhD student at the Faculty of Law, Economics and Finance of the University of Luxembourg

Abstract: The Audiovisual Media Services Directive (AVMSD) which regulates broadcasting and on-demand audiovisual media services is at the nexus of current discussions about the convergence of media. The Green Paper of the Commission of April 2013 reflects the struggle of the European Union to come to terms with the phenomenon of convergence and highlights current legal uncertainties. The (theoretical) quest for an appropriate and future-oriented regulatory framework at the European level may be contrasted to the practice of national regulatory authorities. When faced with new media services and new business models, national regulators will inevitably have to make decisions and choices that take into account providers' interests to offer their services as well as viewers' interests

to receive information. This balancing act performed by national regulators may tip towards the former or latter depending on the national legal framework; social, political and economic considerations; as well as cultural perceptions. This paper thus examines how certain rules contained in the AVMSD are applied by national regulators. It focuses first on the definition of an on-demand audiovisual media service and its scope. Second, it analyses the measures adopted with a view to protection minors in on-demand services and third discusses national approaches towards the promotion of European works in on-demand services. It aims at underlining the significance of national regulatory authorities and the guidelines these adopt to clarify the rules of a key EU Directive of the "media law acquis".

Keywords: Audiovisual Media Services Directive, VOD Services, VOCCCD services

© 2014 Jenny Metzdorf

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: **Jenny Metzdorf**, The Implementation of the Audiovisual Media Services Directive by National Regulatory Authorities National Responses to Regulatory Challenges, 5 (2014) JIPITEC 88, para. 1.

A. Introduction

1 The Audiovisual Media Services Directive (AVMSD) has been the subject of an enormous body of research. As the key legal document defining the various pillars upon which the cross-border provision of audiovisual media services is built in the European Union (EU), its rules and approach have been investigated in-depth. When the Directive was initially adopted in 1989, it regulated certain aspects

of broadcasting envisioning a market of "television without frontiers".¹ In 2007, the Directive's scope was extended to on-demand audiovisual media (VOD) services.² It henceforth distinguished between linear (television broadcasting) and non-linear (VOD) services applying different sets of rules to each. The break-through which was expected of the Directive in light of convergence of media, however, has not been accomplished. Shortly after its adoption,

discussions rekindled as to its modification in view of the emergence of Connected TV which seamlessly weaves the Internet and broadcasting together on the television screen.³ So far, the Commission has clung to the AVMSD and its graduated approach to regulation as the market potential of Connected TV and similar services is gradually unfolding. The Commission's Green Paper of April 2013 which indeed asks crucial questions in fact reveals a high level of uncertainty with regards to the current rules and future approach to Connected TV and other hybrid services.⁴

- 2 In this state of flux, national regulatory authorities (NRAs) assume a pivotal role. Charged with the regulation of audiovisual media services, they ensure the application and implementation of the AVMSD on a daily basis. While their structure, composition and mandate are contingent on national legal frameworks, they generally act as intermediaries between the state and the industry. Where the national media laws transpose the Directive verbatim, the position of NRAs is enhanced. This is particularly true for rules couched in vague and general terms which have to be interpreted and applied in specific contexts and under specific circumstances at national level. NRAs thus enjoy a certain margin of discretion which is constrained mostly by the scope of the mandate granted by the state and the freedoms associated with the former. The establishment by the Commission of a European Regulators Group for Audiovisual Media Services in February 2014 demonstrates increasing awareness of the significance of NRAs and their contribution in shaping the future regulatory landscape.⁵ The Regulators Group constitutes, inter alia, a forum for "exchange of experience and good practice".⁶ This paper starts from similar premises employing a bottom up lens by examining the guidelines and codes adopted by NRAs as well as their practice.
- 3 To this effect, this paper sketches the most pressing challenges NRAs are currently facing in implementing the AVMSD at the grassroots. In its first section, it examines the criteria defining an (on-demand) audiovisual media service in order to determine the regulatory remit of NRAs. Interpretation and specification of the criteria is of enormous practical effect as it will identify the set of rules (and possibly laws) applicable to relevant providers. Secondly, this paper explores the measures taken by NRAs to protect minors from unsuitable content contained in non-linear services and thirdly, it details the activities of NRAs in respect of the promotion of European works in such services. Sections two and three illustrate the graduated approach to regulation which regulates television broadcasting more intensively than on-demand services. Succinctly, this paper endeavors to contribute to the debate about future regulatory responses to an ever more convergent media

environment and a possible revision of the AVMSD by pinpointing its most apparent deficiencies.

B. Criteria for VOD services

I. The definitions outlined in the AVMSD

- 4 Although a comprehensive (horizontal)⁷ reform of the TwFD in light of growing convergence of media was rejected in 2007 in favour of the maintenance of sector-specific regulation, the Directive's scope of application was slightly extended to cover television and "television-like"⁸ services subsumed under the term "audiovisual media service".⁹ In line with Art. 1 (1) (a) (i) AVMSD, an audiovisual media service is defined as:

"a service as defined by Articles 56 and 57 of the [TFEU] which is under the editorial responsibility¹⁰ of a media service provider and the principal purpose of which is the provision of programmes, in order to inform, entertain or educate, to the general public by electronic communications networks".¹¹

- 5 Thus, audiovisual media services are further classified as television broadcasting (linear services), on-demand audiovisual media services (non-linear services) as defined in Art. 1 (1) (e) and (g) AVMSD respectively and audiovisual commercial communication as stipulated by Art. 1 (1) (a) (ii) in conjunction with Art. 1 (1) (h) AVMSD. While a VOD service may be viewed at the "moment chosen by the user and at his individual request"¹², broadcasts are transmitted simultaneously to the general public "on the basis of a [chronological] programme schedule"¹³. The differentiation between linear and non-linear services is crucial for the application of the graduated approach to regulation.¹⁴ Accordingly, VOD services are regulated more lightly whereas a tighter regime applies to television broadcasting. On top of the complexities of distinguishing linear from non-linear services, further difficulties emerge when delineating audiovisual media services from other kinds of services exempted from regulation, the boundaries of which are continually blurring.¹⁵ The preamble to the Directive clarifies that it does not apply to "any form of private correspondence", "games of chance (...), other forms of gambling (...) and search engines".¹⁶ It also exempts user generated content which is shared or exchanged "within communities of interest".¹⁷ Where "text-based services" (merely) accompany an audiovisual service, the Directive applies.¹⁸ However, recital 28 AVMSD indicates that "the scope of this Directive should not cover electronic versions of newspapers and magazines". Although the preamble to the AVMSD is, in principle, non-binding, it nevertheless serves as a valuable point of reference, particularly

for NRAs when implementing and applying the AVMSD “on the ground”.¹⁹

- 6 In several countries, recital 28 AVMSD has moved into the limelight of regulatory activities concerning VOD services.²⁰ The printed press increasingly offers its services online in order to meet competition from news blogs or other websites providing text-based material. The websites of newspapers or other magazines increasingly contain videos as a popular extra in addition to written articles which are their primary business. The pertinent question arising from this phenomenon is at what point a service offering mixed types of content should be subjected to the regulation applicable to VOD services. The question hinges on the criterion of principal purpose as prescribed by Art. 1 (1) (a) AVMSD. The regulators of Austria, Denmark, the Flemish Community of Belgium²¹, Slovakia²² and Sweden²³ have found that parts of websites of electronic versions of newspapers served the required purpose and were thus classified as stand-alone VOD services.²⁴ By contrast, websites of several British newspapers have been excluded as VOD services, although being the subject of intensive investigations by the competent regulatory agencies. Thus, the following section analyses in detail the decisions of the Austrian and British regulatory bodies in order to shed light on their assessment and motives.

II. Video section of online newspaper classified as VOD service in Austria

- 7 In September 2012, the Austrian regulator, the *Kommunikationsbehörde Austria* (KommAustria) qualified the video section of the regional newspaper “*Tiroler Tageszeitung*” (TT service) as an on-demand service, a determination which was upheld in December 2012 by the Austrian *Bundeskommunikationssenat* (Federal Communications Senate, BKS) which was the appeal instance for decisions issued by KommAustria at that time²⁵.²⁶ The website at issue (<http://www.tt.com>) contained the online version of the newspaper and its homepage brought the user to the news section by default. The content was arranged in sub-sections such as “Sports”, “Leisure”, “Video” or “Service” which were accessible via the main menu. In all categories, individual written items were accompanied by videos which served to complement the former. The video section was designed and branded in the same way as the website and also contained the same navigation tools. The videos were catalogued in chronological order and a separate section underneath presented the most popular videos. The whole catalogue was available via certain “categories”. The videos constituted editorial content, professionally made and typically lasted between 30 seconds and several

minutes. Except for the title of the videos and a brief description of the most recent video, all material provided was audiovisual in character.

- 8 In its determination, KommAustria examined the cumulative criteria defining an audiovisual media service as stipulated by Sec. 2 No. 3 *Audiovisuelle Mediendienste-Gesetz* (AMD-G) which transposes Art. 1 (1) (a) AVMSD employing similar wording. More concretely, KommAustria enquired whether the service, if covered by the AMD-G, constituted an on-demand audiovisual media service in line with Sec. 2 No. 4 AMD-G which emulates Art. 1 (1) (g) AVMSD. If this were to be affirmed, the service provider would have been required to notify the service pursuant to Sec. 9 (1) AMD-G. The case centered around two criteria. First, KommAustria posited that the videos constituted programmes within the meaning of Sec. 2 No. 30 AMD-G which reflects Art. 1 (1) (b) AVMSD. It points out that the notion of programmes was not based on a minimum length.²⁷ Rather than prescribing a quantitative requirement, KommAustria referred to the comparability to the form and content of the contested service with such programmes ordinarily shown on TV. In line with recital 24 AVMSD, KommAustria argued that the videos featured on the TT service constituted self-contained items which targeted the same audience as television broadcasts and offered comparable content in comparable form.²⁸ Second, KommAustria investigated in the principal purpose of the video section. It found that this sub-section could be separated from the remainder of the service as it fulfilled an independent function and was not merely accessory to the text-based materials.²⁹ Hence, the video section was considered a user destination in its own right and was regarded by KommAustria as a stand-alone service. Interestingly, KommAustria responded to the provider’s submission that it primarily provided written content that a service provider could not evade the application of the AMD-G simply for that reason. Even if an insignificant part (in terms of quantity) of the overall offer encompassed audiovisual content, such could nonetheless be viewed as a separate audiovisual media service within the meaning of the AMD-G.³⁰ It was not decisive whether the audiovisual content was grouped in a sub-section of the website even if the domain used could be indicative of the independence of the service.³¹ In the appeal instance, the BKS confirmed the assessment undertaken by KommAustria in entirety. With regards to the comparability of the videos with programmes broadcast on TV, it emphasized that the videos covered concrete subject matters.³² Furthermore, the BKS qualified KommAustria’s position with respect to the principal purpose test. It stressed that the overall appearance of a service should be taken into account albeit excluding other services offered by the same provider.³³ In case of TT service, the video section did not, however, merely constitute a “side

effect”³⁴ but rather encompassed almost exclusively audiovisual content which was not of secondary or supplementary nature to the written content. The video section could thus have been consumed, used and offered independently of it being embedded in the TT service.³⁵ In sum, the Austrian regulatory bodies have asserted their authority over providers of websites of electronic versions of newspapers by classifying a sub-section of the entire offer as a non-linear service. They have thereby detailed two important criteria defining an audiovisual media service. Importantly, the case of TT service has reached the Court of Justice of the European Union (CJEU) which is asked to pronounce on two preliminary questions referred by the Austrian *Verwaltungsgerichtshof* (Administrative Court).³⁶ The questions concern firstly, the comparability with programmes broadcast on TV and secondly, whether a part of a service pertaining to an online newspaper can be insulated for the purposes of the AVMSD.³⁷

III. Detailed guidance on principal purpose by British regulator

- 9 Like the Austrian regulator, the British co-regulator³⁸, the Authority for Television On Demand (ATVOD)³⁹ has struggled with the legal evaluation of electronic versions of newspapers. In a series of cases which at first glance seem similar to the Austrian case discussed above, it determined that the video sections of several online versions of newspapers constituted on-demand services within the meaning of Sec. 368A Communications Act 2003 (CA 2003)⁴⁰ holding that the relevant providers had failed to notify their services.⁴¹ The first case decided on appeal by the Office for Communications (Ofcom) was “Sun Video”⁴² which constituted a landmark decision in which Ofcom gave detailed guidance on the interpretation of the principal purpose test^{43,44} Ofcom outlined eight (non-exhaustive and non-cumulative) characteristics from which it could be inferred that the principal purpose was indeed the provision of programmes within the meaning of Sec. 368A (1) (a) CA 2003. It was thus characteristic of an on-demand service to be provided on “its own homepage through which it is accessed” or on a sub-section where the audiovisual material is catalogued.⁴⁵ Furthermore, a service was considered of having the required purpose where the audiovisual content was “presented or styled (and marketed) as a television channel” or where there existed only a “limited number of access [or content] links between the relevant audiovisual material and other content”.⁴⁶ In addition, Ofcom suggested that the principal purpose implied that the audiovisual material was “of substantial duration and/or comprise[d] complete programmes rather than “bite-sized” clips or extracts from longer programmes” which could be “watched and understood fully on [their] own”.⁴⁷ Where a service comprises both audiovisual and written material, Ofcom suggested that the principal purpose test would be satisfied where “the balance of the material is more likely significantly to lean towards the audio visual” implying that the text-based part of the website is “brief and/or merely an introduction to, or summary of, the audio visual material” and is not the “primary means” of conveying information to the user.⁴⁸ Ofcom concluded on the basis of these characteristics that the video section of the website of the Sun did not constitute a non-linear service.⁴⁹ It criticized ATVOD for having focused on the video section while according insufficient attention to the “website as a whole”.⁵⁰ Still, Ofcom did not refuse the application of the rules concerning non-linear services to electronic versions of newspapers *per se*.⁵¹ An interesting case which could cross this threshold is currently pending before Ofcom. In a determination of August 2013, ATVOD considered that the video section of the Vice website (http://www.vice.com/en_uk) was a VOD service.⁵² The portal is comparable to an online version of a magazine. Its video section features the latest videos which are accompanied by an explanatory note as well as shows of over ten minutes in length. The website is also made available on YouTube where it appears to correspond largely to the video section. In contrast to its precedents, the case of Vice appears, to put it bluntly, ‘much more audiovisual’. Still, it remains to be seen whether Ofcom which so far has rejected all attempts of ATVOD to regulate sections of websites will follow ATVOD’s assessment.
- 10 When examined together, the practices of the Austrian and British regulatory bodies paint two opposing pictures regarding the classification of online newspapers as VOD services. Still, the reasons for the decisions and arguments brought forth by regulators are, to a certain extent, similar like the question whether the service constituted a stand-alone service and the rejection of the application of a purely quantitative approach to determining the primary character of a service. Nonetheless, certain differences can be identified with respect to the comparability of videos to programmes diffused on TV. While videos of relatively brief duration (maximum of several minutes) were considered TV-like in Austria, it appears as if such short videos would (taken by themselves) not be conclusive of a VOD service in the UK. Knowledge about such subtle but existing differences in practice of NRAs is crucial for service providers. Editors of newspapers who wish to make their offers available online will have to be aware of the consequences of the design and structure of their services. They will have to reckon with the potential involvement of the regulatory authorities for the media even if their activities would formally fall under press regulation.⁵³

- 11 If editor's chief objective is to provide an online version of their printed medium, they will have to devise their websites accordingly by making sure that video content is not excessive and truly embedded in text-based material. If they plan to group the audiovisual material in a separate video section, they will have to carefully consider whether notification of a VOD is necessary. The Austrian case currently pending before the CJEU might offer further indications in this respect. Regardless of the outcome of this case, should the application of the AVMSD or respectively the relevant national law be affirmed, operators will be obliged to abide by certain standards such as the prohibition of programmes containing incitement to hatred or the safeguarding of the protection of minors, a subject discussed below.

C. Protection of minors in VOD services

I. The standard according to the AVMSD

- 12 The protection of minors from unsuitable (e.g. offensive or sexually explicit) audiovisual content has been a constant policy concern which has been reflected in the Directive since its initial adoption in 1989. Art. 22 TwFD (now 27 AVMSD) was amended in 1997 and subsequently required broadcasters to identify programmes which were susceptible to having a damaging effect on children and adolescents and which were broadcast in unencoded form on free TV.⁵⁴ The extension of the scope of application of the Directive in 2007 was accompanied by the inclusion of a rule purporting to protect minors in on-demand audiovisual media services. Although Art. 12 AVMSD borrows from the wording of the provision protecting minors in broadcasts, the former is less restrictive than the latter illustrating the graduated approach to regulation. Thus, Art. 12 AVMSD prescribes that on-demand services which "might seriously impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see [them]". It follows that service providers are obliged to put in place the (technical) measures whereby access to seriously harmful material is denied to minors (typically under-18's, albeit depending on national context). In line with recital 60 AVMSD read in conjunction with the Recommendation of 2006 of the European Parliament and the Council⁵⁵, "personal identification numbers (PIN codes), filtering systems or labeling" could be employed to this effect. Art. 12 AVMSD lacks any indication as to the type of material covered by the rule. The vague formula of material which "might seriously impair" minors is nonetheless specified in Art. 27 AVMSD (applicable to television broadcasts) which could be consulted by analogy. Accordingly, programmes "that [among other] involve pornography or gratuitous violence" meet this test. In the absence of any clear correlation between Art. 12 and 27 (1) AVMSD, Member States remain entirely free to define the kind of content which is qualified as seriously detrimental to children.⁵⁶ The following section is devoted to the guidance and practice by the British regulatory bodies which seem to have assumed a pioneering role within the EU clamouring for the strengthening of the protection of minors on the Internet.

II. Application of the standard in the United Kingdom

- 13 In the United Kingdom, Art. 12 AVMSD is transposed by Sec. 368E (2) CA 2003. Sec. 368E (2) CA 2003 which reproduces *grosso modo* the text of the Directive but is more detailed by specifying the exact age (eighteen years) of persons addressed by the rule. Since the formulation contained in the national act transposing the Directive is equally imprecise, it falls to the NRAs to interpret its exact scale and scope. ATVOD as the competent co-regulator monitors the application and implementation of the statutory rules. In order to help the industry to conform to the requirements imposed on service providers, ATVOD has accumulated in its guidance the statutory rules which are supplemented by (non-binding) guidance on their meaning and enforcement.⁵⁷ Rule 11 sets out ATVOD's approach to the protection of minors. It highlights that ATVOD has pursued a precautionary approach which is backed by Government and Ofcom.⁵⁸ In spite of the lack of any conclusive evidence about the harm caused to minors by programmes containing sexually explicit material, ATVOD is satisfied that there is a sufficiently strong correlation justifying precautionary measures.⁵⁹ It follows that ATVOD has established a threshold of material it considers harmful.⁶⁰ This threshold is fixed by reference to the classification scheme of the British Board of Film Classification (BBFC), in particular its R18 category. The distribution of such works is restricted to "specifically licensed cinemas (...) and sex shops".⁶¹ According to ATVOD's Rule 11, this includes inter alia "highly sexualized portrayals of children", "pornographic content which is likely to encourage an interest in sexually abusive activity" (e.g. paedophilia, incest or non-consensual sex) or "involves an act which may cause lasting physical harm". In addition, any depiction of "sexual violence", "sadistic violence or torture" and "real injury, violence or death presented with insufficient contextual justification" is prone to being classified as harmful material.⁶² Briefly, the type of material covered by Rule 11 is summarized

bluntly as “hardcore pornography”.⁶³ Since such content is not completely banned, providers of non-linear services are obliged to limit access to persons of age. In this respect, ATVOD requires that an “effective Content Access Control System (“CAC System”)” is installed “which verifies that the user is aged 18 or over at the point of registration or access” of the service.⁶⁴ In practice, unsuitable content is concealed behind a “pay wall” which can be passed by payment methods which are restricted to persons of age (such as payment by credit card).⁶⁵ ATVOD considers permissible similar means which corroborate age on the basis of “an independent and reliable database, such as the electoral roll”.⁶⁶

14 Throughout the past years, ATVOD has proven a robust regulator by rigorously enforcing Rule 11. In fact, it seems to have prioritized the protection of minors in on-demand services, a subject which is repeatedly discussed in its policy documents.⁶⁷ The number of violations detected by ATVOD between 2012 and 2014 underlines this impression. Between 2012 and 2014, it has found 30 UK providers in violation of Rule 11 and thus Sec. 368E (2) CA 2003.⁶⁸ The effect of its determinations is declaratory. ATVOD may, in cases of grave and repeated infringements refer the matter to Ofcom for imposition of sanctions pursuant to Sec. 368I CA 2003.⁶⁹ In January 2013, Ofcom imposed a total fine of £100.000 on the service provider Playboy TV UK/Benelux Limited for two of its services.⁷⁰ ATVOD had previously determined that its services “Demand Adult” and “Playboy TV.co.uk” violated Rule 11 by failing to install an effective CAC system.⁷¹ The two websites displayed a warning about the offensive character of the content offered next to two links reading “Enter. I am over 18” and “Exit if you are under 18”. Following the links brought the user to the respective homepages. The “Demand Adult” website even contained free access to stills of pornographic nature while access to the full video catalogues of both services was opened only upon payment (either pay per view or full subscription). The payment services (“Pay Wizard” and “CCBill.com”) allowed for debit card payment and transfers via regular bank accounts and thus could be used by underage persons. Hence, ATVOD concluded that the measures designed to restrict access to under-18’s could be “easily penetrated by minors and therefore could not be regarded as being effective in securing that such persons will not normally see or hear the relevant material”.⁷² Ofcom, in its decision, sanctioned the provider for failing to take corrective action (after being made aware of its negligence by ATVOD) during a prolonged period of roughly seven weeks.⁷³ The service provider had instead informed ATVOD of its “intention to remove the service from UK jurisdiction”.⁷⁴

15 The question of whether the service provider was established in the UK for the purpose of Sec. 368A in conjunction with Sec. 368R (5) CA 2003 (and

implicitly the AVMSD) was treated separately. While ATVOD regarded Playboy TV UK/Benelux Limited to control editorial decisions (in other words, to have “editorial responsibility”, one of the cumulative criterion defining an audiovisual media service)⁷⁵, Ofcom, by contrast, consented that the provider had relocated to Montreal, Canada and therefore was no longer (as at September 2012) subject to UK jurisdiction as a “genuine reorganisation [had occurred] including redundancies in the UK and the taking on of responsibilities by staff in Montreal”.⁷⁶ Although Ofcom ruled on the matter, ATVOD remains discernibly distrustful of providers establishing abroad (outside the EU) in order to evade stricter legal requirements applicable in the UK (in the EU). Such “tube sites” offer free hardcore pornographic material as honey pots (or “shop window”)⁷⁷ in order to attract user’s attention which is subsequently redirected to complementary paid services necessitating subscription. Interestingly, such websites are very popular with British users⁷⁸ but they have been anathema to ATVOD which does not have jurisdiction over them for their lack of establishment in the UK.

III. Further initiatives by the British co-regulator

16 Against this backdrop, ATVOD published a research report which found evidence of “significant underage access from the UK to adult websites”.⁷⁹ For this reason, it recommended that first, the CA 2003 be amended to specify that material rated R18 would be characterized as impairing minors, second, the AVMSD be modified accordingly to establish a uniform standard across the Union and third, further legislation be devised to allow the UK payments industry to prevent cash flows from the UK to tube sites making available pornographic content to minors.⁸⁰ ATVOD’s suggestions, while proactive and innovative, also raise a number of concerns regardless of the validity of the underlying objective of the protection of minors. Any specification of the type of content which is considered seriously harmful to children would have to rely on solid and more profound scientific evidence than the statistics included in ATVOD’s report.⁸¹ The metaphor of a “slippery slope”⁸² could also be conjured up in this respect whereby the explicit prohibition of hardcore pornographic content is viewed as a first step leading to the banning of less extreme forms of sexually explicit material in the future. Such a development would seriously impact on the fundamental right of the freedom of expression. In a similar vein, a modification of Art. 12 AVMSD as desired by ATVOD seems doomed to failure in view of considerable discrepancies in cultural and social perceptions among Member States which are reflected in the different national classification systems and rating

schemes concerning programmes broadcast on TV. In addition, any amendment referring to “hardcore pornography” (or the like) would still be contingent upon interpretation by NRAs and ultimately national (or the European) judiciaries.

- 17 Furthermore, ATVOD’s lobbying for new legislation to attack the business model of “tube sites” by cutting off monetary flows from the UK seems disputable as it would implicitly extend ATVOD’s reach beyond UK borders. In fact, ATVOD would pass on the task of regulating the protection of minors to the private sector, in particular to commercial actors like Visa, MasterCard or PayPal. For the purpose of the prevention of payments, it is unclear whether providers of such systems would have to enquire about the nature of the content delivered to the user as they typically only process the financial transaction lacking knowledge about the actual product or service purchased. It is furthermore unclear at what point of the transaction access to the (pornographic) service would be blocked, at the time of the request for payment (when it is verified that the credit card holder has sufficient credit to purchase a product or service) or at the time of the actual payment (when the total amount owed is deducted from the account). Moreover, it is unclear whether any UK citizen would be denied access to such websites, even those of age, despite the material being legal (albeit rated as R18). Whether legislation will eventually be adopted in the UK and to what extent will have to be critically observed. The protection of minors as an indispensable public interest concern would nonetheless have to be balanced with fundamental rights, above all, the freedom of expression (entailing the right to receive pornographic information) as well as the right to privacy. In brief, ATVOD’s practice and policy documents discussed above underline its active role in promoting the protection of minors in on-demand services. In interpreting the (broadly formulated) statutory rules, it has developed a standard through its practice which seems sufficiently detailed for service providers to foresee prosecution by ATVOD. It has thereby strengthened its own position and standing in the industry. Still, the transformation of its standards into binding legislation would have to be accompanied by an increase in transparency of the underlying motives and objectives pursued as well as an analysis of the necessity and proportionality of the measures in order to minimize interference with the interests of stakeholders, in particular fundamental rights. The example chosen above is exemplary of many NRAs struggle to adapt national media legislation to the realities of the ubiquity of the Internet⁸³ where long-established standards (like the protection of minors) for traditional modes of transmission have come under pressure.⁸⁴

D. Promotion of European works in VOCCCD services

I. The standard set out in the AVMSD

- 18 As with the protection of minors, the promotion of the production and distribution of European works on television has been a policy concern which was integrated in the original TWFD of 1989. It required that broadcasters dedicate a certain share of their programmes to European works and support the programmes of independent producers by financial or editorial means.⁸⁵ Unlike the protection of minors, an objective seemingly approved of by all Member States, the aims and in particular the means whereby the cultural objectives of plurality and diversity of content have been advanced under the Directive have polarized countries. Not only is the definition of European works⁸⁶ broad and prone to favouring national language films or those produced nationally rather than stimulating the cross-border circulation of multi-national works⁸⁷, the wording of the Directive is ambivalent and rather soft.⁸⁸ When its scope of application was extended, the imprecise language of the provisions applicable to broadcasting (Art. 16 and 17 AVMSD) was replicated in the provision concerning VOD services (Art. 13 AVMSD). Thus, Art. 13 (1) AVMSD encourages providers of on-demand services to “promote, where practicable and by appropriate means, the production of and access to European works”. The phrase “where practicable and by appropriate means” stems from the quota rules for broadcasting and expresses a “political compromise”.⁸⁹ In order to gain a majority for the inclusion of the dispositions in the Directive, they were formulated in such a way as to give service providers, especially smaller and less solvent providers some leeway with regards to their fulfilment.
- 19 Furthermore, Art. 13 (1) AVMSD indicates that promotion may refer to “the financial contribution made [...] to the production and rights acquisition of European works or to the share and/or prominence of European works in the catalogue of programmes”. Recital 69 AVMSD is only marginally more specific by pointing to the “attractive presentation of European works in electronic programme guides” as a form of support envisaged by Art. 13 AVMSD. Still, the rationale of the TWFD and its television quotas was extended to the online environment. This has been criticized as the user bears ultimate control over the content consumed and selects the programmes which cater to his or her tastes (regardless of the fact that a catalogue comprises a majority of European works).⁹⁰

20 Not surprisingly, the Commission found in its first report on the application of Articles 13, 16 and 17 AVMSD of September 2012 that in spite of the success of the well-established quotas the proportions of which has been outdone in many Member States, the transposition and above all enforcement of Art. 13 AVMSD in national legal orders have been restrained and are more problematic.⁹¹ The Commission also noted fundamental discrepancies in conditions and developments of the market for VOD services⁹². Policy makers and national regulators appear hesitant, pursuing a “wait and see”⁹³ approach in order not to stifle innovation of a nascent industry and allow providers to build attractive online offers appealing to large parts of the public. Still, some countries which have traditionally hoisted the “quota flag” for TV have fervently advocated for efficient enforcement of comparable rules for non-linear services. While a conventional approach is applied in France⁹⁴, an innovative solution focusing on enhancing “prominence” has been sought by the regulatory body of the French Community of Belgium.⁹⁵ In addition, the Dutch approach to monitoring shall serve as an example underlining the pragmatism necessary for the enforcement of this provision.

II. Quota rule for VOD services in France

21 Art. 13 AVMSD is transposed by Art. 12 of the French *Décret relatif aux services de médias audiovisuels à la demande* (VOD Decree 2010)⁹⁶ which stipulates that providers reserve 60 percent for European works and 40 percent for French works from the total number of programmes included in the catalogue.⁹⁷ Interestingly, French works are considered European works for the purpose of the quotas. If one were to deduct the support for French works (assuming that all providers meet the target for French works and do not go beyond the threshold set for European works) from the overall goals, the support for European works appears rather insignificant or at least weak in comparison to the protection afforded to the national film industry. Yet, the definition of European works set out in Art. 1 (1) (n) AVMSD does not require a cross-border element (like co-productions) but is deliberately open to accommodate national productions *stricto sensu*. Above all, Art. 13 VOD Decree 2010 specifies that service providers are to permanently present a substantial proportion of the quota on their homepage. To this effect, the Decree explicitly indicates that the mentioning of the title of the work on the home page is not sufficient. Instead, providers are expected to advertise the relevant works (by banner ads, for example) and display trailers or samples. This rule aims at preventing the burying of European and French works in sub-sections of the

website by enhancing their visibility on the primary destination of users, providers’ homepages.

22 In its report about the application of the Decree published in November 2013 drafted on the basis of consultations of stakeholders, the French regulatory authority, the *Conseil Supérieur de l’Audiovisuel* (CSA, hereinafter French CSA) identified difficulties providers encountered in the practical application of the quota rules. The responses by the French CSA are worthwhile with a view to the immediate application and enforcement of the rules in practice as well as potential amendments to the legislative framework.⁹⁸ Thus, the French CSA clarified that the quota applied on an annual basis allowing providers to derogate (even if minimally) from the strict proportions and front page presentations.⁹⁹ Above all, the French CSA acknowledged the restrictiveness of Art. 13 VOD Decree exclusively focusing on the homepage of providers which, in fact, constitutes only one access point for users. Hence, it proposed the recognition of separate sections or buttons dedicated to European and French works, search tools by origin of productions and promotional activities of providers.¹⁰⁰ The Commission, in its staff working document accompanying the report on the application of Art. 13, 16 and 17 AVMSD also referred to these criteria when enumerating “performance indicators” which Member States could take into account when interpreting and specifying the obligations for providers pursuant to Art. 13 AVMSD.¹⁰¹ Interestingly, the French CSA highlighted the increasing significance of recommendation tools. On the basis of personal data, an algorithm is programmed which recommends audiovisual productions to individual users according to their personal preferences and interests and/or previous behaviour and consumption patterns. The French CSA thus advocated their use for the purpose of promoting European and French works in case of websites offering the possibility to personalize the homepage.¹⁰² Yet, French providers seemed little enthused about the integration of a ‘European or French factor’ into their algorithms arguing that the biasing of the algorithm/software would infringe on their editorial freedom and the neutrality of the recommendation tool.¹⁰³ Such instruments also raise more general questions about the collection of personal data and their use and any tracking of user behaviour should be made transparent (by asking the user to consent). The fact that the French CSA proposed to restrain the ‘European and French recommendation tools’ to personalized homepages (and negated them for standardized homepages) which are in any case based on user’s data (voluntarily or so it is assumed) given to the provider, does not solve the data protection issue. Finally, the French CSA rejected the introduction of exemptions for “non-generalist” services.¹⁰⁴ Arguing that a general exception would undermine the quota scheme, the French CSA nonetheless conceded that a VOD could

target only a segment of the public and could cater specifically to that segment. It agreed to propose a relaxation of the quota obligations in compensation for provider's commitment to offer additional services to the European and French works diffused such as the sub-titling or funding for the promotion and their production or the participation in events and shows.¹⁰⁵ Such derogations would presumably have to be negotiated on case-by-case basis. The French CSA's outright refusal to recommend to the French government the formulation of an exception clause to Art. 12 VOD Decree demonstrates the high value the quota rules have had in France and the regulator, as the guardian of the rules, is unwilling to sacrifice them in view of less generalist service providers. This picture is confirmed when globally assessing the legislative and executive framework in France. The VOD Decree has extended the well-established scheme for broadcasting to VOD services. Some reflections about the nature of non-linear services are nonetheless expressed in Art. 13 VOD Decree which are, however, limited to the homepages of providers. In order to guarantee the application of the rules in practice, the French regulator made some compromises in its report allowing for other ways and "places" (like sub-pages) to promote European and French works and exceptions to the quota obligations to be negotiated on individual basis.

III. Prominence as the decisive criterion in the French Community of Belgium

23 In contrast to the rather rigid legal order in France, the regulatory authority of the French Community of Belgium, the *Conseil Supérieur de l'Audiovisuel* (CSA, hereinafter Belgian CSA)¹⁰⁶ has actively shaped the interpretation of the disposition contained in the *Decret coordonné sur les Services de Médias Audiovisuels* (hereinafter AVMS Decree) allowing for a flexible and innovative approach. In the French Community, Art. 13 AVMSD is transposed by Art. 46 AVMS Decree. Art. 46 AVMS Decree is more specific than the Directive by indicating that the list of European and Belgian (produced in the French Community of Belgium) works included in the catalogues should be attractively presented. The French Community thus used the leeway accorded by the Directive selecting "prominence" as the primary means of promotion while refraining from establishing a quota scheme or soliciting investments from VOD providers. The proposal of the AVMS Decree of January 2009 strongly criticized the transfer of the quota regime from linear to non-linear services for its devastating effect on the development of new services and innovative business models.¹⁰⁷ Instead, it advocated for all kinds of promotional techniques including advertisements

screened on provider's homepages or during TV commercials, the creation of special categories and the reference to such works in magazines, feature articles or communications send to its users.¹⁰⁸ Against this background, the Belgian CSA published a recommendation in June 2010 on the interpretation of Art. 46 AVMS Decree going beyond what was provided in the preparatory documents of the AVMS Decree.¹⁰⁹ Hence, the regulator emphasized that the provider can influence the conditions of access to European and Belgian works by the interface of the website. Thus, access by buttons entitled "European films" or "films of the French Community" facilitates according to the Belgian CSA the visibility of such works. In this respect, the regulator pointed out that the works should be included in multiple categories to allow users to find them coincidentally and avoid collating such programmes in one place of the website.¹¹⁰ Thus, a substantial amount of these works should be presented in categories like "new releases", "last chance", "great classics" or "favourites" which frequently guide users through the vast amount of content available.¹¹¹ In addition, the Belgian CSA proposed to include the works in categories for which discounts were offered as long as the films were not devalued.¹¹² With respect to provider's advertising activities, the Belgian CSA suggested to refer to European or Belgian works, events, production teams or actors in all commercial communications available including magazines, special editions or channels or programmes devoted to self-promotion.¹¹³

24 These guidelines¹¹⁴ are very detailed and set out precise requirements for providers. The structuring of the catalogue in parallel to other promotional activities advocated by the CSA in its recommendation appear reasonable for their low level of intrusiveness with provider's editorial freedom.¹¹⁵ In addition, the costs of promotion remain bearable even if such measures are not entirely gratuitous as providers might find themselves investing in advertising spots for European works which they would otherwise not have promoted. In similar vein, the promotion of European or Belgian works "is not detrimental to viewer numbers"¹¹⁶ but instead enhances the attractiveness of the overall offer. Since catalogues may comprise an infinite number of programmes (figuratively speaking), providers do not have to make any trade-offs like broadcasters would have to do when determining the slot when a programme is scheduled for transmission. In 2011 and 2012, the Belgian CSA conducted three evaluations of the implementation of its recommendation thereby maintaining close contact with the providers established in the French Community (Belgacom, VOO and Universciné).¹¹⁷ It found in its opinion of June 2012 that the interface of the websites was not necessarily controlled by providers, some of which relied on recommendation tools based on pre-determined algorithms or other mechanisms like

alphabetical listings of programmes.¹¹⁸ The Belgian CSA underlined the importance of recommendation tools without, however going so far as the French CSA in demanding that the systems should account for European or national works.¹¹⁹ It concluded that European and Belgian works were accessed from video platforms to an “acceptable” proportion.¹²⁰ Yet, the Belgian CSA seemed to struggle with the establishment of a firm causal link between the measures taken to increase visibility and the consumption of the promoted works inferring that further qualitative studies were necessary to that effect.¹²¹

IV. Reporting form as guidance in the Netherlands

25 Finally, the supervision of Art. 13 AVMSD as implemented in national legal orders encompasses a reporting obligation pursuant to Art. 13 (2) AVMSD. In order to monitor the progress and effectiveness of the rules, Member States are to provide reports to the Commission which in turn allows the latter to assess the EU-wide application of Art. 13 AVMSD in line with its third paragraph. The Directive does not lay down concrete reporting methods and thus leaves Member States a margin of discretion as long as the general aim is abided by. The Commission in its first report on the application of Art. 13, 16 and 17 AVMSD stressed that “effective monitoring” was crucial for the success of the rules and called on Member States to establish monitoring systems which verified providers’ reports.¹²² The question is how to construct an effective reporting mechanism as the systematic and permanent oversight of provider’s catalogues is virtually impossible and unnecessary for the implementation of the provisions contained in the Directive. From the perspective of service providers, burdensome and costly collections of data and their quantification and evaluation could be a factor influencing business decisions and could, potentially, deter providers from locating in a specific country. It seems that a relationship of trust which facilitates cooperation is beneficial for the cultural objective sought here. The reporting method selected by a Member State (or its regulatory body) may equally reflect market conditions like the number of VOD providers subject to its regulatory remit and the precise tools employed for ensuring compliance with Art. 13 (1) AVMSD.¹²³

26 In this respect, the Dutch regulator, the *Commissariaat voor de Media* (CvdM) devised a form at the beginning of 2013 (CvdM reporting form). The CvdM reporting form includes instructions to service providers specifying the obligations imposed by Art. 3.29 *Mediawet* 2008 (Media Act)¹²⁴ which corresponds to Art. 13 (1) AVMSD almost to the letter.¹²⁵ Accordingly, service providers pick a representative day and

report on the amount of European works as well as the investments (such as production or licensing costs) made in such programmes.¹²⁶ Above all, a third section of the reporting form is devoted to the “findability”¹²⁷ of European works asking whether the user can search for European works (whether the origin of productions is indicated), whether tools have been developed which recommend relevant works, whether a specific section devoted to European productions has been created or whether any other instruments are used to reinforce the visibility of and access to European works.¹²⁸ These indicators are broadly reminiscent of those set out in the Recommendation of the Belgian CSA and are considered to be “easy to apply in practice and likely to provide good insight in the actual performance of media service providers”.¹²⁹ The drafting of a reporting form by the CvdM appears to be a pragmatic solution which results in a higher degree of uniformity of responses by service providers and thus facilitates the comparability of the data provided. It avoids “high administrative burdens or time-consuming exercises”¹³⁰ for both parties, the service providers as well as NRAs. To this end, the reporting form seems to constitute a useful and proportionate method. In order to meet the Commission’s request for verification, providers could supply screen shots of their catalogue or disclose parts of their finances as far as confidentiality is guaranteed. Still, rigid reporting regimes appear problematic where the effectiveness of promotional measures is questionable and the market is volatile and evolving. In sum, the discussion above demonstrates how the NRAs of France, Belgium and the Netherlands have impacted on the implementation of Art. 13 AVMSD, each at different ‘stages’: while the French CSA clarified certain aspects of the detailed legislative framework in a report on the application of the legislative instrument, the Belgian CSA issued specific guidance on the wide notion of prominence and the Dutch CvdM outlined indicators in its reporting form for providers. They thus helped to form the national legal frameworks and enhance legal certainty for providers.

E. Conclusion

27 This paper sheds light on the implementation of certain aspects of the AVMSD by NRAs. It focuses on the rules concerning non-linear services, application of which currently represents the most challenging issues in a rapidly transforming and converging media landscape. As recital 69 AVMSD emphasizes “on-demand audiovisual media services have the potential to partially replace television broadcasting”. The market for VOD is evolving dynamically offering novel ways of communication and distribution of information.¹³¹ To this end, VOD

services bear not only huge economic potential but are also beneficial to cultural and social goals thereby bolstering the freedom of expression and the right to receive information, a fundamental right which stands in the centre of media law. The analysis of the AVMSD as implemented by NRAs, in spite of its many technicalities and particularities, constitutes an important factor which should be integrated more forcefully in the discussions about the future regulatory framework for audiovisual media as it pinpoints the weaknesses of the Directive and suggests possible ways forward. It is clear that national solutions may not be transferable to the European level in copy/paste style and would require the support by a majority of Member States implying similar perspectives and perceptions about a certain aspect.

28 Yet, divergences of regulatory practice exist. These may be attributed to, among others, the vagueness of the provisions set out in the AVMSD. To some extent, Directives are characterized by the construction of broad concepts which may be flexibly applied in all Member States. As instruments of Secondary Union law, they lay down the rules of the game (by establishing minimum standards for instance) while Member States fill out the details. It is, however, little constructive if the players of the game do not know whether they play football or hockey. In other words, the scope of a Directive should be based on solid footing. The first section of this paper demonstrates that the application of the AVMSD has become instable in light of converging media such as the printed press and the audiovisual industry. Several NRAs found that the national media laws (and thus implicitly the AVMSD) applied to a specific section of online versions of newspapers. Recital 28 AVMSD which uncompromisingly exempts online newspapers from the scope of the Directive will have to be revisited if the AVMSD is opened for revision. In the second section this paper draws attention to the implementation of the rule concerning the protection of minors in VOD services. NRAs are confronted with business models geared to selling sexualized content which if a certain threshold is passed is classified by NRAs as harmful to minors. This section raises not only questions as to the kind of content considered unsuitable but also wider questions of jurisdiction and how this concept should be construed to account for a globalized society and the Internet age.¹³² Due to the imprecise language of the provision set out in the AVMSD, NRAs enjoy a considerable margin of discretion provided that the national legislature has refrained from specifying the law. The same holds true for the implementation of the rule purporting to promote European works in non-linear services as examined in the third section of this paper. It indicates that the rationale and logic underlying the quota regime for TV broadcasting has necessitated an adaption with regards to VOD services. The examples referred to above reveal

just a glimpse of the diverse activities of the NRAs of EU Member States. They hint at the importance of certain standards (like the protection of minors or the support for European works) for certain Member States and thus supposedly reflect the attitudes and public opinions of their peoples.

29 Today, the phenomenon of Connected TV merging previously separate media which are differently regulated constitutes a major challenge which will have to be tackled in the future. This topic is multi-faceted and not restricted to the AVMSD as the only relevant legal instrument. Indeed, it affects standards like consumer protection (such as the protection of minors) or cultural values (like the promotion of European works) set out in the AVMSD but it is also linked to data protection (confer behavioural advertising and profiling) and telecommunications law (confer infrastructure and interoperability). It has become evident that the current tiers of rules prescribed by the AVMSD are insufficient to deal with converging services. As a response to market developments, NRAs which operate under the present legal framework have shaped the audiovisual sector by regulation rather than waiting for new legislation which would be accompanied by lengthy negotiations at European level. They have thus ensured legal certainty and contributed to the flowering of audiovisual media services within the European Union.

* The author is a PhD student at the Faculty of Law, Economics and Finance of the University of Luxembourg. She has worked on a research project supervised by Associate Prof. Dr. Mark D. Cole examining the national legal acts adopted to transpose the AVMSD into national legal orders; see www.medialaw.lu. The author would like to express her gratitude to Dr. Tarlach McGonagle, Institute for Information Law (IViR) of the University of Amsterdam, and to her colleagues Dr. Lawrence Siry and Bernd Justin Jütte of the University of Luxembourg for their valuable assistance in drafting this paper.

- 1 Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, OJ of 17 October 1989, L 298, p. 23 as amended by Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997, OJ of 30 July 1997, L 202, p. 60.
- 2 Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (Text with EEA relevance), OJ of 18 December 2007, L 332, p. 27 as codified by Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010, OJ of 15 April 2010, L 95, p. 1; See also Corrigendum to Directive 2010/13/EU, OJ of 6 October 2010, L 263, p. 15. All references

- to provisions and recitals in this paper are made according to the numbering of the codified version of the Directive of 2010.
- 3 See for instance the Minutes of the 35th Meeting of the Contact Committee established by the Audiovisual Media Services Directive, Doc CC AVMSD(2011)6, 23 November 2011.
 - 4 European Commission, “Green Paper, Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values”, COM(2013) 231 final, Brussels, 24 April 2013, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0231:FIN:EN:PDF> (accessed 18 July 2014).
 - 5 European Commission, Commission Decision of 3.2.2014 on Establishing the European Regulators Group for Audiovisual Media Services, C(2014) 462 final, 3 February 2014.
 - 6 *Ibid.*, Art. 2 (c).
 - 7 In 1997, shortly after the first revision of the TwFD, the Commission proposed a horizontal approach to all kinds of services to react to the phenomenon of convergence; See European Commission, “Green Paper on the convergence of the telecommunications, media and information technology sectors, and the implications for regulation, Towards an information society approach”, COM(97)623, Brussels, 3 December 1997.
 - 8 Recital 24 of Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (hereinafter referred to as ‘AVMSD’) (Text with EEA relevance) OJ L 95, 15.4.2010, p. 1–24.
 - 9 See generally on the scope of application of the AVMSD: Cole, Mark, D., “The European Legal Framework for on-Demand Services: What Directive for Which Services?”, in *The Regulation of on-Demand Audiovisual Services: Chaos or Coherence?*, ed. Nikoltchev, Susanne, IRIS Special (Strasbourg: European Audiovisual Observatory, 2011), pp. 35–45; Blázquez Cabrera, Francisco, “On-Demand Services: Made in the Likeness of TV?”, in *What Is an on-Demand Service?*, ed. Nikoltchev, Susanne, IRIS Plus 4/2013 (Strasbourg: European Audiovisual Observatory, 2013), pp. 7–27; Schulz, Wolfgang, “Medienkonvergenz Light - Zur Neuen Europäischen Richtlinie Über Audiovisuelle Mediendienste”, *Europäische Zeitschrift für Wirtschaftsrecht*, 2008, pp. 107–111; Valcke, Peggy, Stevens, David, Werkers, Evi and Lievens, Eva., “Audiovisual Media Services in the EU, Next Generation Approach or Old Wine in New Barrels?”, *Communications & Strategies* 7, no. 3 (2008): pp. 103–118; Van Eijk, Nico, “Scope of Application of the Modernised Directive”, in *Regulating the New Media Landscape. A Directive for Audiovisual Media Services without Frontiers*, Schriftenreihe des Instituts für Europäisches Medienrecht (EMR) 36 (Baden-Baden: Nomos, 2008), pp. 21–24.
 - 10 The criterion of editorial responsibility defined in Art. 1 (1) (c) AVMSD is similarly ambivalently worded. This uncertainty may have repercussions on the territorial scope of application of the Directive; See Craufurd Smith, Rachel, “Determining Regulatory Competence for Audiovisual Media Services in the European Union”, *Journal of Media Law*, 2011, 3, 2, p. 265–270.
 - 11 See also recitals 21–29 AVMSD which specify certain concepts and give indications on the scope of the Directive.
 - 12 Art. 1 (1) (g) AVMSD.
 - 13 Art. 1 (1) (e) AVMSD.
 - 14 See generally on the graduated approach to regulation Valcke, Peggy and Stevens, David, “Graduated Regulation of ‘Regulatable’ Content and the European Audiovisual Media Services Directive, One Small Step for the Industry and One Giant Leap for the Legislator?”, *Telematics and Informatics* 24 (2007): pp. 285–302.
 - 15 Valcke, Peggy and Ausloos, Jef, “What If Television Becomes Just an App?” Re-Conceptualising the Legal Notion of Audiovisual Media Service in the Light of Media Convergence”, *ICRI Research Paper* 17, 20 December 2013, p. 6.
 - 16 Recital 22 AVMSD.
 - 17 Recital 21 AVMSD.
 - 18 Recital 23 AVMSD.
 - 19 The Court of Justice of the European Union also frequently turns to the recitals of the AVMSD to deduce the intention of the Union legislature and clarify particular issues. On the notion of surreptitious advertising; See Case C-52/10 Eleftheri tileorasi AE «ALTER CHANNEL» and Konstantinos Giannikos v Ypourgos Typou kai Meson Mazikis Enimerosis and Ethniko Symvoulío Radiotileorasis, 9 June 2011, E.C.R. 2011, I-04973, paras. 25, 26. On the interpretation of the right to short news reports as stipulated in Art. 15 AVMSD; See Case C-283/11 Sky Österreich GmbH v Österreichischer Rundfunk, 22 January 2013, n.y.r., paras. 51, 62.
 - 20 See also Blázquez Cabrera, Francisco, “On-Demand Services: Made in the Likeness of TV?”, 2013, *op.cit.*, pp. 20–22.
 - 21 De Bueger, Geneviève, “Supervising On-demand Audiovisual Media Services: Best practices and Methodology”, Comparative Background Document, 38th EPRA Meeting (EPRA, 2013), p. 6.
 - 22 Polak, Juraj, “Tvsm considered on-demand audiovisual media service”, *IRIS Merlin Newsletter* 9, 2012, p. 38, available at <http://merlin.obs.coe.int/iris/2012/9/article38.en.html> (accessed 26 June 2014).
 - 23 The Swedish Broadcasting Commission issued four individual decisions in October 2012; See Granskningsnämnden för radio och tvs beslut i Dnr 12/00777-00780 av den 29 oktober 2012, available at <http://www.radioochtv.se/CaseDecisions/206404.pdf>, <http://www.radioochtv.se/CaseDecisions/206405.pdf>, <http://www.radioochtv.se/CaseDecisions/206406.pdf> (accessed 26 June 2014); See also Ullberg, Erik and Plogell, Michael, “Radio and Televisions Act applies to newspapers’ Web TV services”, *IRIS Merlin Newsletter* 1, 2013, p. 35, available at <http://merlin.obs.coe.int/iris/2013/1/article35.en.html> (accessed 26 June 2014).
 - 24 Machet, Emmanuelle, “New Media & Regulation: Towards a Paradigm Shift? New Services and Scope: ‘What’s In, What’s out Revisted’”, Comparative Background Document, 35th EPRA Meeting (EPRA, 2012), pp. 14, 15, 17; Valcke, Peggy and Ausloos, Jef, “What If Television Becomes Just an App?” Re-Conceptualising the Legal Notion of Audiovisual Media Service in the Light of Media Convergence”, 2013, *op.cit.*, para. 2.4.1, p. 13.
 - 25 Since 31st December 2013, the BKS no longer acts as the appeal instance for decisions of the KommAustria (as foreseen in Sec. 36 (2) KommAustria Gesetz (KommAustria Law). This function has been transferred to the Bundesverwaltungsgericht (Federal Administrative Court) by an amendment adopted in May 2013 which modified Sec. 36 KommAustria Law.
 - 26 Kommunikationsbehörde Austria, Bescheid, KOA 1.950/12-048, Vienna, 9 October 2012, available at https://www.rtr.at/de/m/KOA195012048/KOA_1.950-12-048.pdf (accessed 26 June 2014). Bundeskommunikationssenat, Bescheid GZ. 611.191/0005-BKS/2012, Vienna, 13 December 2012, available at <http://www.bundeskanzleramt.at/DocView.axd?CobId=49930> (accessed 26 June 2014); See also Matzneller, Peter, “Video section of newspaper website is notifiable on-demand service”, *IRIS Merlin Newsletter* 3, 2013, p. 9, available at <http://merlin.obs.coe.int/iris/2013/3/article9.en.html> (accessed 25 June 2014).
 - 27 Kommunikationsbehörde Austria, Bescheid, KOA 1.950/12-048, *op.cit.*, para. 4.4.1, p. 10.
 - 28 *Ibid.*
 - 29 *Ibid.*, para. 4.4.2, p. 11.
 - 30 *Ibid.*
 - 31 *Ibid.*

- 32 Bundeskommunikationssenat, Bescheid GZ. 611.191/0005-BKS/2012, Vienna, 13 December 2012, para. 8, p. 4.
- 33 *Ibid.*, paras. 9, 10, p. 5, 6.
- 34 *Ibid.*, para. 10, p. 5.
- 35 *Ibid.*
- 36 See pending case C-347/14 New Media Online.
- 37 See the order of the Austrian Administrative Court of 26.06.2014, available at https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vwgh&Dokumentnummer=JWT_2013030012_20140626X00.
- 38 In March 2010, the Office for Communications (Ofcom), as the UK's independent regulator for the communications industry designated ATVOD, previously a self-regulatory body, as the competent co-regulator in charge of the regulation of certain aspects of the provision of on-demand audiovisual media services; See the original designation of March 2010: Ofcom, "Designation pursuant to Section 368B of the Communications Act 2003 of Functions to the Association for Television On-Demand in Relation to the Regulation of On-Demand Programme Services", 2010, <http://atvod.co.uk/uploads/files/designation1803101.pdf> (accessed 25 June 2014); See the amended designation of September 2012 Ofcom, "The Amended Designation Dated 14 September 2012, Designation pursuant to Section 368B of the Communications Act 2003 of Functions to the Association for Television On-Demand in Relation to the Regulation of on-Demand Programme Services", 2012, <http://atvod.co.uk/uploads/files/amended-designation140912.pdf> (accessed 25 June 2014).
- 39 For a concise overview of ATVOD's regulatory tasks see Mac Sithigh, Daithi, "Convergence, The Impact of Broadcast Regulation on Telecommunications", in *Telecommunications Law and Regulation*, ed. Walden, Ian, fourth edition, (Oxford: Oxford University Press), 2012, paras. 14.5 et seq., pp. 680–687.
- 40 In the UK, the AVMSD was primarily transposed by means of the Audiovisual Media Services Regulation of 2009 which inserted, among others, Sec. 368A CA 2003 in the CA 2003. For an overview of the legal acts adopted to transpose the AVMSD in the UK; See http://www.en.uni.lu/recherche/fdef/droit_des_medias/audiovisual_media_services_directive/national_execution_measures/united_kingdom (accessed 25 June 2014).
- 41 ATVOD Notice of Determination that the provider of the service "Sun Video" has contravened Section 368BA of the Communications Act 2003, 11 February 2011; Notice of Determination that the provider of the service "News of the World Video" has contravened Section 368BA of the Communications Act 2003, 11 February 2011; Notice of Determination that the provider of the service "Sunday Times Video Library" has contravened Section 368BA of the Communications Act 2003, 11 February 2011; Notice of Determination that the provider of the service "Guardian Video" has contravened Section 368BA of the Communications Act 2003, 28 June 2011; Notice of Determination that the provider of the service "Financial Times Video" has contravened Section 368BA of the Communications Act 2003, 30.6.2011. ATVOD's determinations are available at <http://www.atvod.co.uk/complaints/determinations/2011-determinations> (accessed 25 June 2014).
- 42 Ofcom, "Appeal by News Group Newspaper Limited against a notice of determination by ATVOD that the provider of the service "Sun Video" has contravened Section 368BA of the Communications Act 2003", 21 December 2011; See http://www.atvod.co.uk/uploads/files/Ofcom_Decision_-_SUN_VIDEO_211211.pdf (accessed 25 June 2014).
- 43 The Ofcom guidance was subsequently "codified" in ATVOD's guidance on "Who needs to notify" as updated in February 2014, paras. 3.10-3.13, pp. 9, 10; See http://www.atvod.co.uk/uploads/files/Guidance_on_who_needs_to_notify_Ed_4.0_Feb_2014.pdf (accessed 25 June 2014).
- 44 Lowde, Shaun and Wells, Orlando, "ATVOD Determined to Do Better", *Computer and Telecommunications Law Review* 18, no. 4 (2012), pp. 102–104; Metzdorf, Jenny, "Regulierung der Elektronischen Presse in Großbritannien? Ein Anwendungsbeispiel zum Erwägungsgrund 28 der AVMD-RL", in *IT Und Internet - Mit Recht Gestalten*, ed. Taeger, Jürgen, Tagungsband Herbstakademie 2012 (Oldenburg: Oldenburger Verlag für Wirtschaft, Informatik und Recht, 2012), pp. 497–516; Pimlott, Nick and Lewis, David, "Regulation of Video on Demand Services Following the 'Sun Video' Appeal", *Entertainment Law Review* 23, no. 3 (2012), pp. 65–68; Valcke, Peggy and Ausloos, Jef, "What If Television Becomes Just an App?" Re-Conceptualising the Legal Notion of Audiovisual Media Service in the Light of Media Convergence", 2013, *op.cit.*, para. 2.4.2, p. 15.
- 45 Ofcom, Appeal by News Group Newspaper Limited against a notice of determination by ATVOD, 21 December 2011, paras. 90 a., b., p. 27.
- 46 *Ibid.*, paras. 90 c., e., f. p. 28.
- 47 *Ibid.*, para. 90 d., p. 28.
- 48 *Ibid.*, para. 90 g., pp. 28, 29.
- 49 In general, Ofcom may (i) uphold ATVOD's determination, (ii) quash ATVOD's determination and remit it back for reconsideration or (iii) substitute its decision for ATVOD's assessment. Proof of the importance of the case Sun Video is reinforced by Ofcom's substituting its decision for that of ATVOD's.
- 50 Ofcom, Appeal by News Group Newspaper Limited against a notice of determination by ATVOD, 21 December 2011, paras. 91, 96, 97, pp. 29, 30.
- 51 *Ibid.*, para. 186, para. 47.
- 52 ATVOD, Summary of determination that the provider of "Vice (Video)" is in breach of ATVOD's Rules 1 & 4 and thereby has contravened Section 368BA and Section 368D (3) (ZA) of the Communications Act 2003, 14 August 2013.
- 53 See on the increasingly "complex [national] regulatory landscape[s]", Craufurd Smith, Rachael, "Determining Regulatory Competence for Audiovisual Media Services in the European Union", 2011, *op.cit.*, p. 284.
- 54 The specific provisions of Art. 12 and 27 AVMSD are supplemented by other rules protecting minors in view of advertising and commercial communications. Above all, Art. 9 (1) (g) AVMSD requires that commercial messages do not harm minors and do not directly exhort minors to buy the products and services advertised; See also Art. 10 (1) (b) AVMSD, Art. 11 (1) (3) (b) AVMSD, Art. 22 (a) AVMSD.
- 55 Recommendation 2006/952/EC of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry, OJ of 27 December 2006, L 378, p. 72, paras. II 1, 2.
- 56 Harrison, Jackie and Woods, Lorna, "European Broadcasting Law and Policy", *Cambridge University Press*, Cambridge 2007, pp. 235, 236; Lievens, Eva, "Protecting Children in the Digital Era, The Use of Alternative Regulatory Instruments", *Martinus Nijhoff Publishers*, Leiden, 2010, p.44-47, 350.
- 57 ATVOD, "Rules & Guidance, Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services (ODPS)", Edition 2.1, 26 February 2014, http://atvod.co.uk/uploads/files/ATVOD_Rules_and_Guidance_Ed_2.1_February_2014.pdf (accessed 25 June 2014).
- 58 Ofcom, "Sexually Explicit Material and Video On Demand Services, A Report to DCMS by Ofcom", 4 August 2011, <http://stakeholders.ofcom.org.uk/binaries/internet/>

- explicit-material-vod.pdf (accessed 25 June 2014); See also Government's response in form of a letter from Ed Vaizey, Department for Culture, Media and Sport to Ed Richards of 3 August 2011, available at <http://webarchive.nationalarchives.gov.uk/20121204113822/http://www.culture.gov.uk/images/publications/EVletter-to-ed-richards-3aug2011pdf.pdf> (accessed 25 June 2014).
- 59 In several policy documents, ATVOD outlined its precautionary approach: ATVOD, "House of Lords Select Committee on Communications, Media Convergence and Its Public Policy Impact, The Submissions of the Authority for Television On Demand", 20 September 2012, p. 6, http://www.atvod.co.uk/uploads/files/Media_Convergence_call_for_evidence_ATVOD_submission_FINAL.pdf (accessed 26 June 2014); ATVOD, "The Culture, Media & Sports Inquiry into Online Safety, Submission from the Authority for Television On Demand", 3 October, 2013, paras. 2.2, 2.3, <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmcmmeds/729/729vw64.htm> (accessed 26 June 2014); ATVOD, "For Adults Only? Underage Access to Online Porn", 28 March 2014, pp. 7, 9.
- 60 This threshold is without prejudice to the material which is considered illegal under Sec. 1 of the Obscene Publications Act (OPA) of 1959 & 1964 and is thus prohibited under Sec. 2 OPA unless justified by the "defense of public good" laid down in Sec. 4 OPA.
- 61 BBFC, "BBFC Guidelines, Age Ratings You Trust", 2014, http://bbfc.co.uk/sites/default/files/attachments/BBFC%20Classification%20Guidelines%202014_0.pdf (accessed 26 June 2014).
- 62 ATVOD, "Rules & Guidance, Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services" (ODPS), Edition 2.1, *op.cit.*, Rule 11, pp. 12, 13.
- 63 ATVOD, "For Adults Only? Underage Access to Online Porn", p. 9; See also ATVOD, "UKCCIS Parental Controls Consultation, The Submission of the Authority for Television On Demand", 18 September 2012, pp. 6, 7, http://www.atvod.co.uk/uploads/files/Parental_controls_consultation_-_ATVOD_response_FINAL.pdf (accessed 26 June 2014).
- 64 ATVOD, "Rules & Guidance, Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services" (ODPS), Edition 2.1, *op.cit.*, Rule 11, p. 13.
- 65 In similar vein, the German Federal Supreme Court (*Bundesgerichtshof*) ruled in September 2007 that an age verification system based on the number included in the identity card (*Personalausweis*) or passport in addition to the indication of the postal code of the city where the document was issued did not constitute an "effective barrier" in order to guarantee that underage persons could not access the content; See BGH vom 18.9.2007 – I ZR 102/05 – ueber18.de – OLG Düsseldorf, *Zeitschrift für Urheber- und Medienrecht* 2008, pp. 511-516.
- 66 ATVOD, "Rules & Guidance, Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services" (ODPS), Edition 2.1, *op.cit.*, Rule 11, p. 13.
- 67 With regards to the protection of children from inappropriate content, several UK regulators across different media launched the initiative ParentPort in 2011. It aims at facilitating the detection of inappropriate content and education of parents; See <http://www.parentport.org.uk/> for more information (accessed 26 June 2014).
- 68 ATVOD, For Adults Only? Underage Access to Online Porn, p. 9.
- 69 See also Ofcom, "Procedures for the Consideration of Statutory Sanctions Arising in the Context of On-Demand Programme Services", 1 October 2013, <http://stakeholders.ofcom.org.uk/binaries/broadcast/tv-ops/vod/sanctions-procedures.pdf> (accessed 26 June 2014).
- 70 Ofcom, "Sanction: Decision by Ofcom Imposed on Playboy TV/Benelux Limited for the provision of the on-demand programme service "Demand Adult" from 31 May 2012 to 24 July 2012", 83(12), 16 January 2013; Ofcom, "Sanction: Decision by Ofcom Imposed on Playboy TV/Benelux Limited for the provision of the on-demand programme service "Playboy tv.co.uk" from 31 May 2012 to 24 July 2012", 84(12), 16 January 2013. For all determinations of ATVOD and subsequent appeals to Ofcom discussed below; See ATVOD's website <http://www.atvod.co.uk/complaints/determinations> (accessed 26 June 2014).
- 71 ATVOD, "Determination that the provider of the on demand programme service "playboytv.co.uk" was in breach of rule 11", 2 July 2012; ATVOD, "Determination that the provider of the on demand programme service "Demand Adult" was in breach of rule 11", 2 July 2012.
- 72 ATVOD, "Determination that the provider of the on demand programme service "playboytv.co.uk" was in breach of rule 11", 2 July 2012, pp. 6, 7; ATVOD, "Determination that the provider of the on demand programme service "Demand Adult" was in breach of rule 11", 2 July 2012, p. 6.
- 73 The exact time period when the service provider contravened Rule 11 and thereby Sec. 368E (2) CA 2003 was from 31 May to 24 July 2012 as indicated by the sanction decision of Ofcom.
- 74 ATVOD, "Determination that the provider of the on demand programme service "playboytv.co.uk" was in breach of rule 11", 2 July 2012, pp. 6; ATVOD, "Determination that the provider of the on demand programme service "Demand Adult" was in breach of rule 11", 2 July 2012, p. 7.
- 75 See ATVOD's determinations of September 2012: Notice of Determination that Playboy TV UK/Benelux Limited is the provider of the service "Demand Adult", 17 September 2012; Notice of Determination that Playboy TV UK/Benelux Limited is the provider of the service "Playboytv.co.uk", 17 September 2012.
- 76 Ofcom, "Ofcom Decision, Appeal by Playboy TV UK/Benelux Limited against a notice of determination by ATVOD that it was the provider of the service "Demand Adult" as at 14 September 2012", 23 September 2013, para. 34, p. 8; Ofcom, "Ofcom Decision, Appeal by Playboy TV UK/Benelux Limited against a notice of determination by ATVOD that it was the provider of the service "Playboy TV" as at 14 September 2012", 23 September 2013, para. 33, p. 8.
- 77 ATVOD, The Culture, Media & Sports Inquiry into Online Safety, para. 1.8.
- 78 The research commissioned by ATVOD found that "the eight most visited adult sites were all free tube sites, as were 15 of the top 16.", ATVOD, For Adults Only? Underage Access to Online Porn, p. 19.
- 79 ATVOD, For Adults Only? Underage Access to Online Porn, p. 21.
- 80 ATVOD, For Adults Only? Underage Access to Online Porn, p. 24.
- 81 ATVOD, For Adults Only? Underage Access to Online Porn, pp. 13-17. The surveys conducted by Nielsen Netview by order of ATVOD are based on an assessment of consumption using a computer or laptop and exclude the use of tablets, smartphones and other devices. ATVOD therefore relies on research conducted by Ofcom which shows that minors of particular age groups increasingly use mobile phones or tablets to go online in order to conclude that its figures are underestimated; See also Ofcom, "Children and Parents: Media Use and Attitudes Report", 3 October 2013, p. 44, <http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/october-2013/research07Oct2013.pdf> (accessed 26 June 2014).

- 82 Siry, Lawrence, "Knowing It When It Is Seen, The Polemic of the Regulation of Sexualized Speech in the United States and Europe", soon to be published, p. 324.
- 83 For an overview of NRAs activities concerning the protection of minors see Machet, Emmanuelle, "The Protection of Minors in a Connected Environment", Comparative Background Document, 37th EPRA Meeting, 2013, pp. 7–9.
- 84 In Germany, for instance, the reform of the relevant laws for the protection of minors failed in December 2010 when the Parliament of one of the German Länder rejected the 14th amendment to the Interstate Treaty for the Protection of Minors. So far, the reform has been on hold but has received new impetus by an online consultation which is currently taking place on the future of the Interstate Treaty and the system of regulated self-regulation concerning the classification of content and youth protection programmes as well as parental control systems. The consultation is organized by the Landesmedienanstalten (LMA, media authorities of the German Länder) under <https://www.jugendmedienschutz.sachsen.de/sachsen/de/home> (accessed 26 June 2014); See also the Discussion Paper of the LMA available at <https://www.jugendmedienschutz.sachsen.de/ecm-politik/sachsen/de/home/file/fileId/952> (accessed 26 June 2014).
- 85 Art. 4 and 5 TWFD of 1989.
- 86 Art. 1 (1) (n) AVMSD; See on the lack of a quality criterion in the definition of European works Harrison, Jackie and Woods, Lorna, "European Broadcasting Law and Policy", 2007, *op.cit.*, p. 254-259.
- 87 In its Weber report of 2005, the European Parliament recommended the precision of the definition of "European works" and an introduction of a definition of "independent producer". It further advocated the development of "European co-productions and joint marketing strategies" which implies its dissatisfaction with the construction of the definitions in the TWFD; See European Parliament, "on the application of Articles 4 and 5 of Directive 89/552/EEC (the "TV without Frontiers" Directive), as amended by Directive 97/36/EC, for the period 2001-2002", (2004/2236(INI)), 21 June 2005, Explanatory Statement, para. 1, p. 12.
- 88 Burri-Nenova, Mira, "The New Audiovisual Media Services Directive: Television without Frontiers, Television without Cultural Diversity," *Common Market Law Review* 14 (2007): 1707; Craufurd Smith, Rachel, "From Heritage Conservation to European Identity: Article 151 EC and the Multi-Faceted Nature of Community Cultural Policy," *European Law Review* 32, no. 1 (2007): 48–69; Katsirea, Irini, "Why the European Broadcasting Quota Should Be Abolished", *European Law Review* 28, no. 2 (2003): 190–209; McGonagle, Tarlach "The Quota Quandary: An Assessment of Articles 4-6 of the Television without Frontiers Directive," in *The European Union and the Culture Industries, Regulation and the Public Interest*, ed. David Ward, United Kingdom, Ashgate Publishing, 2008, 187–212.
- 89 Castendyk, Oliver, "Article 4 TWFD (Promotion of European Works)", in *European Media Law*, ed. Castendyk, Oliver, Dommering, Egbert and Scheuer, Alexander (The Netherlands: Kluwer Law International, 2008), para. 63, p. 452.
- 90 Burri-Nenova, Mira, "Cultural Diversity and the EC Audiovisual Media Services Directive: Beyond the Handsome Rhetoric", NCCR Trade Regulation Working Paper No. 2009/09, 30 March 2009, pp. 12–17, available at SSRN: <http://ssrn.com/abstract=1370439> or <http://dx.doi.org/10.2139/ssrn.1370439>.
- 91 This may partly be explained by the fact that the Commission examined the application of Art. 13 AVMSD in the years 2009 and 2010, a period immediately following the deadline for transposition. In fact, transposition of the Directive was delayed in several Member States (such as Luxembourg, Portugal, Poland or Slovenia). In addition, measures to promote European works in VOD services were introduced for the first time in many Member States so that the industry needed some time to adapt and conform to the new requirements; See European Commission, "Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, First Report on the Application of Articles 13, 16 and 17 of Directive 2010/13/EU for the period 2009-2010, Promotion of European works in EU scheduled and on-demand audiovisual media services", COM(2012) 522 final, Brussels, 24 September 2012, para. 1.1.1, p. 3; para. 1.1.3, p. 5; para. 3, p. 11; See also the European Parliament's resolution of 11 September 2012 on the online distribution of audiovisual works in the European Union (P7_TA(2012)0324) which calls on Member States to effectively implement Art. 13 AVMSD, para. 34. On the application of Art. 16 AVMSD see para. 2.2, p. 9.
- 92 European Commission, "Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, First Report on the Application of Articles 13, 16 and 17 of Directive 2010/13/EU for the period 2009-2010, Promotion of European works in EU scheduled and on-demand audiovisual media services", COM(2012) 522 final, Brussels, 24 September 2012, para. 1.1.1, p. 3.
- 93 Entraygues, Alexandre, "French Solutions", in *Video on Demand and the Promotion of European Works*, ed. Nikoltchev, Susanne, IRIS Special (Strasbourg: European Audiovisual Observatory, 2013), p. 25.
- 94 Interestingly, a French Decree of December 2010 provides for a circumvention rule in case of a VOD provider established outside of France but directing its service wholly or principally to the French public. The French regulator could, on the basis of Art. 4 of this Decree take action against service providers allegedly failing to comply with the rules on promotion of European works. "Décret n° 2010-1593 du 17 décembre 2010 relatif aux services de télévision et de médias audiovisuels à la demande relevant de la compétence d'un autre Etat membre de l'Union européenne ou partie à l'accord sur l'Espace économique européen ou à la convention européenne sur la télévision transfrontière du 5 mai 1989", JORF n°0294 du 19 décembre 2010, p. 22368, texte n° 29, NOR: MCCE1019062D; See also Craufurd Smith, Rachael, "Determining Regulatory Competence for Audiovisual Media Services in the European Union", 2011, *op.cit.*, p. 281.
- 95 The analysis below focuses on the aspect of promotion and thus omits any assessment of financial contributions prescribed by the respective national laws.
- 96 Décret n° 2010-1379 du 12 novembre 2010 relatif aux services de médias audiovisuels à la demande, JORF n°0264 du 14 novembre 2010, p. 20315, texte n° 58, NOR: MCCE1019142D. Hereinafter 'French VOD Decree of 2010'.
- 97 The obligation is triggered when the catalogue of a service provider comprises 20 audiovisual works of more (confer Art. 11 French VOD Decree of 2010) and gradual compliance with the quotas is permissible pursuant to Art. 12 of the French VOD Decree of 2010.
- 98 Conseil supérieur de l'audiovisuel, "Rapport au Gouvernement sur l'application du décret n° 2010-1379 du 12 novembre 2010 relatif aux services de médias audiovisuels à la demande (SMAD)", November 2013, available at <http://csa.fr/Services-interactifs/Services-de-medias-audiovisuels-a-la-demande-SMAD/Rapport-au-Gouvernement-sur-l-application-du-decret-n-2010-1379-du-12-novembre-2010-relatif-aux-services-de-medias-audiovisuels-a-la-demande-SMAD> (accessed 26 June 2014). Hereinafter 'CSA Report of November 2013'.
- 99 The French CSA noted in its report that the calculation should take into account the number of days when the title was featured in the catalogue on an annual basis; See CSA Report of November 2013, para. 3. b), p. 34; para. 6. a), p. 44.
- 100 *Ibid*, para. 6. b), p. 45.

- 101 European Commission, “Commission Staff Working Document, Promotion of European Works in EU scheduled and on-demand audiovisual media services, Part I on the application of Article 13 of Directive 2010/13/EU for the period 2009-2010, Accompanying the document First Report on the Application of Articles 13, 16 and 17 of Directive 2010/13/EU for the period 2009-2010 (COM(2012) 522 final)”, Brussels, 24 September 2012, SWD(2012) 269 final, para. 1.3.
- 102 CSA Report of November 2013, para. 6. b), p. 46.
- 103 *Ibid.*
- 104 *Ibid.*, para. 6. c), p. 47.
- 105 *Ibid.*
- 106 On the organization, tasks and sanctioning powers of the Belgian CSA see Valcke, Peggy and Lievens, Eva, *Media Law in Belgium* (The Netherlands: Kluwer Law International, 2011), paras. 278 et seq., pp. 144–149.
- 107 Parlement de la Communauté Française (Belgique), “Projet de décret modifiant le décret du 27 février 2003 sur la radiodiffusion et le décret du 9 janvier 2003 relatif à la transparence, à l’autonomie et au contrôle des organismes publics, des sociétés de bâtiments scolaires et des sociétés de gestion patrimoniale qui dépendent de la communauté française”, Projet de décret 634 (2008-2009), N°1, 22 December 2008, Art. 63, pp. 23, 24, available at <http://www.pfwb.be/le-travail-du-parlement/doc-et-pub/documents-parlementaires-et-decrets/documents/001274595> (accessed 26 June 2014). Hereinafter ‘Draft AVMS Decree’.
- 108 Draft AVMS Decree, Art. 63, p. 24.
- 109 Collège d’autorisation et de contrôle, “Recommandation relative à la mise en valeur des oeuvres européennes et de la Communauté française de Belgique dans les services de vidéo à la demande”, 24 June 2010, available at <http://www.csa.be/documents/1313> (accessed 26 June 2014). Hereinafter ‘CSA Recommendation of 2010’.
- 110 CSA Recommendation of 2010, para. 4, p. 8. The Recommendation even referred to “ghettoisation” (or marginalization) and user prejudices regarding works of European or national origin.
- 111 *Ibid.*
- 112 *Ibid.*
- 113 *Ibid.*
- 114 Interestingly, the Belgian CSA outlined “other parameters” which could impact on the prominence of European and Belgian works. In this context, it called on providers to carefully consider the date they would enter the relevant programme in their catalogues with a view to avoiding direct competition with American blockbusters. It acknowledged that such dates habitually depended on the windows within which the distribution rights of a film could be exploited. Still, the duration of the inclusion of the work in the catalogue as well as the simultaneous offer of competing works (whether European/Belgian or not) were factors likely to influence the visibility of European and Belgian productions; See CSA Recommendation of 2010, para. 6, pp. 9, 10.
- 115 Furnémont, Jean-Francois, “New Issues and Challenges for Audiovisual Policy-Makers, Films Institutions and Audiovisual Regulators: The Example of the French Community of Belgium”, in *Video on Demand and the Promotion of European Works*, ed. Nikoltchev, Susanne, IRIS Special (Strasbourg: European Audiovisual Observatory, 2013), p. 39.
- 116 *Ibid.*
- 117 The opinions of the Belgian CSA evaluating the measures taken to promote European and Belgian works are available at <http://csa.be/documents/1779> (accessed 26 June 2014); See in particular Collège d’autorisation et de contrôle, “Avis n° 11/2012, Evaluation du dispositif de mise en valeur des oeuvres européennes et de la Fédération WallonieBruxelles dans les services de vidéo à la demande – article 46 du décret SMA”, 28 June 2012, available at http://www.csa.be/system/documents_files/1779/original/CAC_20120628_avis_evaluation_recommandation_VOD.pdf?1341305335 (accessed 18 July 2014).
- 118 Collège d’autorisation et de contrôle, “Avis n° 11/2012, Evaluation du dispositif de mise en valeur des oeuvres européennes et de la Fédération WallonieBruxelles dans les services de vidéo à la demande – article 46 du décret SMA”, 28 June 2012, para. 4.5, p. 11.
- 119 *Ibid.*, para. 6.1, p. 19.
- 120 *Ibid.*, para. 7, p. 23.
- 121 *Ibid.*, paras. 6.2 and 6.3, pp. 20 and 21; para. 7, p. 23.
- 122 European Commission, “Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, First Report on the Application of Articles 13, 16 and 17 of Directive 2010/13/EU for the period 2009-2010, Promotion of European works in EU scheduled and on-demand audiovisual media services”, COM(2012) 522 final, Brussels, 24 September 2012, para. 1.1. b), p. 6.
- 123 In Belgium and France, for instance, providers of VOD services are obliged to submit a report annually in line with Art. 40 Belgian Decree AVMS and Art. 21 French VOD Decree 2010 respectively. To verify the data supplied by service providers, the French CSA carries out random spot checks while the Belgian CSA for the purpose of its final report of 2012 appeared to compile data within a specific reference period; See European Commission, “Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, First Report on the Application of Articles 13, 16 and 17 of Directive 2010/13/EU for the period 2009-2010, Promotion of European works in EU scheduled and on-demand audiovisual media services”, COM(2012) 522 final, Brussels, 24 September 2012, para. 1.1. b), p. 6; See also Entraygues, Alexandre, “French Solutions”, in *Video on Demand and the Promotion of European Works*, ed. Nikoltchev, Susanne, IRIS Special (Strasbourg: European Audiovisual Observatory, 2013), p. 29; Collège d’autorisation et de contrôle, “Avis n° 11/2012, Evaluation du dispositif de mise en valeur des oeuvres européennes et de la Fédération WallonieBruxelles dans les services de vidéo à la demande – article 46 du décret SMA”, 28 June 2012, para. 5.1, p. 12.
- 124 Wet van 29 december 2008 tot vaststelling van een nieuwe Mediawet.
- 125 Commissariaat voor de Media, “Rapportageformulier/Vragenlijst ten behoeve van rapportage Europese quota cmoa”, available at <http://www.cvdm.nl/praktisch/commercielemediadienst-op-aanvraag-aanmelden/> (accessed 26 June 2014). Hereinafter ‘CvdM Reporting form’.
- 126 CvdM Reporting form, paras. I – N dedicated to the share of European works in the catalogue and paras. O-T concerning financial contributions.
- 127 The term “findability” is distilled from the European Parliament’s resolution of 4 July 2013 on connected TV, paras. L, M and 1. The expression adequately captures the vast amount of content available on connected TV devices and raises the question of prioritization of content (how and by whom?) and the creation of user-friendly and transparent tools whereby content is structured and can thus be found more easily by users.
- 128 CvdM Reporting form, paras. U-X.
- 129 Betzel, Marcel, “The Dutch Approach”, in *Video on Demand and the Promotion of European Works*, ed. Nikoltchev, Susanne, IRIS Special (Strasbourg: European Audiovisual Observatory, 2013), p. 35.
- 130 *Ibid.*

- 131 The Commission's Green Paper of 2013 highlights that consumption of audiovisual content is increasingly moving online. European Commission, "Green Paper, Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values", COM(2013) 231 final, Brussels, 24 April 2013, *op.cit.*, para. 2, p. 4.
- 132 See Hörnle, Julia, "The Jurisdictional Challenge of the Internet", in *Law and the Internet*, eds. Edwards, Lilian and Waelde, Charlotte, third edition (Oxford and Portland, Oregon: Hart Publishing, 2009), pp. 121–58; Schmitz, Sandra and Siry, Lawrence, „Internationale Gerichtliche Zuständigkeit Bei Persönlichkeitsverletzungen Im Internet“, in *Die Welt Im Netz - Folgen Für Wirtschaft Und Gesellschaft, Tagungsband Der Herbstakademie 2011* (Oldenburg: Oldenburger Verlag für Wirtschaft, Informatik und Recht, 2011), pp. 83–100.

A Qualitative Study on the Adoption of Copyright Assignment Agreements (CAA) and Copyright License Agreements (CLA) within Selected FOSS Projects

by **Sylvia F. Jakob**, LL.B.(Hons.), Dipl. L.P., LL.M., Solicitor (n.p), Research Assistant, Institute for Legal Informatics, Hannover

Abstract: Open source software projects are multi-collaborative works incorporating the contributions of numerous developers who, in spite of publishing their code under a public license such as GPL, Apache or BSD, retain the copyright in their contributions. Having multiple copyright-owners can make the steering of a project difficult, if not impossible, as there is no ultimate authority able to take decisions relating to the maintenance and use of the project. This predicament can be remedied by centring the dispersed copyrights in a single authority via contributor agreements. Whether to introduce contributor agreements, and if so in which form, is a pressing question for many emerging, but also for established

projects. The current paper provides an insight into the ethos of different projects and their reason for adopting or rejecting particular contributor agreements. It further examines the exact set-up of the contributor agreements used and concludes that smart drafting can blur the difference between CAAs and CLAs to a considerable extent, manoeuvring them into a legal grey area. To avoid costly litigation to test the legal enforceability of individual clauses, this paper proposes the establishment of an international committee comprised of developers, product managers and lawyers interested in finding a common terminology that may serve as a foundation for every contributor agreement.

Keywords: Free and Open Source Software (FOSS), Public Licenses, Outbound Licenses, Inbound Licenses, Contributor Agreements, Contributor Assignment Agreements (CAA), Contributor License Agreements (CLA)

© 2014 Sylvia F. Jakob

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

This article may also be used under the Creative Commons Attribution-Share Alike 3.0 Unported License, available at <http://creativecommons.org/licenses/by-sa/3.0/>.

Recommended citation: Sylvia F. Jakob, A Qualitative Study on the Adoption of Copyright Assignment Agreements (CAA) and Copyright License Agreements (CLA) within Selected FOSS Projects, 5 (2014) JIPITEC 105, para. 1.

A. Introduction

- 1 Open source software projects are multi-collaborative works incorporating the contributions of numerous developers who, in spite of publishing their code under a public license such as GPL, Apache or BSD, retain the copyright in their contributions. The public license, also referred to as an “outbound license”, regulates the usage rights granted by the developer to the outside world. It ensures that the code can be used by virtually everyone having an interest in doing so as long as the user follows the terms of the outbound license.
- 2 However, having multiple copyright-owners can make the steering of a project difficult, if not impossible, as there is no ultimate authority able to take decisions relating to the maintenance and use of the project. This predicament can be remedied by centring the dispersed copyrights in a single authority via contributor agreements, also referred to as “inbound licenses” because they regulate the relationship of the developer with a particular organizational entity.
- 3 In recent years many FOSS projects have incorporated as non-profit organizations¹ and many corporations have begun to release protected code under open source licenses to harness the wisdom of the crowd.² Many of these organizations require their contributors to sign a contributor agreement, either in the form of a Copyright Assignment Agreement (CAA), whereby the developer transfers and abandons his intellectual property rights in the contribution for the benefit of a project’s administration, or a Contributor License Agreement (CLA),³ whereby the developer is only required to grant usage rights. Some projects, in turn, continue to follow the notion of “outbound” equals “inbound”,⁴ arguing that a public license sufficed and no intellectual property management within the project was necessary.⁵
- 4 To date no comprehensive, legal study⁶ has been conducted asking which kind of projects use CAAs, which CLAs, and which forego the management of intellectual property of contributions entirely. The existence of a pattern would be particularly interesting for new projects, as many find it difficult to determine into which end of the spectrum they fall, whether to use a contributor agreement, and if so, how to draft it, or where appropriate, to refrain from using a contributor agreement from the outset.
- 5 It is thus the objective of this study to search for common denominators and gain valuable insights for the benefit of different stakeholders, first and foremost developers, product managers and lawyers.

B. Qualitative Interviews and Research

I. Questions and Methodology

- 6 To accomplish this aim, a questionnaire was created and used as common thread during a series of interviews. Sixteen stakeholders⁷ agreed to be interviewed, including (legal) representatives of projects, independent consultants, product managers, independent and employed FOSS developers and one professor of computer science with a special focus on open source software,⁸ thus constituting a representative sample of interested stakeholders. In addition, further research was undertaken in the fields of law, organizational science and business informatics to back up the results obtained.
- 7 As expected, a clear distinction could be made between projects that actively managed contributions and those that did not. The following paragraphs shall provide an overview of selected FOSS projects, examining their makeup and reasons for using or refusing particular contributor agreements.

C. Projects That Do Not Actively Manage Contributions

I. The Linux Kernel

- 8 The Linux Kernel is only a small part of the software on a full Linux system, not including systems software, libraries or applications, but as the core, it is responsible for managing the hardware, running user programs and maintaining the overall security and integrity of the system.⁹
- 9 The Kernel was originally written by Linus Torvalds, who published it as a pet project on a usenet posting in August 1991.¹⁰ At first it was released under its own licence, which had a restriction on commercial activity; however, Torvalds soon changed the license to the GPL 2, encouraging thousands of developers to actively contribute.¹¹ Today the Kernel is celebrated as the most important open source project in history, not only running on desktops, smartphones, routers, web servers, supercomputers, TVs, refrigerators, tablets and even the stock market (London, NY, Johannesburg, etc.), but in many areas being the undisputed leader.¹²
- 10 Legally, the Kernel may be regarded as a “composite work”¹³ comprised of Linus Torvalds’ original code with extensions and modifications contributed by other developers.¹⁴ Torvalds thus holds the copyright

of the composite work.¹⁵ As such, he can “distribute and reproduce”¹⁶ the contributions as part of the composite work. However, he cannot modify or re-license the code under any license that goes against the rules of the individual works, nor can he defend possible violations in a court of law. To date every contributor is asked to provide his patches under the GPL v. 2, which is incompatible with many other outbound licenses including the GPL v. 3. Consequently, Torvalds or any other successor is not able to re-license – i.e. change – the outbound license or defend possible violations in a court of law unless he obtains the permission of all contributors in the form of contributor agreements.

- 11 But Torvalds vehemently refuses to adopt contributor agreements

not because they allow organizations to re-license, but because the copyright assignment paperwork ends up basically killing the community. Basically, with a CLA, you don't get the kind of “long tail” that the kernel has of random drive-by patches. And since that's how lots of people try the waters, any CLA at all – changing the license or not – is fundamentally broken.¹⁷

- 12 Linus emphasizes that the Kernel benefits from many “drive-by-developers” who would be deterred if they were requested to sign contributor agreements before being able to submit a patch. It would further mean a disproportionate administrative outlay for Linus lieutenants. The “trusted lieutenants”¹⁸ are roughly a dozen hackers responsible for maintaining a part of the Linux Kernel. Many developers send their patches directly to them instead of Linus.

II. Perl

- 13 The general-purpose Unix scripting language Perl is in a similar situation.
- 14 Perl was originally developed by Larry Wall in 1987 and published under the Artistic License v. 1,¹⁹ an open source license, likewise developed by Larry Wall. Thousands of programmers used and improved Perl, turning it into one of the most widely known open source programming languages.²⁰
- 15 The development process is overseen by Larry Wall and a small group of main developers called the “pumpkins”. They make the day-to-day decisions on where Perl should go and make releases. Below that are the people with commit access to the repositories, who filter and apply patches and changes. Beyond that are the general community and contributors who submit patches and participate in the mailing lists.²¹
- 16 In the year 2000, Larry Wall and Alison Randall, decided to redesign Perl v. 5 and adapt it to the challenges of the 21st century. They attempted to

migrate the project from the Artistic License v. 1 to v. 2, which was a legally overseen re-draft of version 1, and to convince every contributor to sign a CLA. However, instead of redesigning Perl 5, Perl 6 turned into a completely new language with a completely new developer community. This was largely due to the fact that most Perl 5 developers, estimated at around 500,000, refused to agree to a license change and boycotted the signing of CLAs.²² As a result of the Perl language split, Perl 5 continues to be developed, now having arrived at v. 5.18, and Perl 6 has multiple implementation projects such as Rakudo Perl, which is based on Parrot and NQP (Not Quite Perl).²³ In order to be able to contribute to Perl 6, developers are required to sign a CLA, whereas developers of Perl 5 continue to follow the inbound=outbound approach.

III. LLVM

- 17 LLVM (formerly Low Level Virtual Machine) is a compiler infrastructure written in C++ designed for compile-time, link-time, run-time and “idle-time” optimization of programs written in arbitrary programming languages. Languages with compilers that use LLVM include ActionScript, Ada, D, Fortran, OpenGL Shading Language, Haskell, Java bytecode, Julia, Objective-C, Python, Ruby, Rust, Scala and C#.²⁴
- 18 The LLVM project started in 2000 at the University of Illinois at Urbana-Champaign as a research infrastructure to investigate dynamic compilation techniques for static and dynamic programming languages. It was released under the University of Illinois/NCSA Open Source License, a non-copyleft license.²⁵
- 19 The LLVM project managers decided against introducing contributor agreements and reasoned as follows:

The LLVM project does not require copyright assignments, which means that the copyright for the code in the project is held by its respective contributors who have each agreed to release their contributed code under the terms of the LLVM License.

An implication of this is that the LLVM license is unlikely to ever change: changing it would require tracking down all the contributors to LLVM and getting them to agree that a license change is acceptable for their contribution. Since there are no plans to change the license, this is not a cause for concern.

As a contributor to the project, this means that you (or your company) retain ownership of the code you contribute, that it cannot be used in a way that contradicts the license (which is a liberal BSD-style license), and that the license for your contributions won't change without your approval in the future.²⁶

IV. Outlook

- 20 The outbound = inbound approach is the very nucleus of open source programming. It was Stallmann's vision to free software development from appropriation through copyrights and patents.²⁷ To achieve this aim he developed a copyright license, the General Public License (GPL), which drew on the existing copyright regime to ensure exclusive rights for the public at large and not just for the original copyright holder. The only condition he imposed was that any derivative works and combinations of GPL licensed code should also be published under the GPL. For that reason the GPL has often been referred to as "viral".²⁸
- 21 This virality helped volunteer communities come together on an informal basis to exchange ideas and build upon each other's work,²⁹ resting assured that this collective work and the license behind it would be enforced by the courts.³⁰
- 22 The above projects were initiated during a *Zeitgeist* of free procreation of code – formalities such as contributor agreements were unknown. Companies were still sceptical, but allowed a couple of developers to write code in their working time if that saved money or raised efficiency. As a result, there is now an enormous user and developer base.
- 23 The management of these projects knows that they would be able to manage the projects much more efficiently by holding, or having particular usage rights, of the individual copyrights. However, this dilemma is accepted as given, since the administrative burden of introducing contributor agreements would hinder creativity and the acquisition of "eyeballs"³¹ for effective bug detection.
- 24 This approach is thus perfectly acceptable for young and small projects wanting to test the ground and explore their creativity. Should the project take off, there is no obstacle to commercialization as such, if no contributor agreements have been requested – it all depends on the outbound license used.³²
- 25 According to *Schaarschmidt et al.*,³³ the outbound = inbound approach is also suitable for R&D alliances not interested in paying expensive lawyers for drafting complicated contracts on the distribution of the intellectual property rights of the ensuing products.³⁴ Instead, everything is regulated by the public license. Thereby the completed product belongs to the community, and its source is open and visible for everybody. Depending on the nature of the public license, firms can practise open innovation protection to different degrees: should they use a strong copyleft outbound license, e.g. the AGPL or the GPL, they are no longer able to market their investment directly; however, the competition is also barred from doing so. Should they, on the other hand, use a permissive license, e.g. Apache or BSD, all parties can appropriate the code and include it into commercial products without having to share their changes with the public.³⁵
- 26 Contributor agreements only become relevant when it comes to the management of the project, e.g. the ability to re-license the code under a different public license, to sublicense the code under a certain trademark or the ability to enforce possible violations in a court of law.
- 27 In theory, a project could also decide to introduce contributor agreements at a later stage. KDE, for instance, introduced its Fiduciary License Agreement (FLA) nearly ten years after its first release.³⁶ This is unproblematic where the number of committers is manageable. But for very big projects, it requires sure instincts to know when the crossroads is reached after which the perceived benefit of having contributor agreements is outweighed by the burden of seeking out untrackable developers. The latter, however, should apply to only a very small percentage of projects, given that less than 10% of all projects have more than 1,000 active committers at any given time. Most projects have only one to three committers.³⁷
- 28 It may thus be concluded that certain projects, in this paper exemplified as Linux, Perl or LLVM, made a conscientious choice of not introducing contributor agreements in order to save on administrative resources and open the door for a flourishing community of developers. Due to their tremendous size, however, a change in the managerial approach is no longer conceivable. Smaller projects, by contrast, always have the choice of starting out without contributor agreements and introducing them at a later stage, should this be desirable.

D. Projects That Actively Manage the Intellectual Property of Contributions Through Contributor Agreements

- 29 For other projects, legal certainty, ability to enforce or flexibility to use the code outweigh the outbound licensing terms outweigh the administrative burden.
- 30 Those projects are governed by
1. foundations,
 2. development partnerships (co-operatives) and
 3. individual companies (single-vendor projects).
- 31 A selection of those projects shall be presented below.

I. Foundations

1. The FSF

- 32 Although Stallmann may be regarded as the forefather of the “inbound= outbound” approach, he soon abandoned this path for his own projects. He believed that the ability to re-license the code and enforce the GPL terms in a court of law³⁸ were fundamental to ensure a defensive free software regime.
- 33 To that end he created the Free Software Foundation (FSF), a neutral organization entrusted with the administration and enforcement of the copyrights in the ensuing collaborative works. In order for the FSF to become copyright holder of these works, each contributor is asked to sign a Contributor Assignment Agreement (CAA) transferring his ownership rights in the respective contribution to the foundation. For some GNU packages,³⁹ the FSF does not accept contributions of developers who have not signed a CAA. Problematic in this respect is that some jurisdictions do not accept outright transfers of ownership in copyright,⁴⁰ rendering the CAA in those jurisdictions most probably unenforceable.⁴¹
- 34 This problem is most salient in Europe, where the FSFE,⁴² a sister organization of the FSF, provides legal support for developers and project managers.

KDE e.V.

- 35 A prominent protégé of the FSFE is KDE, e.V., whose community builds the graphic user interface (desktop) for Linux- or Unix-based operating systems.⁴³
- 36 KDE is the prototype of a community-initiated project. Ever since the project started, the community has been driven by the creativity of the volunteers who contribute to the project. The administrative affairs of KDE are governed by the board, but there is no steering or central control for the development direction. The freedom of the code and independence of the developers is paramount.⁴⁴
- 37 KDE licenses the ensuing code under the LGPL for the core framework and the GPL for applications ensuring that the code remains open for the community and is not appropriated by a third party.⁴⁵ Although the software produced in this way is not marketable as such, many businesses provide support, services and training around the freely downloadable software. Famous examples constitute the distributors Mint, Kubuntu and Debian.⁴⁶
- 38 In line with the FSF(E)’s ideals, KDE e.V. takes up the role of fiduciary for its developers and asks, but does not compel, everybody to sign a Fiduciary License

Agreement (FLA). This agreement is *strictu sensu* a CAA, since it triggers the transfer of ownership of the contribution to KDE. But it also has a fall-back clause: should ownership in the copyright not be transferable due to compulsory national laws, an exclusive license is granted.⁴⁷

§ 1 Grant

[..]Beneficiary assigns to KDE e.V. the Copyright in computer programs and other copyrightable material world-wide, or in countries where such an assignment is not possible,

grants an exclusive licence, including, inter alia:

1. the right to reproduce in original or modified form;
2. the right to redistribute in original or modified form;
3. the right of making available in data networks, in particular via the Internet, as well as by providing downloads, in original or modified form;
4. the right to authorize third parties to make derivative works of the Software, or to work on and commit changes or perform this conduct themselves.

- 39 As a fiduciary, KDE is interested in sustaining the project and ensuring its longevity. Accordingly, two main tools are necessary to achieve this aim: the ability to 1) re-license⁴⁸ and adapt the project to new technological circumstances and 2) defend the project and its developers in its own name.⁴⁹

§ 3 K DE e.V.’s Rights and Re-Transfer of Non-Exclusive Licence

KDE e.V. shall exercise the granted rights and licences in its own name. Furthermore, KDE e.V. shall be authorized to enjoin third parties from using the software and forbid any unlawful or copyright infringing use of the Software, and shall be entitled to enforce all its rights in its own name in and out of court. KDE e.V. shall also be authorized to permit third parties to exercise KDE e.V.’s rights in and out of court.

- 40 KDE, in line with the FSFE, chose CAAs, or exclusive licenses, because it believes that simple, non-exclusive CLAs are not as effective when going to court or trying to re-license.⁵⁰
- 41 The former has recently been confirmed by Engelhardt.⁵¹ The latter, however, is being circumvented expressly and impliedly by other projects discussed below, an indication that in the absence of common standards and/or judicial precedents, legal uncertainty as to the effects of CAAs and CLAs is still common.

2. The Open Source Initiative (OSI)

- 42 With the birth of the OSI⁵² and the proliferation of public licenses, the open source business model grew popular with companies that had previously been sceptical and hostile due to the viral effect of the free software. Permissive licenses, such as the Apache or the BSD license, however, encouraged companies interested in displacing established

software companies to form alliances or sponsor open source projects.⁵³

- 43 As some of these companies were fierce competitors,⁵⁴ the idea to outsource the administrative affairs and intellectual property issues for the ensuing product to a neutral, non-profit organization began to gain momentum.

a.) Apache

- 44 One of those organizations is Apache, a US 501(c)(3) non-profit corporation which provides organizational, legal and financial support for a broad range of over 140 open source software projects.⁵⁵

- 45 Projects that have been admitted as Apache projects are promoted under the Apache license, a permissive license that allows companies to take the open source infrastructure, change it and subsume it into closed source projects. The Apache license, for instance, would be recommendable for the development of a reference implementation for a standard.⁵⁶ Thereby the competition is shifted from the infrastructure market to the market for applications and complementary products.⁵⁷

- 46 Companies or individual developers engage in particular Apache projects because they are interested in supporting the quality of the Apache trademark. It allows them to vouch for the openness and quality of the software they use within their end-products.⁵⁸ Some, in turn, contribute for intrinsic reasons, wanting to give something back to the community.

- 47 Since Apache caters for many commercially oriented companies that form R&D alliances under its auspices, it has a strong interest in being able market the code under its trademark and vouch for the provenance of the code. As such, a prerequisite of becoming a committer and being able to submit patches is to sign an Individual⁵⁹ Contributor License Agreement (ICLA).⁶⁰

- 48 Apache rejects CAAs as these are difficult to obtain.⁶¹ The companies for which most individual developers work do not want to part with the intellectual property of the individual contributions in case they are patentable or otherwise commercially applicable.⁶²

- 49 Through the CLA, however, they retain the intellectual property rights, and grant Apache:⁶³

a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, sublicense, and distribute [their] Contributions and such derivative works.

There is, however, no explicit right to enforce the copyright in a court of law. This may be explained with the fact that Apache, and projects that follow Apache's example, are not too keen to be involved in copyright infringement claims.⁶⁴ Since the code is designed to be used within proprietary products, all that is required is a copyright notice and the preparedness to provide the source code upon request. Hitherto cease and desist letters were sufficient to secure this outcome.

Since non-exclusive licenses do not automatically confer standing in a court of law, however, it might be recommendable to include such a right expressly in a CLA, simply to be in the position to sue should it become necessary at some point.

II. Development Partnerships (Co-operatives)

- 50 More and more (commercial) software customers are dissatisfied with what they perceive as “vendor lock-in” and join forces to commission open source software solutions that replace individually grown strategic IT systems and are flexible enough to meet the challenges of the future.

- 51 These alliances are generally organized as development partnerships or co-operatives in a specific economic area.

- 52 Particularly problematic is e.g. the maintenance and development of energy and water networks⁶⁵ in light of the transition from the fossil fuel and nuclear energy age to the solar and efficient energy age (*Energiewende*). This is largely due to the fact that the IT-systems landscape dates back to a time when software developers designed monolithic, proprietary systems that were unable to interact with each other or allow for new functionalities without exposing the providers to considerable expenses.

- 53 A solution is the commissioning of open source solutions which use service-oriented architecture (SOA) to break the monolithic software incrementally and integrate it as separate components.

- 54 Other fields include e.g. the automotive industry in the form of AUTOSAR,⁶⁶ which is an open and standardized automotive software architecture jointly developed by automobile manufacturers, suppliers and tool developers whose objective is to create and establish open standards for automotive E/E (Electrics/Electronics) architectures.⁶⁷

- 55 Such user co-operatives place orders with different IT providers who develop new functionalities and/or cross-system interfaces. In order to avoid future vendor lock-in, a prerequisite is the transfer of copyrights in the developed work to the user co-operative in the form of a CAA, akin to a “quasi-

employment relationship". Since research in this area is still in its infancy, and details as to the exact wording of the CAA are being held confidential, no further information could be retrieved.⁶⁸

III. Individual Companies (Single Vendor Open Source Software Project)

- 56 Single-vendor commercial open source software projects are projects that are owned by a single firm that derives a direct and significant revenue stream from the software. Using a single-vendor open source approach, firms can get to market faster with a superior product at lower cost than possible for traditional competitors.⁶⁹
- 57 Where a firm decides to open-source previously closed source software (firm-initiated – single vendor project),⁷⁰ it will most certainly want to be able to have the intellectual property rights in the contributions in order to effect different commercialization strategies and business models.⁷¹
- 58 Single vendors thus tend to use GPL licenses and request extensive contributor agreements in the form of CAAs or CLAs that allow them to pursue a dual licensing strategy.⁷² This approach is particularly smart since code developed under the GPL does not normally lend itself to being commercialized in different ways. The traditional business model around GPL licensed code is the provision of support, services and training, as offered by the Linux distributor Red Hat. Due to the viral nature of the GPL, it is impossible to include GPL-licensed code in proprietary products. The dual licensing strategy, however, opens new revenue streams for the initiating firm by e.g.
- 59 including the code in proprietary products of their own and selling commercial licenses to competitors.

1. CAA or CLA?

- 60 A widespread belief is that in order to be able to sublicense GPL-licensed code under any license, including commercial licenses, there would have to be an outright transfer of ownership in the form of a CAA.
- 61 Many projects therefore choose an outright transfer of ownership – including the fall-back option of granting an exclusive license should local copyright laws not allow a straight transfer of ownership.⁷³ Others, however, bend the wording of a CLA to the extent they reserve the rights normally only attainable under a CAA. An example of the former approach is ETAS,⁷⁴ a company that

provides engineering services, consulting, training and support for the development of embedded systems for the automotive industry; an example for the latter is Digia, the owner of the programming environment QT, which will be explored later.

2. ETAS

- 62 ETAS and Robert Bosch Engineering and Business Solutions (RBEI) jointly published BUSMASTER,⁷⁵ a free open source PC software that allows for flexible modification and extensions regarding bus systems, protocols and hardware interfaces. The current BUSMASTER version is based on the preceding software tool CANvas, conceptualized, designed and developed by RBEI.
- 63 When the company decided to open source the code, they chose the LGPL, which permits the provision of proprietary add-ons that can be dynamically linked to the open source core.
- 64 In addition, they opted for a CAA based on Harmony v. 1.0.⁷⁶ The main reason for choosing the CAA was to be able to adapt the project to new circumstances, e.g. if at some point it might be beneficial for the project to be turned into an Eclipse project, there would have to be a licensing change from the LGPL to the Eclipse Public License (EPL), which are incompatible and could not be effected without the permission of all contributors.⁷⁷
- 65 Of course, owning the copyright in the contributions ETAS is automatically able to use the code in proprietary products, to defend violations in a court of law and to license the code commercially to third parties without having to explicitly state it in their CAA, although they do so:⁷⁸

We may license the Contribution under any license, including copyleft, permissive, commercial, or proprietary licenses...

- 66 The outright transfer of ownership has, however, often been criticized as too restrictive for two main reasons:⁷⁹ It bars developers (and their companies) from exploiting their contributions otherwise, e.g. by contributing to a different project, using it in a commercial distribution or applying for a patent. In addition, there is the constant danger of the project management changing its business strategy and converting the open source project into a commercial one.
- 67 In the following paragraphs these points shall be discussed, highlighting the solutions hitherto developed under Harmony v. 1⁸⁰ and as such adopted by ETAS, or where appropriate by contributoragreements.org.⁸¹

a.) The Contribution Cannot Be Exploited Otherwise

- 68 Some critics of CAAs argue that by requesting a CAA, the original developer is barred from exploiting the contribution otherwise. Particularly Apache, referred to above, stated that they chose CLAs since CAAS were too difficult to obtain. However, this point of criticism could be mitigated by providing a generous license back to the contributor. For instance, this could take the form envisaged by ContributorAgreements.org,⁸² a project dedicated at the standardization of contributor agreements:

Upon such grant of rights to Us, We immediately grant to You a worldwide, royalty-free, non-exclusive, perpetual and irrevocable license, with the right to grant or transfer an unlimited number of non-exclusive licenses or sublicenses to third parties, under the Copyright covering the Contribution to use the Contribution by all means, including, but not limited to:

to publish the Contribution,

to modify the Contribution, to prepare Derivative Works based upon or containing the

Contribution and to combine the Contribution with other software code,

to reproduce the Contribution in original or modified form,

to distribute, to make the Contribution available to the public, display and publicly perform the Contribution in original or modified form.⁸³

This license back is limited to the Contribution and does not provide any rights to the Material.

- 69 Given this wording, the developer has *prima facie* all the rights he would have had he only ever signed a CLA.
- 70 Another way forward could be a joint, independent copyright assignment. This approach allows each individual party to use the contribution as the “quasi-owner”, in the words of one interviewee:

one party can do whatever they want with licensing in the future and the other party can do whatever they want – it’s like having two separate works.⁸⁴

- 71 A famous example using joint, independent copyright assignments was Sun/Oracle:

Contributor hereby assigns to Sun joint ownership in all worldwide common law and statutory rights associated with the copyrights, copyrights application, copyright registration and moral rights in the contribution to the extent allowable under applicable local laws and copyright conventions. Contributor agrees that this assignment may be submitted by Sun to register a copyright in the contribution. Contributor retains the right to use the contribution for Contributor’s own purposes.[...]⁸⁵

b.) Project Management Might Close the Open Source Project

- 72 Unfortunately, Oracle changed its business strategy after acquiring SUN and “closed” open Solaris, an open source operating system with the ability to become a serious competitor to Linux. This left thousands of developers owning a part to an unattainable whole and evoked the anger of the community.⁸⁶

- 73 Drafters of CAAs have thus suggested ensuring that the transfer of ownership takes place only upon the condition that the project will always maintain an open source branch. For instance, this could be framed as follows:

As a condition on the exercise of this right [to use the contribution under any license], We agree to also license the Contribution under the terms of the license or licenses which We are using for the Material on the Submission Date⁸⁷

- 74 This approach was suggested by Harmony’s CAA v. 1.0 and is currently used by ETAS.

- 75 ETAS thus reserves the right to use the contribution under any license; however, it grants a broad license back to the developer and ensures there will always be a branch under the LGPL, the open source license in force on the submission date.

3. Digia

- 76 Another approach might be the use of a CLA reserving far-reaching rights. A prominent example is Digia,⁸⁸ the owner of the programming environment QT.⁸⁹ Digia is a Finnish company which not only provides commercial support, services and training around QT, but also distributes the GPL-licensed code under commercial licenses.⁹⁰ These allow interested parties to modify and extend the code without having to make the changes available to the public. Digia requires every developer to sign a CLA in which he agrees to license his contribution and give Digia a

sublicensable, irrevocable, perpetual, worldwide, non-exclusive, royalty-free and fully paid up copyright and trade secret license to reproduce, adapt, translate, modify, and prepare derivative works of, publicly display, publicly perform, sublicense, make available and distribute (the) Licensor’s Contribution(s) and any derivative works thereof under license terms of Digia’s choosing including any Open Source Software license.

- 77 Digia is thus granted a non-exclusive license which conveys the right to sublicense and make available the code under any license of Digia’s choosing, i.e. a right to re-license may also be inferred.

- 78 Digia is further aware that a multi-licensing business model is not feasible without being in the position to

pursue enforcement of the code in front of a court of law:

3.5 Enforcement Authorization

The Licensor hereby authorizes, and agrees to execute without undue delay any and all documents reasonably necessary to effect such authorization, for Digia to enforce the Licensor's copyrights in and to a Licensor Contribution on the Licensor's behalf against any third parties as Digia at its discretion deems appropriate, at Digia's expense.

In jurisdictions where such authorization is not possible under mandatory applicable law, the Licensor hereby undertakes upon Digia's request and at Digia's expense, to act jointly with Digia (as a co-plaintiff) in enforcing the Licensor's copyrights,[...]'⁹¹

- 79 In line with *Engelhardt's* assumptions that a non-exclusive license does not per se confer standing in a court of law, Digia expressly reserves the rights to have standing to defend possible violations in a court of law. Had Digia chosen a CAA, it would not have had to make these rights explicit.
- 80 Digia thus assumes it can obtain the same rights conveyed by an outright transfer of ownership through a CLA if they are expressly listed therein. Whether this is truly the case has not yet been tested.
- 81 It is also important to note that critics condemn far-reaching CLAs to the same extent as CAAs elaborated above. Although a CLA allows a contributor to otherwise exploit the contribution, there is always the danger of a single vendor abandoning the open source project and leaving a developer with a part to an unattainable whole. For CLAs it is therefore equally important to include a clause stating that any license grant takes place upon the condition that the project will always remain under a free and open source license.
- 82 From the aforesaid, one may conclude that there is a variety of foundations/cooperatives and single vendor open source businesses with contrasting ethos using different CAAs and CLAs for differing purposes.
- 83 Upon a closer look, however, it becomes clear that despite having different agendas, parties of contributor agreements generally have the same aim: owners want to be able to perform all acts exclusively reserved for copyright owners under copyright law, i.e. copy, distribute, modify and communicate to the public, but most importantly they want to be able to re- and sub-license the code to third parties, in some cases even under a different outbound license, and to defend possible violations in a court of law.
- 84 Developers in turn want to retain the right to use the contribution in another project, possibly even in a commercial application or even a patent, and be sure that the open source project will always remain under a free and open source license and not become a victim of a business strategy change.
- 85 Since there is no accepted standard definition of what a contributor agreement should contain in order to have a particular effect, legal departments constantly re-invent the wheel and draft contributor agreements either based on outdated assumptions or adventurous developments of the law. These reduce the understandability and add to the confusion and distrust of developers and their respective employers.
- 86 It might thus be time to start thinking about a standardization effort by means of an open source contributor agreement platform, where interested parties come together and decide what infrastructure should underlie every contributor agreement. These parties should include developers, project managers, product managers and lawyers.
- 87 It should have a modular architecture, so that interested parties could add individual conditions and rights depending on their particular needs. All of these modules would be endorsed by a legally qualified committee, thus ensuring that the use of a contributor agreement of said format would be a qualitatively high legal document produced in the transparency of the open source process.

E. Conclusion

- 88 To conclude, it is safe to say that the divide between projects which use outbound as inbound and those which actively manage intellectual property rights is (currently) here to stay.
- 89 It would be tilting against windmills to try to convince the unconvinced of using contributor agreements of any sort. Neither the standardization nor possible automatization of rights management is in these projects' interest as it would mean an increased administrative burden, i.e. costs, which would be difficult to raise.⁹²
- 90 On the other hand, more and more projects have an interest in being able to actively manage the intellectual property of their contributions. Due to the lack of a common standard, however, legal departments constantly re-invent the wheel, resulting in a very unhomogenous contributor agreement landscape, prone to distrust and criticism.
- 91 The current paper thus proposes a standardization effort, using the very same open source method to

create an acceptable infrastructure for understandable and effective contributor agreements.

- 1 Perl Foundation, <http://www.perlfoundation.org/>, Linux Foundation, <http://www.linuxfoundation.org/>, Mozilla Foundation, <https://www.mozilla.org/en-US/foundation/>, accessed 16 May 2014.
- 2 Busmaster of ETAS, http://www.etas.com/de/products/applications_busmaster.php, accessed 16 May 2014.
- 3 Maracke, C., Editorial: Copyright Management for open collaborative projects: Inbound Licensing Models for open Innovation, Volume 10, Issue 2, August 2013, p. 143, <http://script-ed.org/wp-content/uploads/2013/08/editorial.pdf>, accessed 7 May 2014.
- 4 Maracke, C., Metzger, A., Concept Paper: Network of Stewards for Free and Open Source Software projects, p. 2, http://contributoragreements.org/wp-content/uploads/2013/05/ConceptPaper_NetworkV9_Abstract.pdf, accessed 16 May 2014.
- 5 Famous examples constitute e.g. the Linux Kernel, Perl 5 or the LLVM Project .
- 6 Much research on the topic is conducted in the field of computer science and economics; see e.g. Riehle, D. Three Positions on the Future of Open Source Research, p. 2, <http://dirkriehle.com/wp-content/uploads/2010/01/FOSS-2010-Position-Paper.pdf>, Controlling and Steering Open Source Projects, IEEE Computer Society, July 2011, p. 94.
- 7 A full transcript of any given interview may be available upon request: sylviajakob@live.de.
- 8 Riehle, D., Friedrich – Alexander University of Erlangen (Nürnberg, Germany).
- 9 Corbeth, J., Kroah-Hartman, G. & McPherson, A., Linux Kernel Development: How Fast It Is Going, Who Is Doing It, What They Are Doing, and Who Is Sponsoring It, A white paper by the Linux Foundation, 2009, <http://www.linuxfoundation.org/sites/main/files/publications/whowriteslinux.pdf>, accessed 14 May 2014.
- 10 <https://groups.google.com/forum/#lmsg/comp.os.minix/dlNtH7RRrGA/SwRavCzVE7gJ>, accessed 4 June 2014.
- 11 <http://web.archive.org/web/20110721105526/http://www.kernel.org/pub/linux/kernel/Historic/old-versions/RELNOTES-0.12>, accessed 4 June 2014.
- 12 Contreras, F., Why the Linux Kernel is the most important project in history, <http://felipec.wordpress.com/2011/03/06/why-linux-is-the-most-important-software-project-in-history/>, accessed 16 April 2014.
- 13 17 U.S.Code § 201 c).
- 14 Linus as copyright holder of the composite Linux Kernel: http://yarchive.net/comp/linux/collective_work_copyright.html, accessed 20 May 2014.
- 15 Discussion of Contributor Agreements between Linus Torvalds, Greg Kroah-Hartmann & others on Google + on 20 January 2014, <https://plus.google.com/111049168280159033135/posts/NstZfwXbAti>, accessed 2 April 2014.
- 16 17 U.S.Code § 201 c) other jurisdictions?
- 17 Discussion of Contributor Agreements between Linus Torvalds, Greg Kroah-Hartmann & others on Google + on 20 January 2014, <https://plus.google.com/u/0/111049168280159033135/posts/NstZfwXbAti>, accessed 2 April 2014.
- 18 Dafermos, G., On the fourfold structure, http://p2pfoundation.net/Linux_-_Governance, accessed 16th April 2014
- 19 <http://opensource.org/licenses/Artistic-1.0>, accessed 16 April 2014; see further Jacobsen v. Katzer for the enforceability of the Artistic License, <http://www.cafc.uscourts.gov/images/stories/opinions-orders/08-1001.pdf>, accessed 16 April 2014.
- 20 Large projects written in Perl include cPanel, Slash, Bugzilla, RT, TWiki, and Movable Type; high-traffic websites that use Perl extensively include bbc.co.uk, [Priceline.com](http://priceline.com), [Craigslist](http://craigslist.com), [IMDb](http://imdb.com), [LiveJournal](http://livejournal.com), [DuckDuckGo](http://duckduckgo.com), [Slashdot](http://slashdot.com) and [Ticketmaster](http://ticketmaster.com). It is also an optional component of the popular LAMP technology stack for web development, in lieu of PHP or Python; see <http://en.wikipedia.org/wiki/Perl>, accessed 16 April 2014.
- 21 http://www.perlfoundation.org/how_tfp_works, accessed 16 March 2014.
- 22 Perl Foundation President, personal communication, August 2013.
- 23 http://en.wikipedia.org/wiki/Perl_6.
- 24 <http://en.wikipedia.org/wiki/LLVM>.
- 25 <http://llvm.org/>.
- 26 <http://llvm.org/docs/DeveloperPolicy.html>, accessed 16 April 2014.
- 27 Jaeger/Metzger, Open Source Software, Rechtliche Rahmenbedingungen der Freien Software, 3. Auflage, Verlag C.H. Beck, 2011, p.12.
- 28 See e.g. the court in *Versata v. Ameriprise*, p. 9 <http://de.scribd.com/doc/212507936/Versata-Software-v-Ameriprise>, accessed 16 May 2014.
- 29 See e.g. Lerner & Tirole, Some Simple Economics of Open Source, THE JOURNAL OF INDUSTRIAL ECONOMICS 0022-1821, Volume L, June 2002 No., p. 201,202, <http://onlinelibrary.wiley.com/doi/10.1111/1467-6451.00174/pdf>, accessed 15 June 2013, Gonzales- Barahona, J.M., Robles, G., Trends in Free, Libre, Open Source Communities: From Volunteers to Companies, IT 55 (2013) 5, Oldenbourg Wissenschaftsverlag, p. 173- 180, p. 174.
- 30 See e.g. <http://www.pro-linux.de/news/1/11486/gerichtskype-verletzt-die-gpl.html>, accessed 16 May 2014.
- 31 Famous quote of Raymond, E.S.: “Given enough eyeballs, all bugs are shallow” (Linus’ Law), in *The Cathedral and the Bazaar*, 1999, p. 22
- 32 Where a strict copyleft license is used, for instance the AGPL, the code cannot be incorporated into closed source products, but many other business models can be pursued. Where a weak copyleft outbound license has been used, for instance the BSD license, any sort of commercialization is allowed.
- 33 Schaarschmidt, M., Bertram, M., Zerwas, D.& Kortzfleisch, H., Kommerzialisierungsansätze in Open Source Software Projekten, HMD, 283, p. 6-16, p. 12, <http://download.springer.com/static/pdf/209/art%253A10.1007%252FBFB03340658>.
- 34 See e.g. AMQP.org, an alliance of blue chip companies that developed an advanced message queuing protocol, which was recognised as an international standard and does not request CAs of any sort: <http://www.amqp.org/>, accessed 16 May 2014.
- 35 See e.g. the Apache License v. 2, <http://oss-watch.ac.uk/resources/apache2> or the BSD license <http://oss-watch.ac.uk/resources/modbsd>, accessed 15 May 2014.
- 36 “At the General Assembly of KDE e.V. in August 2008 the membership voted to adopt a Fiduciary Licensing Agreement as the preferred form for assigning copyright to KDE e.V.: <http://ev.kde.org/rules/fla.php>, accessed 24 June 2014.
- 37 <http://bit.ly/1Bk5Vld>
- 38 Metzger, A., Internationalisation of FOSS contributory Copyright Assignments and Licenses: Jurisdiction-Specific or “Unported”, SCRIPTed, Vol. 10, Issue 2, August 2013, p. 178-206, p. 179.
- 39 Metzger, A., Internationalisation of FOSS Contributory Copyright Assignments and Licenses: Jurisdiction-Specific or “Unported”, SCRIPTed, Vol. 10, Issue 2, August 2013, p. 178-206, p. 179.

- 40 See e.g. § 29 German Copyright Law.
- 41 <https://fsfe.org/work.en.html>, accessed 14 May 2014.
- 42 <https://fsfe.org/index.de.html>, accessed 14 May 2014.
- 43 <http://www.kde.org/>, accessed 15 April 2014.
- 44 Former Board Member of KDE, Mirko Boehm, personal communications, September 2013.
- 45 Ibid.
- 46 <http://www.kde.org/download/distributions.php>, accessed 12 May 2014.
- 47 <http://ev.kde.org/resources/FLA-prefab.pdf>, accessed 24 February 2014.
- 48 <http://ev.kde.org/resources/FRP.pdf>, accessed 24 February 2014.
- 49 <http://ev.kde.org/resources/FLA-prefab.pdf>, accessed 24 February 2014.
- 50 Legal Counsel, FSFE, personal communication, October 2013.
- 51 Engelhardt, T., Drafting Options for Contributor Agreements for Free and Open Source Software: Assignment, (Non) Exclusive Licence and Legal Consequences. A Comparative Analysis of German and US Law, SCRIPTed, Volume 10, Issue 2, August 2013, p. 148-176, p. 164-65.
- 52 <http://opensource.org/>, accessed 14 March 2014.
- 53 Riehle, D., The economic case for Open Source Foundations, IEEE, January 2010, p. 86-90, p. 88.
- 54 Barahona-Gonzales, J., Trends in Free, Libre, Open Source Software Communities: From Volunteers to Companies, IT, 55 (2013) 13, p. 173-180, p. 175, Oldenbourg Wissenschaftsverlag.
- 55 <http://projects.apache.org/>, accessed 27 January 2014.
- 56 The standardization of the Java Portlet Specification 3.0 under the sponsorship of IBM is being developed, at least in parts, under the auspices of the Apache Foundation.
- 57 Personal communications with Java Portlet Specification Manager, Martin Scott Nicklous, August 2013.
- 58 Riehle, D., Controlling and steering open source projects, IEEE Computer Society, July 2011, p. 96.
- 59 <https://www.apache.org/licenses/icla.txt>, accessed 7 March 2014.
- 60 For those who are employed by a particular company, the employer has to sign a Corporate CLA (CCLA): <http://www.apache.org/licenses/cla-corporate.txt>, accessed 7 March 2014.
- 61 Personal communication with board member of the Apache Foundation, Bertrand Delacretaz, August 2013.
- 62 Ibid.
- 63 <https://www.apache.org/licenses/icla.txt>, accessed 24 February 2014.
- 64 Personal communication with Apache board member Bertrand Delacretaz, August 2013, and Django Foundation President, Russell Keith-Maggee, October 2013.
- 65 Herdt, P., Konsortiale Software Entwicklung im Energiesektor, <http://www.osbf.eu/blog/konsortiale-open-source-softwareentwicklung/im-energiesektor/#.U3ZGG1d-r6M>, 26 November 2013, accessed 15 March 2014.
- 66 AUTomotive Open System Architecture, <http://www.autosar.org/>, accessed 15 April 2014.
- 67 <http://en.wikipedia.org/wiki/AUTOSAR>, accessed 16 May 2014.
- 68 Herdt, P., supra, p. 6
- 69 Riehle, D., The commercial open source business model, <http://dirkriehle.com/publications/2009-2/the-commercial-open-source-business-model/>, accessed 18 November 2013.
- 70 Riehle, D., The single vendor Commercial Open Source Business Model, Information Systems and e-Business Management archive, Volume 10 Issue 1, March 2012, p. 5-17, p. 5.
- 71 Schaarschmidt et al., supra, p. 11.
- 72 See also Comino, S. & Manenti, F.M., Dual licensing in Open Source Software markets, http://www.webmeets.com/files/papers/EARIE/2009/244/CominoManenti_Dual_licensing.pdf, accessed 10 May 2014.
- 73 See KDE supra.
- 74 ETAS, <http://www.etas.com/en/index.php?langS=true&>, accessed 16 May 2014.
- 75 BUSMASTER, http://www.etas.com/en/products/applications_busmaster.php?langS=true&, accessed 16 May 2014.
- 76 CAA, https://raw.githubusercontent.com/rbei-etas/busmaster-documents/master/contributor_agreement_entity.pdf, accessed 24 November 2013.
- 77 Personal communication with the product manager of BUSMASTER, Dr. Tobias Lorenz, August 2013.
- 78 CAA, see note 73.
- 79 Personal communications with several stakeholders, August – October 2013.
- 80 <http://harmonyagreements.org/>, accessed 14 February 2014.
- 81 <http://contributoragreements.org/>, accessed 16 May 2014.
- 82 Ibid.
- 83 <http://development.contributoragreements.org/>, accessed 16 May 2014.
- 84 Personal communication with economist/ IT consultant, Joseph Potvin, Canada, August 2013.
- 85 <https://www.openoffice.org/licenses/jca.pdf>, accessed 16 May 2014.
- 86 Personal communication with IT student, Jens Kadenbach, August 2013, backed up by <http://www.cnet.com/news/oracle-apparently-shuts-doors-on-opensolaris/>, accessed 20 October 2013.
- 87 <http://harmonyagreements.org/>, accessed 16 May 2014.
- 88 <http://qt-project.org/>, accessed 16 May 2014.
- 89 <http://www.digia.com/>, accessed 16 May 2014.
- 90 <http://www.digia.com/en/Home/Company/Press/2012/Digia-to-acquire-Qt-from-Nokia/>, accessed 16 May 2014.
- 91 <http://qt-project.org/legal/QtContributionLicenseAgreement.pdf>. An interesting twist in Digia's licensing terms is the granting of "consideration", which turns the CLA prima facie into a sale; see ECJ in *Usedsoft v. Oracle*, C 128/11).
- 92 Just think of the 500,000 Perl 5 developers.

Proportionality of Website Blocking:

Internet Connectivity Providers as Copyright Enforcers

by **Pekka Savola***, Lic.Sc.(Tech.), Master of Laws, LL.D. candidate. Legal Counsel at CSC–IT Center for Science Ltd, Researcher at University of Helsinki, Finland,

Abstract: Internet connectivity providers have been ordered to block access to websites facilitating copyright infringement in various EU countries. In this paper, the proportionality of these enforcement measures is analysed. After addressing preliminary questions, the recent CJEU ruling UPC Telekabel Wien (C-314/12) and then case law from all Member States are examined from the perspective of proportionality. Finally, five criteria are submitted for proportionality analysis, and a proportionality evaluation

is provided. The major observation is that the underlying goal of copyright enforcement has implications on how the scale tilts. In particular, ineffective enforcement mechanisms can be more easily accepted if the goal of symbolic, educational or politically motivated enforcement is considered legitimate. On the other hand, if the goal is to decrease the impact of infringement, higher efficiency and economically quantifiable results may be required.

Keywords: Proportionality, Fundamental Rights Conflicts, Copyright Enforcement, Website Blocking, ISP

© 2014 Pekka Savola

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Pekka Savola, Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers, 5 (2014) JIPITEC 116, para. 1.

A. Introduction

- 1 There has been an increasing tendency to oblige various kinds of intermediaries to perform web filtering and aid in enforcement.¹ This paper focuses on enforcement of specific right (copyright), target (Internet connectivity, i.e. access providers), means (court order to block access to a website) and perspective (proportionality of such order).²
- 2 Intermediaries are typically faultless third parties with respect to the dispute between right holders and infringers.³ Therefore, passive or neutral intermediaries are generally exempt from liability within varying constraints. To balance the lack of liability, a court may issue an injunction ordering—for example, to stop or prevent a specific infringement.⁴ Indeed, intermediaries are an attractive tool to enforce local policies on foreign sites.⁵ However, broad liability for activities that intermediaries cannot and need not control or monitor would result in *inter alia* stifling of innovation, preventive censorship and increased operating costs.⁶
- 3 Proportionality evaluation is depicted as three or four steps. The initial and sometimes omitted step is the *legitimacy* of the pursued objective.⁷ The first two of the three main stages are *suitability* and *necessity* of the means in achieving the objective, i.e. that the goal can be achieved and there are no better means, respectively. Third, the actual balancing part is *proportionality* in the narrow sense (*stricto sensu*), i.e. whether the burden of the means is excessive in relation to the objective sought.⁸
- 4 In this context, proportionality analysis concerns fundamental rights conflicts in national measures implementing EU legislation. Because blocking measures are unlikely to affect the fundamental freedoms,⁹ the evaluation occurs between conflicting fundamental rights. Here EU and national fundamental rights coexist, but in conflict the supremacy of EU law prevails.¹⁰ CJEU case law provides minimum and maximum standards¹¹ and guidelines that must be applied when national courts interpret EU law. Issues at stake are the effectiveness of protecting the right holders' intellectual property in contrast to the costs and limits on the freedom to conduct a business on the ISP and the limitations of

freedom of information (expression) on the users.¹² ECtHR has not made very significant rulings in this aspect.¹³ The evaluation is augmented with more intense scrutiny.¹⁴

- 5 This paper is structured as follows. Section B first discusses the differences in liability exemptions between hosting and connectivity providers, and what constitutes a general monitoring obligation. Then various parties' interests, EU IPR enforcement principles, and the effect of national legislation are briefly covered. After these preliminary questions, we move on to Section C, where the case law of CJEU and all Member States is covered from the proportionality perspective mixed with analysis and commentary. Using these as a basis, Section D formulates five criteria for assessing proportionality of website blocking. Finally, Section E provides proportionality analysis. Brief conclusions are presented last in Section F.

B. Preliminary Considerations

I. Legal Basis of Website Blocking Injunctions

- 6 Article 8(3) of the Infosoc Directive¹⁵ obliges Member States to provide a possibility for copyright injunctions against intermediaries:

Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

- 7 Per Recital 59, the conditions and modalities are to be determined in national legislation. Essentially identical provisions also exist for other intellectual property rights *in fine* of Article 9(1)(a) and 11 of the Enforcement Directive.¹⁶ Indeed, the E-Commerce Directive allows national law to provide specific injunctions against connectivity providers in Article 12(3), but on the other hand prohibits general monitoring obligations in 15(1):

[12(3)]. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

[15(1)]. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or

store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

II. Different Providers and Liability Exemptions

- 8 While Internet service providers are not liable for information transmitted or stored, they may be subject to various obligations.¹⁷ As connectivity and hosting providers provide a different kind of service, the conditions and scope of potential obligations also differ.¹⁸
- 9 The liability exemption of connectivity providers is based on neutrality, passivity and technical nature of automatic communication. According to the recital, this implies lack of knowledge and control over the transmitted information; deliberate collaboration in order to undertake illegal acts is also excluded.¹⁹
- 10 On the other hand, the exemption of hosting providers is conditional on awareness or knowledge of illegal activities or facts or circumstances from which illegality is apparent. Upon obtaining awareness of illegal material, hosting providers also need to act expeditiously to remove or disable access to it. The exemption does not apply if the provider has authority or control over the user and the content.²⁰ The awareness of facts relating to illegality appears to have been the grounds to exclude the operators of sites such as The Pirate Bay from the hosting defence; even if material on the site might not be infringing, its role in overall infringing activities has been apparent.²¹
- 11 In the latest case on hosting providers, *L'Oréal v eBay*, it was held that the operator must not have an active role allowing it to have knowledge of the data stored. To measure awareness (or "neutrality"²²), a standard of diligent economic operator was established as to when illegality should have become apparent.²³
- 12 This interpretation is inapplicable to connectivity providers, because their liability exemption is not tied to knowledge or awareness in the same manner as hosting providers.²⁴ Further, their role is more passive, neutral and automatic, and transmitted data is transitory. They also have no obligation to act upon obtaining awareness of illegality²⁵ unless explicitly required by national law as provided by Article 15(2) of the E-Commerce Directive.²⁶

III. Restrictions on General Monitoring and Orders

- 13 The prohibition against imposing monitoring obligations of a general nature applies to all kinds

of providers. Likewise, a general obligation to seek facts or circumstances indicating illegal activity is forbidden. However, monitoring (in a fairly narrow meaning) “in a specific case” by orders of national authorities is possible.²⁷ Court or administrative authority may also require termination of present or prevention of specific future infringement.²⁸ In particular, in *UPC Telekabel Wien* rather severe requirements regarding judicial review were imposed on generic orders targeting a website.²⁹ In contrast, the Advocate General had more explicitly suggested that a specific kind of generic blocking order would not amount to a general monitoring obligation.³⁰

- 14 Only hosting providers may be subjected to “duties of care” in order to detect and prevent certain types of illegal activities.³¹ National legislation may also establish procedures governing the removal or disabling of access to information (i.e. notice-and-takedown mechanisms).³² Examples of court orders to prevent future infringements in the context of hosting providers were suspending infringing users’ accounts or making user identification on the marketplace easier.³³ In national courts, there have also been “stay-down” orders, obliging the hosting provider to ensure that a specific infringement is not repeated. Unless carefully constructed, these might be disproportionate or amount to a general monitoring obligation.³⁴
- 15 All in all, the differences in the legal basis and the scope when comparing connectivity and hosting providers suggests that appropriateness of injunctions varies. Because for connectivity providers the conditions for liability exemption are broader, similar limitations could very well also apply to all types of injunctions. Depending on circumstances, it may be more proportionate and technically feasible to order a hosting provider rather than a connectivity provider to implement a certain kind of blocking. In contrast, issuing orders grounded on duties of care or knowledge assumed by a diligent economic operator at connectivity providers would not be appropriate. Also, accepting the premise of narrower injunctions, all the conditions in case law relating to hosting providers that restrict the orders (e.g. what constitutes a monitoring obligation and principles for weighing proportionality) would be *prima facie* valid. On the other hand, those conditions which expand the scope should be critically evaluated.

IV. Interests in Balancing

- 16 The following table summarizes private and public interests at stake; detailed elaboration is not possible here.

| | Private interests | Public interests |
|-----------------------|---|---|
| IPR Holder | IPR protection | Sufficient protection, innovation, policy, culture |
| Connectivity provider | Freedom to conduct a business (and protection of property) | Market economy, network neutrality |
| User | Freedom of expression (and protection of personal data) | Democracy, freedom of expression in general, culture |
| Website operator | Freedom of expression, right to fair trial (and business freedom) | Possibility to enforce national policies on foreign sites |

- 17 Intellectual property rights are not absolute, and it is impossible to completely protect them through enforcement. Therefore, trying to find the least restrictive means (LRM) to eliminate IPR infringement is misguided. This specifically applies to copyright, given the extensive exclusive rights also governing non-commercial activities, whereas in contrast e.g. trademarks or patents can be used by private individuals more freely. This was emphasised in *Scarlet Extended* and affirmed in *UPC Telekabel Wien* very explicitly as follows:³⁵

There is, however, nothing whatsoever in the wording of [Article 17(2) of Charter stating that “Intellectual property shall be protected”] or in the Court’s case-law to suggest that that [intellectual property] right is inviolable and must for that reason be absolutely protected.

- 18 A better question is to ask which degree of IPR enforcement is deemed appropriate when balanced with other issues at stake, in particular other fundamental rights.³⁶ This reflects the underlying (and unresolved) policy issue on the level and constraints of enforcement an IPR holder is entitled to.
- 19 Rather than trying to find LRM in general, one must survey the means and their trade-offs (e.g. effectiveness, costs and other impacts). Based on this analysis, the appropriate balance between certain degrees of enforcement using a specific means and other rights can be considered. In *UPC Telekabel Wien*, issuing a generic order incurred requirements to the national procedure in order to ensure proportionality evaluation.³⁷ This was noted more explicitly in the Advocate General’s Opinion that proportionality cannot be evaluated if the necessary measures could not be reviewed.³⁸

V. IPR Enforcement Principles in EU Law

- 20 The Infosoc Directive does not provide guidance on how to balance injunctions of Article 8(3).³⁹ On the other hand, Article 3 of the Enforcement Directive applies to (all) measures, procedures and remedies necessary to ensure the enforcement of IPRs covered

by the Directive. These shall be “fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays”, and also “effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.”⁴⁰

| Strong | Neutral | Weak |
|----------------|----------------------|-----------------|
| effective | fair | proportionate |
| dissuasive | equitable | not complicated |
| no time-limits | not abusable | not costly |
| no delays | no barriers to trade | |

- 21 It is challenging to realize all of these at the same time. In consequence, case-by-case balancing will be needed.⁴¹ In the preceding table these are classified as “strong” (pro-rights), “weak” (pro-users) and “neutral” principles. However, in different interpretative contexts – for example, against infringer versus a third party – the principles could have an entirely different meaning.⁴² Per Article 2(1), a Member State may provide stronger enforcement only “in accordance with Article 3”, i.e. the balance must not be upset.⁴³
- 22 Norrgård noted in 2005 that a national judge could reasonably adopt both a weak or strong enforcement ideology based on the discretion granted by the directive.⁴⁴ A balanced interpretation was suggested based on principles of Article 3, fundamental rights, context-sensitivity and the comparative method.⁴⁵ These have since then materialised in CJEU case law, and this paper also continues on that path. Similarly, Ohly has underlined the need of proportionality to balance effectiveness and dissuasiveness, referring in a similar fashion to taking due account of the specific characteristics of the case as noted in Recital 17.⁴⁶
- 23 Both directives have been geared towards infringers. Applying principles of effectiveness and dissuasiveness against a faultless intermediary is questionable.⁴⁷ Indeed, in his Opinion in *L'Oréal v eBay*, Advocate General Jääskinen was not convinced that the identical scope of injunctions available against the intermediary and the infringer would be a reasonable interpretation of Article 11 of the Enforcement Directive.⁴⁸ Similarly, the requirement for context-sensitivity would suggest caution with regard to third-party injunctions.⁴⁹ Further, the notions attached to injunctions are different and comparisons difficult between infringers and intermediaries as well as between legal systems.⁵⁰

VI. National Principles and Triggers for Evaluation

24 National law may specify the grounds for a proportionality evaluation or leave issuing the order at the court's discretion. While this may give the national court leads on what to evaluate, it is important to note that EU law provides the minimum (and maximum) level of protection to various competing rights. This will perforce affect the court's discretion and evaluation.⁵¹

25 As an example of national law,⁵² in Finnish Copyright Act (404/1961, as amended by 679/2006) Section 60c(1):⁵³

[...The] court [...] may order [...the] intermediary to discontinue [...] unless this can be regarded as unreasonable in view of the rights of the person making the material available to the public, the intermediary and the author.

26 On the other hand, many countries seem to have transposed Article 8(3) in a very minimal fashion, almost verbatim, or without substantial additional details or modalities.⁵⁴

C. Proportionality in Case Law

I. Introduction

27 The latest blocking requests targeting connectivity providers at the user end in EU/EEA are illustrated in the following table. In other EU/EEA countries, blocking has not been requested. The table notes the highest court which has made the latest decision. The rulings are final except the Netherlands (pending appeal to Supreme Court). The type of proceedings (civil and/or criminal) has also been noted.

28 “(X)” under “ruling” implies that the decision has been reversed in contrast to a lower court instance or earlier proceedings. This illustrates that while the general trend has been to order one or more ISPs to block access to a website, in some cases requests have also been rejected on various grounds. The most prominent reason for rejection (particularly in Ireland and Norway, and arguably in Germany) has been attributed to the lack of legal basis due to the implementation (or lack thereof) of Article 8(3).⁵

| Country | Site | Provider | Date | Court | Type | Ruling |
|---------|-----------|------------------|------------|-----------------|-------------|--------------|
| Spain | Other | Vodafone etc. | 16.7.2014 | Appeal | Criminal | No block (x) |
| Austria | Kino.to | UPC Telekabel | 24.6.2014 | Supreme/ CJEU | Civil | Block |
| The NL | TPB | Ziggo etc. | 28.1.2014 | Appeal (to Sct) | Civil | No block (x) |
| France | Streaming | All ISPs | 23.11.2013 | First instance | Civil | Block |
| Belgium | TPB | Belgacom etc. | 22.10.2013 | Supreme | Civil+Crim. | Block (x) |
| Ireland | TPB | UPC etc. | 12.6.2013 | First instance | Civil | Block (x) |
| Finland | TPB | TeliaSonera etc. | 11.2.2013 | Appeal | Civil | Block |
| UK | TPB etc. | All ISPs | 13.11.2013 | First instance | Civil | Block |
| Greece | Other | Vodafone etc. | 16.5.2012 | First instance | Civil | Block |
| Germany | Other | Unknown | 22.12.2010 | Appeal | Civil | No block |
| Denmark | TPB | Telenor etc. | 27.5.2010 | Supreme | Civil | Block |
| Norway | TPB | Telenor etc. | 10.2.2010 | Appeal | Civil | No block |
| Italy | TPB | All ISPs | 23.12.2009 | Supreme | Criminal | Block (x) |

29 Next, a summary of all cases is provided, with particular focus on issues relating to proportionality. The goal is to review arguments used in CJEU and national decisions as a step of formulating the criteria for balancing.

II. The Court of Justice

30 As for blocking injunctions,⁵⁶ in *L'Oréal v eBay*, it was held that courts of Member States must be able to order online marketplaces to take measures to stop current infringements as well as – if justified by the circumstances – prevent future ones. These must be effective, proportionate and dissuasive and must not create barriers to legitimate trade. The measures must also be fair and not excessively costly. A couple of examples were provided.⁵⁷ This provides little guidance in the present context.

31 *Scarlet Extended* applied the aforementioned proportionality principles to whether a connectivity provider could be ordered to install a comprehensive filtering system.⁵⁸ The system would have monitored all the data relating to all customers in order to prevent any future infringement of claimants' intellectual property rights. CJEU held that it would have constituted a general monitoring obligation in violation of Article 15(1); nonetheless, proportionality was also considered.⁵⁹ As introduced in *Promusicae*, protection of the IPR must be balanced against other fundamental rights. Specifically, the connectivity provider's freedom to conduct a business would be inappropriately balanced against the interest to protect the IPR, because the order would require installing a complicated, costly and permanent system at the provider's own expense. The cost and complicated nature of the system were also against Article 3(1) of the Enforcement

Directive.⁶⁰ The system would also be questionable from the perspective of users' data protection and freedom of expression, as it would have applied to all the communications and would also have misidentified and blocked lawful communications.⁶¹ This judgment is relevant, but given the intrusiveness of the contested filtering system, the constraints it provides for blocking orders are limited.⁶²

32 *UPC Telekabel Wien* concerned a more restricted form of blocking, only one specified site. In summary, the CJEU in principle accepted generic orders (where adopted measures are chosen by the provider), but imposed judicial review requirements that might make issuing them unattractive for national courts. This restricted the applicability of generic orders and transformed generic orders into court-approved specific orders.⁶³ The Advocate General was more straightforward and suggested rejecting them instead of crafting requirements. In the end, the essential result was the same.⁶⁴ More detailed analysis follows.

33 The CJEU held that national law must be transposed in a manner allowing a fair balance to be struck between competing interests. The law must also be interpreted in the manner that takes fundamental rights and proportionality into consideration.⁶⁵ The fundamental rights conflict was construed between Charter Articles 17(2) (IPR holders' right to property), 16 (the provider's freedom to conduct a business), and 11 (users' freedom of information).⁶⁶

34 Business freedom was characterized as *inter alia* the right to freely use the economic, technical and financial resources available to the provider. An injunction was considered to constrain the free use of resources, as it obliges taking measures which may represent a significant cost, have considerable impact on the organization of activities, or require difficult and complex technical solutions. However, such an injunction was held not to infringe on the very substance of conducting business.⁶⁷ With a generic order, the provider can choose measures that are best adapted to the resources, abilities and challenges facing it. The provider can also avoid being in breach of an order by proving at the execution stage that all reasonable measures have been taken. Specifically, no unreasonable sacrifices are required.⁶⁸ However, legal certainty was held to require that the evaluation of reasonableness – i.e. which means can be expected – is done in court prior to issuing any sanctions due to the lack of sufficient compliance.⁶⁹ Essentially, the CJEU transferred the evaluation of proportionality from the ordering phase to the execution phase, with a mandate to provide for court review. In consequence, the provider can obtain confirmation of compliance in court by first doing a minimal implementation. Very likely this will decrease the use of generic orders.⁷⁰

- 35 With generic orders and uncertainty, the A.G. had been concerned with providers opting for intrusive means, endangering users' freedom of information or facing the risk of disobeying the order.⁷¹ The CJEU's approach was to impose requirements on the adopted measures and require allowing court review for both providers and users. In particular, measures must comply with Internet users' right to freedom of information: they must be strictly targeted to end infringement, and must not affect users lawfully accessing information.⁷² The A.G. provided an example of collateral damage by referring to the ECtHR ruling *Yildirim v Turkey*, where the whole Google Sites service was blocked when only one site hosted there should have been targeted. This violated the freedom of expression guaranteed by Article 10 ECHR in various ways.⁷³
- 36 The CJEU held that national courts must be able to verify that the measures are appropriate. This may not be possible if the provider chooses the measures and their use is not contested. In consequence, in this case users must be provided *locus standi* to assert their rights before the court.⁷⁴ It is submitted that this also applies to national courts issuing specific orders, unless proportionality has also been reviewed from the users' perspective.⁷⁵
- 37 As previously noted, the IPR is not inviolable in that it must be absolutely protected. It is possible that a complete cessation of IPR infringement is not achieved, if for example some measures that would achieve the result would not be reasonable for the provider, or because means do not exist or the goal is not in practice achievable.⁷⁶ The adopted measures should still be "sufficiently effective" or at least discourage users from accessing the site and make accessing the site difficult to achieve.⁷⁷ Therefore, even if infringement is not completely prevented, the fair balance and proportionality in the light of Article 52(1) is achieved provided that freedom of information to lawful material is not unnecessarily prevented and that blocking prevents access or at least makes it difficult and seriously discouraged.⁷⁸
- 38 The CJEU's emphasis on effectiveness, a high degree of IPR protection, and the means which may place significant obligations on the provider could be read to imply that the balance should be shifted more towards IPR protection. This reading must be rejected. The CJEU appears to have taken no clear stance on the balance of protecting the IPR and business freedom.
- 39 The fourth question was whether it was proportional to order a provider to implement specific means even if these incurred significant costs and the blocking could be easily circumvented without technical knowledge. The CJEU's final answer displays naiveté or evasion, because those issues were also in the background in the third question. The problem is apparent when considering the ineffectiveness of blocking in general, and that there may not be "sufficiently effective" and "seriously discouraging" means that would not also be complicated, costly and/or too intrusive. The CJEU provided no guidance on the provider's required degree of involvement. The problem of unlawful material on a site which also includes lawful material was also not addressed. In consequence, essentially both balancing exercises (IPR holder vs provider and IPR holder vs user, respectively) were effectively deferred to national evaluation or a future referral. Therefore, the A.G.'s guidelines on the fourth question are valuable and will be used tentatively as a basis.
- 40 When assessing suitability, the A.G. noted that protecting the rights of others was a valid grounds for limitation. It was questionable whether ineffectiveness of blocking could imply unsuitability, but he opined that this would not necessarily be the case. While users can circumvent blocking, it does not follow that every one of these users will do so. If the user learns about a website's illegality, he might forgo accessing the site. Finally, even if many users could circumvent blocking, all of them cannot. Also, even if the same site is available through another domain name or IP address, it does not *prima facie* mean that blocking would be unsuitable. The users here could also forgo accessing the site, and they need to use a search engine to find the site. With repeated blocking, it is also more difficult to find the site with search engines. In consequence, the A.G. held that generally speaking even somewhat ineffective means are not unsuitable.⁷⁹
- 41 When assessing necessity, appropriateness and proportionality *stricto sensu*, the A.G. noted that the least restrictive means should be adopted. It would be the responsibility of the national court to make the assessment based on guidelines and the non-exhaustive list of considerations provided. First, the estimated efficacy of the order would be one factor to consider. However, the possibility to circumvent blocking would not in general exclude the means. Second, the complexity, costs and duration needs to be assessed. The A.G. expected that this may be a test case, and more blocking injunctions might be pending. If one of them were disproportionate under those three grounds, the court might need to consider whether proportionality would be ensured by making the right holder liable for costs wholly or in part. Third, the right holders should have some means against an infringing site, but notably the provider has no contractual relationship with the infringer. This implies that the right holder must primarily target the infringer or the infringer's provider. Fourth, an injunction must not undermine the legitimate business of providing Internet connectivity. In general, the A.G. underlined freedom of expression and its necessity in a democratic

society as essential and access to the Internet as an essential right.⁸⁰

- 42 All of these seem applicable against the backdrop of the CJEU's judgment, with a potential caveat with regard to the third criterion. The CJEU had rejected contractual relationship as a prerequisite for injunction.⁸¹ The A.G. had done likewise, but had opined that it is "obvious" that an intermediary without contractual link can "in no circumstances" be held unconditionally responsible for stopping infringements, laying out implications for proportionality of the third consideration.⁸² Further, "in many cases such intermediaries are best placed" in Recital 59 (and respectively Recital 23 in the Enforcement Directive) implies that in some cases intermediaries are *not* best placed. In that case, the infringer should be targeted. This also conveys an additional issue of *which* intermediary is best placed; typically there are three to five connectivity providers in the "chain" between the user and the source. As an example, the A.G. opined that an injunction would be appropriate against a website connected by a non-European provider, because the website and its operators often cannot be prosecuted.⁸³ *E contrario* websites operated in the EU or connected by providers in the EU might be evaluated differently.
- 43 Orders may target the infringing website's connectivity provider, a provider in the middle of the Internet, or a provider at the user end.⁸⁴ A contractual relationship between the provider and the website operator exists only in the first case. In the second case, some providers may obtain indirect financial gain (through transit agreements between providers), but in the third case there is not even such indirect benefit.⁸⁵ This study focuses on blocking at the user end, because actions against infringing customers are in many aspects more proportionate, and in any case different from those against a completely third party.
- 44 A few interim observations are in order before moving on to examine national case law. The rights to balance in enforcement have been confirmed. However, the evaluation has been rather thin except for the A.G. opinion on the fourth question (unaddressed by the CJEU) in *UPC Telekabel Wien*. In all likelihood, in the future courts will mainly issue specific orders. Also, neither the CJEU nor the A.G. addressed the required level of efficiency when constraining a provider's rights.⁸⁶ The CJEU's position on the provider's function to discourage users could possibly be seen as approving the suitability of educating the users of the site's illegality. Finally, the A.G. made a number of points that the CJEU did not get a chance to address. He noted that proportionality would be affected by the right holder's possibility of primarily targeting the infringer or the infringer's connectivity provider. Second, effectiveness could

be used as a factor both in suitability (with limited impact) and necessity. Third, the assumption seemed to be that the connectivity provider might bear the costs, but an alternative cost model could also be used particularly if the number of blocking requests grew.

III. Expanding Blocking in the UK

- 45 A Usenet newsgroup service *Newzbin*, whose content consisted primarily of infringing files, was ordered to stop copyright infringement with a restricted injunction.⁸⁷ The site ceased operations, but essentially the same service reappeared overseas, and the claimants sought an order against the connectivity provider British Telecom to block access to the new *Newzbin2* site. Judge Arnold examined the issues in depth and *inter alia* found the specific injunction order to be compatible with Articles 12 and 15(1) of the E-Commerce Directive and Article 10 ECHR. Against the backdrop of the referral of *L'Oréal v eBay* and *Scarlet Extended*, he held that the court had jurisdiction to block the whole site.⁸⁸
- 46 Arnold also considered and rejected four reasons why the court should exercise its discretion to decline the request. First, the order targeting the whole site would also affect other right holders. This benefit would rather support issuing the order, and further, the incidence of non-infringing uses was considered *de minimis*.⁸⁹ Second, it was immaterial that accepting the request might lead to more requests in the future.⁹⁰ Third, ineffectiveness of blocking was not decisive. Specifically, users will need to acquire additional expertise to circumvent blocking. Even if they were able to do so, it was not clear that the users wished to expend the time and effort. Arnold also seemed to rely on advocacy research claiming that in Italy, the use of The Pirate Bay had been markedly reduced. All in all, he stated that the order would be justified even if it only prevented access to the site by a minority of users.⁹¹ Fourth, Arnold evaluated proportionality against EHCR in the light of *L'Oréal v eBay*. He held that it was necessary to protect the right holders' property rights, and this clearly outweighed freedom of expression by the users and the connectivity provider, and even more clearly by the site operator. The order was narrow and targeted, it included safeguards against changes of circumstances and the cost of implementation would be modest and proportionate. He also rejected the requirement of notifying infringing files by URLs as being disproportionate and impracticable for the claimants when the site did not have a substantial proportion of non-infringing content.⁹²
- 47 After the main judgment in *Newzbin2*, additional issues on details of the order were raised, some of which may be of relevance here. Arnold found

it proportional to apply the order to all services which use BT's Cleanfeed, but in essence excluded access and wholesale business from blocking. Other IP addresses and URLs, whose sole or predominant purpose was to enable or facilitate access to the Newzbin2 website, could also be added later to the block list without judicial determination. The request to allow temporary shutdown of blocking (e.g. due to operational reasons) without court or claimant approval was rejected. The relatively modest implementation costs would be borne by the connectivity provider, at least in this case. The legal fees were divided based on the merits of the arguments.⁹³ Later the blocking was also extended to other connectivity providers.⁹⁴

- 48 Blocking of The Pirate Bay was soon to follow in *Dramatico Entertainment*, where it was held that the users and website operators infringed copyrights of the claimants in the UK. After *Newzbin2*, the connectivity providers have elected not to actively participate in court proceedings.⁹⁵ In a subsequent ruling, the injunction was issued on the terms the claimants had agreed with connectivity providers. Again, Arnold considered the discretion to grant the order. He stated that the proportionality of orders must be considered, referring to the principles of the Enforcement Directive and *L'Oréal v eBay*. While the terms of the order may be proportionate between the right holders and connectivity providers, it was the duty of the court to ensure the proportionality from the perspective of those who are not before the court (in particular, the users). Given that the IP address of The Pirate Bay was not shared, blocking it was appropriate.⁹⁶ Since this judgment, specific terms of orders have been agreed in advance between the claimants and providers, and those have not been described in the ruling or scrutinized by the court.⁹⁷
- 49 In *Emi v Sky*, blocking was extended to cover three more sites (KAT, HEET and Fenopy). In this case, proportionality was more extensively discussed in the light of recent English judgments. Specifically, Arnold had established a balancing test of conflicting fundamental rights in the context of an order to disclose identities of subscribers, and it had been later endorsed by the UK Supreme Court.⁹⁸ Also, he considered the referral questions posed in *UPC Telekabel Wien*. Arnold rather brusquely dismissed the third preliminary question on whether "prohibition of outcome" would be inappropriate, essentially stating that UK courts carefully consider such matters before any blocking order is made.⁹⁹ Arnold also seemed to dismiss the Austrian Supreme Court's desire for European uniformity in assessing the proportionality of specific blocking measures by referring to the context-sensitivity of such evaluations.¹⁰⁰ The cost of compliance was also not relevant in the UK context because no connectivity provider had resisted making the orders on the basis that compliance would be unduly burdensome

or costly. He still held that blocking order *may be justified* (emphasis added) even if it only prevents access by a minority of users, and that the efficacy depends on the precise form of the order. For example, orders in *Dramatico Entertainment* were likely less easy to circumvent due to the ability of the right holders to revise the list of blocked resources. Finally, Arnold noted that evidence indicates that orders are reasonably effective, again pointing to the Italian study and the drop of The Pirate Bay in Alexa site popularity rankings.¹⁰¹ In conclusion, the orders were deemed necessary and appropriate to protect IPR, and these interests outweighed the freedom of expression rights by users, connectivity providers and website operators.¹⁰² Since then, blocking has extended to cover over 40 sites, but no new considerations of proportionality have come up.¹⁰³

- 50 Access to FirstRow, a site consisting of user-generated streams of sports events, was also blocked in a similar manner. The claimant, FAPL, contended that the order would be proportionate because 1) the providers do not oppose the order and implementation costs are modest and proportionate; 2) the orders are necessary to protect copyrights infringed on a large scale and identifying and bringing proceedings against the operators of the website would be difficult, leaving no other effective remedy in this jurisdiction; 3) the orders are necessary or at least desirable to protect sporting objectives in general; 4) while also foreign content is available, the vast bulk of content infringes the rights of FAPL; and 5) the orders are narrow and targeted ones, and include safeguards against changes of circumstances. The orders will also likely be reasonably effective, even if not completely efficacious. Arnold did not object to these grounds.¹⁰⁴ FAPL had submitted evidence that FirstRow's IP address is not shared, but this later seemed to turn out to be incorrect, leading to substantial overblocking.¹⁰⁵ Further, Arnold added an additional provision to the orders introduced earlier by Mann J, so that any website operator claiming to be affected by the order would have permission to apply to vary or discharge it.¹⁰⁶

IV. Mixed Approach in Nordic Countries

- 51 The Supreme Court of Denmark has issued two relevant judgments on preliminary injunctive relief. The first judgment in 2006 concerned a file transfer (FTP) server and TDC as the connectivity provider for that subscriber. Because the injunction would have essentially required terminating the Internet connection, it was held that Article 8(3) of the Infosoc Directive requires consideration with balancing of interests.¹⁰⁷ In a case concerning blocking users' access to a website, it was submitted that injunctive relief should be rejected as ineffective under the

balance of interest requirement, but this claim was denied with reference to obligations of Article 8(3).¹⁰⁸ In the second judgment, on blocking The Pirate Bay, in the Supreme Court it was mainly argued that the requested interim relief was too imprecise and the balance of interest did not favour injunction. This was rejected because the court felt the order was precise enough to be granted, and there would be no harm to the connectivity provider in a way which would make it disproportionate.¹⁰⁹

- 52 In Sweden there have been no court cases on blocking at the user end. One reason may be the Swedish Copyright Act tying injunctive relief to contributing to infringement.¹¹⁰ However, a website's connectivity provider has been ordered to implement blocking. In *Black Internet*, the Svea Court of Appeal upheld the order to cease providing connectivity to The Pirate Bay. The provider's argument was that the site also had other connectivity providers, the access prevention would not be effective and the site had been reorganised so that the order would not be effective. These did not prevent injunctive relief, and the balance of interest also favoured granting it. Further, the freedom of expression or other fundamental rights would not be restricted in a manner that would violate the ECHR.¹¹¹ Similarly, in *Portlane*, a connectivity provider was ordered to prevent access to a peer-to-peer tracker service "tracker.openbittorrent.com". The court noted that the relief was fair and equitable and not unnecessarily complicated or costly as required by the Enforcement Directive.¹¹² Later, Portlane and other providers were persuaded to stop servicing The Pirate Bay.¹¹³
- 53 In Norway, the request to block access to The Pirate Bay was rejected because providers had no obligation to remove or block illegal content in the implementation of Article 12 of the E-Commerce Directive. Therefore, there was no legal basis for granting an injunction. In another EEA state, Iceland, an initial attempt at blocking failed due to the claimants' procedural error.¹¹⁴ Since the cases in Norway the Copyright Act has been amended in this respect, and a blocking request is expected in the near future.¹¹⁵
- 54 In Danish and (former) Norwegian statutes, injunctive relief shall not be granted if it would cause harm or inconvenience to the defendant in a manner that would be obviously disproportionate to the plaintiff's interest in the injunction. Balancing thus occurs between the parties. However, because the court has some discretion, in special circumstances third-party interests may also be considered, and this has indirectly happened in case law. In contrast, in Sweden the balance of interests has been developed in case law and legal theory. In the two described cases, third-party interest was not considered. As such, in all three countries extraordinary circumstances

seem to be required before a court would take third parties into account when balancing interests.¹¹⁶ In Finland, the statute also provides for reasonableness balancing only between the IPR holder, intermediary and infringer.¹¹⁷ These are in stark contrast to the more recent CJEU case law.

- 55 In Finland, the three largest providers have been ordered to block access to The Pirate Bay with specific orders to avoid uncertainty for the providers. Also, specifying and updating the list of blocked IP addresses and domain names was deemed to require judicial review. It was acknowledged that all measures differed with regard to their effectiveness, precision, cost and implementation time. By citing earlier reports, it was held that none of the proposed technological measures was so ineffective as to preclude issuing the order. The efficacy of blocking could be measured only after implementation. Costs and harm of the injunction were not unreasonable.¹¹⁸ The blocking order affected the providers' whole network, and for example the connectivity provided to other providers or the government could not be excluded.¹¹⁹ It was considered proportionate that the providers needed to cover their own implementation expenses (ca. 10,000 euro) and legal fees (ca. 100,000 euro) each.¹²⁰ While the blocking must not endanger third parties' communications, the minor amount of legal content on the website did not prohibit blocking. Targeting the infringers in Sweden was also not required by law.¹²¹

V. Divergence of Positions in Benelux

- 56 In The Netherlands, summary proceedings to block access to The Pirate Bay failed in July 2010. The judge argued that access could only be blocked from those who directly infringe copyrights rather than non-infringing visitors of the site, and that the individual infringers should have been targeted first.¹²²
- 57 In new proceedings, Ziggo and XS4ALL were ordered to block access to the site, with the right holders having authority to update the list as needed. On subsidiarity the claimant had already sued The Pirate Bay operators and hosting providers, and proceedings against connectivity providers were appropriate; suing users was not needed. On proportionality, given the amount of illegal content on the site, the interests of the copyright holders outweighed those of ordinary Internet users. Also the necessity in a democratic society was briefly addressed. Claims as to effectiveness of blocking were made, which subsequently turned out to be unfounded.¹²³ Other providers have also been ordered to block access, but this time the list of sites needed to be updated in court.¹²⁴
- 58 The first order was overturned on appeal in January 2014.¹²⁵ Based on recent research by the University of

Amsterdam, the blocking was found to be ineffective, particularly if it targeted only one site, because most of the affected users would just use another website or circumvent blocking.¹²⁶ Only the images of art works of music albums and video covers and such material were found to be infringing, and blocking access to these was not sufficiently important when contrasted to the operators' freedom to conduct a business.¹²⁷ It seemed that the court might have been more amenable if the claimants had requested blocking more sites at once instead of proceeding step-by-step.¹²⁸ This would have arguably made blocking more effective.

59 In Belgium, interlocutory proceedings to block access to The Pirate Bay also failed in July 2010. Immediate blocking was deemed disproportionate, especially since the site had already existed for years.¹²⁹ Blocking a fixed list of 11 domain names was established in September 2011 on appeal. The court held that subsidiarity is not required by Article 8(3) of the Infosoc Directive, and the order was also proportionate.¹³⁰ In a different set of cases, in criminal investigation against unidentified operators of The Pirate Bay, all connectivity providers were ordered to block access to the site in April 2012. This was appealed but upheld in February 2013. In October 2013, the Supreme Court upheld the decision that required providers to stop all current and future Pirate Bay domain names and monitor them. Strangely enough, it was not considered a general monitoring obligation.¹³¹

VI. Varied or Lack of Action in Other EU countries

60 In Ireland, a blocking injunction was rejected in 2010 due to lacking implementation of Article 8(3) of the Infosoc Directive.¹³² The law was amended, and six providers were ordered to block access to The Pirate Bay in June 2013.¹³³ A draft order had been agreed in advance between the parties, though concern with overblocking was voiced. The blocking list could be updated without judicial determination as in *Newzbin2*. Providers bore the cost of implementation and most of their legal expenses. The judge considered the draft order both proportionate and reasonable.¹³⁴

61 In Italy the access to The Pirate Bay was blocked for a while in 2008–2009 as a criminal seizure, then the blocking was rejected and then again blocked, the latest order being from February 2010.¹³⁵ There is no explicit provision to issue connectivity providers a blocking order in civil proceedings, and the easier criminal procedure has been used.¹³⁶ There have also been subsequent orders to block other sites.¹³⁷ At the end of 2013, the law changed so that the regulatory authority AGCOM could block sites, though the

EU Commission had serious doubts about various aspects of the draft regulation.¹³⁸

62 In Germany there is no explicit statutory provision on Article 8(3) of the Infosoc Directive. The alternative “Störerhaftung” (disturber) liability imposes a high bar on these injunctions. A prevailing opinion has been that the Infosoc Directive has been adequately implemented, and Störerhaftung is an acceptable solution as to “the conditions and modalities”. Website blocking has also been considered with strong scepticism. Yet *UPC Telekabel Wien* may require reconsideration through expanding interpretation of Störerhaftung or legislation.¹³⁹

63 The lack of an explicit legal basis and evaluation against Störerhaftung has been adopted in a number of cases.¹⁴⁰ For example, in the Hamburg Court of Appeals ruling, the legal basis for injunction was deemed insufficient. It was also stated that Article 8(3) would not require providing for blocking injunctions.¹⁴¹ Last, in the Cologne District Court ruling, a request to order a connectivity provider to block access to certain URLs in the eDonkey peer-to-peer networking service was likewise rejected. This was due to the lack of explicit legal basis, Störerhaftung liability not being met, and the lack of technical capabilities in preventing infringements. In consequence, the blocking would have been unreasonable and ineffective due to the small effort of circumventing such measures.¹⁴² On the other hand, a preliminary injunction has been issued to an operator providing connectivity to The Pirate Bay.¹⁴³

64 There has been no blocking in Portugal, but a request to block The Pirate Bay is to be expected.¹⁴⁴ In Spain, there have been mixed rulings on the legality of operating peer-to-peer indexing sites such as The Pirate Bay. A single case of website blocking has been overturned in appeal due to insufficient grounds.¹⁴⁵ In France, due to the efforts aimed at users through Hadopi, The Pirate Bay has not been blocked, but ISPs and search engines have been ordered to block a set of video streaming sites.¹⁴⁶ In Greece, only two music sites have been blocked.¹⁴⁷ There has been no news of any blocking activity in Eastern Europe.¹⁴⁸

D. Criteria for Assessing Proportionality

I. Overview

65 Blocking cases essentially concern four parties, each with its own private interests: the IPR holder, provider, user and website operator.¹⁴⁹ The operator's interests have not usually been considered explicitly, and they are also not in the main focus here.¹⁵⁰ Public

interests in the background may also implicitly affect the weight court affords each private interest.

- 66 Proportionality has been considered in case law, though often in a summary fashion. Typically it is difficult to even find the criteria used in the evaluation. The criteria may also have been formulated at so high a level (as with most CJEU judgments) that applying them *in concreto* is challenging. However, there are also exceptions. The A.G. opinion on the fourth, unanswered question in *UPC Telekabel Wien* is useful, as well as UK cases *Newzbin2* and *FAPL v Sky*. Also, several recurring themes can be noticed from other national case law. These concern in particular effectiveness (or lack thereof), impact of subsidiarity, effect on the third parties and implementation costs.¹⁵¹ Further, in the literature, comprehensive lists of criteria have been formulated at least by Lodder and van der Meulen,¹⁵² Husovec,¹⁵³ Savola¹⁵⁴ and Pihlajarinne.¹⁵⁵ These also have many recurring issues, but the interest for brevity precludes detailed discussion of each. Various requirements for adequate safeguards have also been suggested, but these are less relevant here.¹⁵⁶
- 67 A generic balancing rule, which as such is not yet very helpful *in concreto*, could be formulated as follows. The more significant negative economic impact infringements cause to the IPR holder, the stronger enforcement mechanisms should be available, and in contrast the more significant negative impact of ordering such blocking needs to be on the other parties. Respectively, the more costs or constraints blocking causes to the provider, and the more it impacts freedom of information of the users, the more significant the losses must be to the IPR holder.
- 68 In consequence, in the crux are effectiveness and costs (or burden in general), respectively. If blocking is ineffective, it cannot mitigate the economic losses of IPR holders; such blocking would only have symbolic value. On the other hand, if blocking is cheap, non-intrusive and precise, it usually does not have a major immediate impact to providers and users. The more intrusive, expensive or vague blocking becomes, the stronger its justification and effectiveness needs to be in order to be proportionate.
- 69 In the following, concrete evaluation criteria are submitted. Interpretation of these criteria is based on the enforcement principles and fundamental rights.

II. Degree and Basis of Illegality

- 70 The legal basis of blocking, the illegality of the source, has implications on proportionality. If some other court has already established the illegality (as with *The Pirate Bay*),¹⁵⁷ or the court issuing blocking does so when the operators have been served summons, more extensive blocking may be appropriate. Blocking is always dubious if the operators have not been represented and the illegality has not been subject to rigorous analysis.¹⁵⁸ Proxies that enable circumventing blocking provide a problematic example of this.
- 71 Is the intent of blocking to prevent site operators from (facilitating) making available copyrighted material,¹⁵⁹ blocking access from users as such, or to prevent users from copying and sharing the material? If illegality cannot be clearly attributed to the site (e.g. because it at most facilitates infringements by others), the legal basis of blocking the site may be in doubt. Because accessing the site is not as such infringing, the focus should be on preventing the main infringement, i.e. users downloading and sharing material. It might be sufficient to target blocking only to those users – i.e. consumers – who are expected to become infringers, rather than e.g. wholesale business, companies or the government.¹⁶⁰
- 72 The scale of infringement also matters as to how invasive blocking mechanisms may be appropriate. For example, a site which has essentially no legal material at all could more easily be blocked as a whole, but this may not be appropriate for a site which has substantial legal uses or where the illegality is doubtful. Specifically, in some such cases URL blocking (for example) has been required instead of blocking the whole site.¹⁶¹ Also, if blocking is targeting a site hosted in the EU/EEA, it also seems relevant to assess whether the site is operating legally in the origin state.¹⁶²

III. Effectiveness

- 73 The relevance of ineffectiveness has come up in almost every case as well as in the literature.¹⁶³ Users' and operators' ease to circumvent blocking, respectively, could be distinguished. The accuracy and completeness of measures may also be measured.¹⁶⁴ The possibility of revising the blocking list already allows taking into account the website operator's actions, although blocking proxies would still be challenging. Overblocking will be discussed below. Therefore, in practice the effectiveness – or more precisely, circumventability – of blocking from the user's perspective is most relevant.
- 74 IPR holders have conducted or commissioned unverifiable advocacy research on the effectiveness of blocking. For example, Italian or Belgian studies, where effectiveness ranges between 73 and 80%, have been cited first when requesting blocking to support its effectiveness. Yet afterwards the ineffectiveness has been implicitly or explicitly argued to justify extending blocking. Alexa ratings

have also been cited, but those are unreliable as they do not apparently account for those that arrive at the site through non-conventional channels.¹⁶⁵ In contrast, in a University of Amsterdam study, it was noted that blocking could in theory only affect the behaviour of those 27 to 28% of consumers who download or intend to download from illegal sources. Of these infringing consumers, the large majority (70-72%) was found to be non-responsive to blocking by finding other ways to access the same or a different site. There was essentially no lasting effect, and even the awareness effect wore off quickly. In consequence, blocking affected only 4 to 6% of all users. Respectively, in another survey Dutch university students were asked if they were downloading less illegal material after the blockade of The Pirate Bay. 13 % of 302 respondents used only legitimate sources, the rest at least sometimes downloaded from illegal sources: 39 % used The Pirate Bay and 48 % used other sources. Of The Pirate Bay users, 66 % used various techniques to bypass blocking, 18 % did not even notice blocking, and 17 % no longer had access to the site. Only 22 % of its users told they now downloaded less from the site. Because some downloaded more, statistically blocking had no discernible impact on the amount of infringement.¹⁶⁶ Connectivity providers have also similarly observed no significant impact on traffic levels. This is also supported by an intuitive finding that those who are already aware of the site (say, “The Pirate Bay”) can just enter the name in a search engine and obtain the list of proxy services on the first page of results.¹⁶⁷

75 It is obvious that blocking may affect some users, especially the ones who are not already familiar with the sites and arrive at the site by web references or by searching for specific content.¹⁶⁸ Equally obvious is that blocking will not affect those regular users who know sites by name, and will continue using them or the alternatives through other, essentially equally easy means (e.g. proxies). This is exacerbated by the fact that infringing users are more knowledgeable and determined than users on average.¹⁶⁹ In consequence, blocking seems to – at most – accomplish a slight deterrence against some non-recurring users, provide “education” to those users,¹⁷⁰ and make it seem that IPR holders are doing something. It seems obvious that almost everyone downloading or sharing from clearly notable unauthorized sources is aware of its illegality. In consequence, education as a goal seems difficult to justify.¹⁷¹ Indeed, the reasoning that users do not bother or will forgo accessing the site when encountering a block seems to apply at most with non-recurring users.¹⁷² Therefore, the A.G.’s justification for ineffective blocking as deterrence is questionable. As will be discussed in the context of legitimacy below, it is not obvious that subordinating providers to such a task is proportionate, especially if it incurs expenses.

76 Blocking with inefficient mechanisms usually results from having to resort to a least bad solution. While a more effective mechanism would in principle be desirable, usually one does not exist or must be rejected on other grounds. Therefore, the main alternative would be to reject the request. As previously noted, it seems easier for courts to accept inefficiency if a more effective order could not be granted.¹⁷³

77 Acceptance of inefficient mechanisms therefore depends on the associated costs, degree of efficiency, and whether using blocking for (somewhat ineffective) educational, symbolic or political purposes is considered legitimate. It is submitted that blocking must be at least reasonably effective by substantially reducing IPR holders’ economic losses. Otherwise, it would be reduced to a symbolic gesture, a useless attempt to educate users, or as a political power play in the field of legal policy.¹⁷⁴

IV. Negative Burden

78 With blocking, the IPR holder shifts the burden of enforcement to third parties, i.e. providers.¹⁷⁵ For providers, this implies implementation cost and expenses for legal services. In all the reviewed cases, the cost of implementation has been borne by providers, even if this is not required by EU legislation.¹⁷⁶ Given that costs have been modest, at most 10,000 euro for a large provider, these are only important in principle.¹⁷⁷ On the other hand, requiring the installation of a URL-blocking mechanism (for example) would likely be disproportionate.¹⁷⁸ Providers likely fear the expansion of mechanisms and costs. Arnold J and the A.G. anticipated this and noted that there may be reasons to cover some or all costs in the future.¹⁷⁹

79 Given that blocking furthers the IPR holder’s private interest, and the IPR holder is also the sole beneficiary, it would not seem unreasonable for it to cover all costs.¹⁸⁰ This would guide it to do a rigorous assessment of which blocking would be economically justified. This might also allow adopting more efficient yet costlier means.

80 However, to date, implementation costs have been dwarfed by 10 to 30 times larger legal expenses. It would be disproportionate to require the provider also to bear the claimants’ costs if an order is granted. This applies in particular to countries where the provider is not even legally allowed to implement blocking without court approval.¹⁸¹ Likewise, if the provider makes good arguments in court and the claimant’s request is restricted, the provider’s costs should also be compensated.¹⁸² An appropriate default might be that both parties bear their own costs if the blocking order is granted essentially as requested.

- 81 Other burdens may also be relevant because the order will restrict how the provider is able to use its resources.¹⁸³ The order may also require reducing the security and reliability of the network.¹⁸⁴ Likewise, there may be limits (usually hundreds or thousands of entries) of blocked targets until the provider faces a serious performance penalty. In consequence, there may also be an issue of scalability if the number of blocking entries grows significantly.¹⁸⁵
- 82 Usually blocking orders have been ordered without a time limit. This imposes restrictions on the provider because as a matter of business, services (e.g. BT's Cleanfeed and equivalents) might need to be replaced or retired. Blocking orders should not restrict innovation and maintenance of services.¹⁸⁶ Also, even if the site disappears, blocking will stay in place until the order is discharged. In that case, the blocking might unduly affect the new user of (in particular) IP addresses. It would be appropriate for the order to have a fixed time limit of two to five years, but renewable as need be with a simple substantiated request.¹⁸⁷ Alternatively, the IPR holder could have the obligation to apply for discharging or varying the order if circumstances change or face liability for potential damages.¹⁸⁸ These would hopefully ensure that the list of blocked sites will contain only relevant and up-to-date entries.
- 83 The impact of this kind of burden must be accounted for, though admittedly the potential technical and innovation implications may be difficult to qualify.

V. Subsidiarity

- 84 The issue of addressing the infringement at its source has been a recurring theme in national case law as well as in the literature. While the CJEU confirmed that the connectivity provider at the user end may be issued a blocking order, it is not always necessarily best placed to end or prevent infringement.¹⁸⁹ In contrast to subscriber identification requests that the CJEU referred to, the user end provider is not the *only* provider that could implement blocking. Further, the A.G. opined that as a consideration of proportionality, if possible, primarily the infringer or infringer's provider should be targeted. This might be the case in particular if an upstream provider is located in the EU.¹⁹⁰ It must also be observed that Article 8(2) of the Infosoc Directive does not require Member States to provide for injunction (against infringers), except when infringement occurs on its territory.¹⁹¹ While wider protection may be provided, this portrays the general principle that in some cases it is not unreasonable to require that the IPR holder pursues the case abroad.¹⁹²
- 85 All of this seems to indicate that subsidiarity does have some role in evaluating proportionality. This is underlined especially if the measures would be burdensome, ineffective, the infringer is operating in EU, there has been no attempt to target him/her or to disconnect the site and/or the illegality is suspect. On the other hand, if there is evidence that the website has repeatedly changed providers (as with The Pirate Bay) or the administrators are anonymous and difficult to identify,¹⁹³ addressing the issue at the user end might be more easily proportionate.

VI. Avoiding Collateral Damage

- 86 The CJEU has emphasised the importance of freedom of information, and the A.G. also underlined its necessity for democracy and supporting the provider's legitimate business.¹⁹⁴ Legal communications in particular must not be "unnecessarily" disturbed.¹⁹⁵ This implies that a minor disturbance might be acceptable in some circumstances; one example might be a site that has a small fraction of legal content. However, it is difficult to conceive of a scenario where overblocking – i.e. blocking affecting unrelated sites – would be acceptable. This comes up (and has come up) in particular with IP address blocking. For example, Arnold J has noted in two UK blocking cases that IP address blocking would not be appropriate if the address was shared.¹⁹⁶
- 87 While overblocking has not yet caused significant problems with the top infringing sites, the ever-expanding blocking implies that this would become a problem. Specifically, for example, proxy sites and less significant websites will most likely almost always use a shared IP address. Thus IP address-based blocking would be excluded. On the other hand, more detailed forms of blocking (e.g. URL blocking) might be unavailable, and more generic ones such as DNS blocking might suffer from other problems. Given the crudeness of the website blocking as a tool, the result may be that blocking would be disproportionate.
- 88 Another difficult-to-qualify issue, as already touched on in the context of burdens, concerns the technical, architectural and security implications of blocking mechanisms, among others. All blocking mechanisms have their problems. DNS blocking undermines the security of the Internet by decreasing trust in domain name lookup services. IP blocking is simple, yet it has a risk of overblocking if not used with caution. There is also a danger of permanent blocking orders hindering innovation as some addresses cannot be recycled to new uses due to lingering blocking orders all over Europe. URL blocking may be expensive and it is incompatible with secure web connections. All of these might cause collateral damage through specific problems or as unreliability in general.¹⁹⁷

E. Proportionality Evaluation

I. Legitimacy of the Objective

- 89 The objective might be construed as IPR protection in such a manner that it does not disproportionately affect other rights. *Prima facie* this could be accepted as legitimate as is, but closer examination reveals doubts on the ultimate goal of blocking.
- 90 The general goal of blocking would seem to be protecting the private interests of IPR holders.¹⁹⁸ The political motives of IPR holders include strengthening the position against other parties, obtaining ever more effective enforcement mechanisms, and being seen to be doing something. The latter is essential to legitimise the existence of central copyright organisations to the actual copyright holders, as well as to affect public opinion that “piracy” cannot be tolerated. On the other hand, the more concrete motive would be to decrease the amount of infringement to regain some “lost” sales.
- 91 The crucial question is which and to which degree these underlying motives of blocking can be accepted as legitimate. Specifically, are enforcement mechanisms (especially at intermediaries’ expense) available only for efficient enforcement that produces economically quantifiable results?¹⁹⁹ Or is blocking also acceptable for educational, symbolic or politically motivated gestures?²⁰⁰ There is likely no single right answer to this because the symbolic value of copyright enforcement is also tied to the public interests, with varied valuations. However, at least using enforcement to enhance your own political agenda at others’ expense must be rejected.

II. Suitability for the Purpose

- 92 The Advocate General suggested that, in general, specific blocking is not inappropriate for the purpose of furthering the aim of protecting the IPR holder’s rights. This was essentially based on a belief that many users would forgo accessing the site and would not bother to search for it because finding a way to access the material would become significantly more difficult. These also seemed to rest on an uneasy assumption that users would not be familiar with the illegality of the site, and blocking would have an educational purpose, affecting users’ behaviour. This displays naiveté or undue optimism. Almost everybody seems to know that downloading and especially sharing is illegal; clearly “illegal sites” are typically also identifiable as such. Most infringers are likely recurring users who are not affected either by blocking or such subtle forms of education. Also, as demonstrated, searching is also trivial, and the increase in deterrence is minimal. As such, the A.G.

seemed to overestimate the suitability of blocking as a deterring and educational mechanism.²⁰¹

- 93 The University of Amsterdam study²⁰² and other public studies confirmed that the anticipated efficacy of deterring and also educating users is too optimistic. In the survey, 71% of infringing users reported that they did not intend to decrease or stop their infringing behaviour; after blocking, 77% continued (similar and even more pessimistic figures were found in other Dutch studies). This was one of the grounds for the Appeals Court rejection of blocking in The Netherlands. It raised an issue, however: would an order be more easily proportionate if the IPR holder requested extensive blocking at once? The court rejected proceeding with a step-by-step approach, which perforce is more ineffective than blocking more sites at once. The court seemed to think “yes”, but it is not clear if this was a fair assessment given that The Pirate Bay was only a test case.²⁰³ On the other hand, a step-by-step approach demonstrates IPR holders’ rhetorical twists: first it is claimed that blocking is effective and as such the request should be granted, and later insufficient effectiveness is used to argue for extending blocking.²⁰⁴
- 94 What is deemed to be the legitimate goal of blocking affects the evaluation of effectiveness and subsidiarity in suitability analysis. If symbolic gestures, education or politics are accepted, even completely ineffective means could be deemed appropriate, assuming that the negative impact on providers and users is minimal. If the goal is to make a significant impact on sharing and reduce the economic loss of IPR holders, a much higher degree of effectiveness may be required. The scale also tilts towards higher requirements if the negative impact on others increases. For example, Arnold J seemed to accept blocking even if it only affected a minority of users.²⁰⁵ This might be suspect unless a broad notion of the goals of blocking is adopted.

III. Necessity: What Is the Least Restrictive Means?

- 95 Necessity concerns whether there are better means of achieving the objective. With the objective of preventing infringements, targeting the infringer (if possible) or infringer’s provider (especially if located in the EU, unless the operator has already switched providers multiple times) would be preferable to a patchwork of step-by-step blocking separately in all Member States. Blocking at the user end incurs much higher costs overall in the form of implementation costs and legal expenses than addressing the problem at its source.²⁰⁶ The necessity to try alternative means first, if at all possible, was also underlined in the A.G. opinion in *UPC Telekabel*

Wien. This is more important in particular if the cost and burden for the provider or the impact on users' freedom of expression is not minimal.

96 Again, if the objective of blocking is deemed to (also) be symbolic, educational or political, there may not be much better means. It is in the IPR holder's interest to increase the duties and responsibilities of intermediaries irrespective of efficacy. Further, blocking appears to be the second- or third-best solution to educating the users, with graduated response probably being preferable; there seems to be a mixed reaction to the relatively expensive and, in PR terms, uncertain trend to sue the users.²⁰⁷ On the other hand, deploying ineffective mechanisms may also result in ridicule, especially from infringing website operators. It would be a much more powerful message from IPR holders to pursue infringers directly.

IV. Proportionality: Weighing the Burden against the Objective

97 Criteria and their impact have already been discussed. Here only a general observation is made. As has already come up repeatedly, the goal of blocking as perceived and accepted by a court doing a proportionality evaluation incurs implications on the level of accepted proportionality. This is in particular the case with ineffective measures that do not cause significant costs or burden to the provider or the users. With a stricter focus on the economically quantifiable results – that is, proof that blocking significantly reduces the losses by IPR holders – ineffective mechanisms might be more easily rejected.

98 One point is worthy of noting, however. The effectiveness or lack thereof in a particular country or context can be measured only (and even then with difficulty) after blocking has been implemented. Erring on the side of restraint, however, might cause the issues to be addressed at higher courts or referred to the CJEU. This might also allow (or force) the IPR holder to conduct more rigorous studies of effectiveness in other countries.²⁰⁸

F. Conclusions

99 IPR holders, intermediaries, users and website operators each have very different interests, and satisfying all of them is obviously impossible. As CJEU case law provides only very high-level guidance, five interrelated criteria for assessing proportionality were formulated: degree and basis of illegality, effectiveness, negative burden, subsidiarity and avoiding collateral damage.

100 As was already observed by Norrgård in 2005, the Enforcement Directive affords a national judge wide discretion in how strong an enforcement model is adopted. It is submitted that by using these criteria, it would be possible to untangle the Gordian Knot of proportionality evaluation and make more reasoned, nuanced and explicit decisions. Too little attention has also been given to the different interpretative contexts (infringer vs intermediary) of enforcement principles.

101 Blocking has not been requested in most EU countries. This is likely due to strategic choices of major national IPR holders and associations: e.g. unsatisfactory benefit compared to the expenses. On the other hand, with reasoned judgments the UK has been in the forefront of blocking. Different aspects of discretion and proportionality have also been considered in many UK rulings, even if on most issues there has not been detailed scrutiny. The appropriateness of blocking, even if impacting only the minority, hinted at particular regard for the symbolic value of copyright enforcement; this was also observable from Ireland.

102 Case law from Scandinavian countries provides an example of how proportionality has traditionally been assessed mainly between the parties in proceedings – a model which is now insufficient. Finland is an example of a country that adopted a very strict interpretation on establishing and updating the blocking list through judicial review only. Norway and several other countries such as Germany also demonstrated the rejection of requests when Article 8(3) of the Infosoc Directive was not explicitly transposed. Belgium was atypical in the sense that both criminal and civil proceedings were used. Criminal proceedings resulted in probably the most extensive blocking and a related monitoring obligation in Europe, closely followed by criminal proceedings in Italy.

103 In contrast, a Court of Appeals decision in the Netherlands was striking. It adopted an unconventional and restricted interpretation of the illegality of the site, and rejected blocking in a proportionality evaluation due to ineffectiveness as demonstrated by public research.²⁰⁹ It remains to be seen if this will be considered an anomaly and overturned in the Supreme Court or CJEU, or if this will be a sign of a new kind of critical movement in European case law.

104 As was seen, the key point in proportionality analysis is establishing which goals in blocking are accepted. Blocking may be portrayed as a technical measure aimed at reducing the economic losses from infringement by increasing sales. Legitimacy of this objective requires substantial impact and effectiveness. On the other hand, if it is accepted that IPR holders have a legitimate aim to try to use

connectivity providers (at their own expense) to perform vain attempts at educating users, or to make symbolic gestures or political moves to increase their own power, inefficient mechanisms might be considered more easily acceptable as well. While the national case law from various EU countries has suggested that the latter justification has also been implied to some degree, it is submitted that a critical assessment is needed before embarking on that path.

* Lic.Sc.(Tech.), Master of Laws, LL.D. candidate. Legal Counsel at CSC-IT Center for Science Ltd, Researcher at University of Helsinki, Finland, and part-time expert member on IPR issues in Market Court. The author likes to thank in particular Taina Pihlajarinne, Martin Husovec, Simon Morrison and Cedric Manara for discussions and feedback.

- 1 See e.g. Van Eecke, "Online service providers and liability: A plea for a balanced approach", 48 CML Rev. (2011) 1455, pp. 1461, 1497-1501; Kohl, "The rise and rise of online intermediaries in the governance of the Internet and beyond - connectivity intermediaries", 26 IRLCT (2012) 185, pp. 192-193, 200. See also Bright - Agustina, "Mediating Surveillance: The Developing Landscape of European Online Copyright Enforcement", 9 J Contemporary European Research (2013) 120, pp. 122-124; Lodder - 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 (2013) 130, paras. 3, 5, 10, 57; Montero - Van Enis, "Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries: Squaring the circle?", 27 CLSR (2011) 21, p. 22.
- 2 A blocking order is just one of the many possible mechanisms an IPR holder may use. See e.g. Edwards, *Role and Responsibility of the Internet Intermediaries in the Field of Copyright* (WIPO study, 2011).
- 3 Husovec, "Injunctions against Innocent Third Parties: The Case of Website Blocking", 4 JIPITEC (2013) 116, paras. 1, 18, 24; Sandfeld Jacobsen - Salung Petersen, "Injunctions against mere conduit of information protected by copyright: A Scandinavian perspective", 42 IIC (2011) 151; 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 13, 2012, pp. 45-46.
- 4 Arts 12-15 of E-Commerce Directive, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. O.J. 2000, L 178/1. See also Van Eecke (n 1), p. 1464.
- 5 Kohl (n 1), pp. 186, 190-191, 193; Husovec (n 3), para. 25; Feiler (n 3), pp. 71-73; Bright - Agustina (n 1), pp. 123-124, 131. See also Savola, "The Ultimate Copyright Shopping Opportunity: Jurisdiction and Choice of Law in Website Blocking Injunctions", 45 IIC (2014) 287. Generally on governments' control of Internet, see Goldsmith - Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP, 2006), pp. 65-85.
- 6 Van Eecke (n 1), p. 1465; Kohl (n 1), p. 191; Blevins, "Uncertainty as Enforcement Mechanism: The New Expansion of Secondary Copyright Liability to Internet Platforms", 34 Cardozo L Rev (2013) 1821; Senftleben, "Breathing Space for Cloud-Based Business Models: Exploring the Matrix of Copyright Limitations, Safe Harbours and Injunctions", 4 JIPITEC (2013) 87, para. 6; Montero - Van Enis (n 1), pp. 28-29.
- 7 See e.g. Pirker, *Proportionality Analysis and Models of Judicial Review* (Europa Law Publishing, 2013), p. 16; Sauter, "Proportionality in EU Law: A Balancing Act?", 15 CYELS (2013) 439, p. 448; Stone Sweet - Mathews, "Proportionality Balancing and Global Constitutionalism", 47 CJTL (2008) 72, p. 75.
- 8 See e.g. Ibid; Craig - de Búrca, *EU Law: Text, Cases and Materials* (OUP, 5th ed. 2011), p. 526; Harbo, "The Function of the Proportionality Principle in EU Law", 16 ELJ (2010) 158, p. 165.
- 9 Websites have typically been held to infringe copyrights in almost all countries. See Savola, "Blocking Injunctions and Website Operator's Liability for Copyright Infringement for User-Generated Links", 36 EIPR (2014) 279. Feiler (n 3, pp. 67-69, 71) sees a potential for market fragmentation and creating barriers to legitimate trade.
- 10 See generally e.g. Sarmiento, "Who's afraid of the charter? The Court of Justice, national courts and the new framework of fundamental rights protection in Europe", 50 CML Rev. (2013) 1267, pp. 1294-1295.
- 11 By analogy, see Husovec (n 3), paras. 7-8; Peukert "The Fundamental Right to (Intellectual) Property and the Discretion of the Legislature", Goethe Institut Frankfurt am Main Faculty of Law research paper 7/2013, also forthcoming in Geiger (ed.), *Human Rights and Intellectual Property: From Concepts to Practice* (Edward Elgar, 2014), p. 3.
- 12 See e.g. Case C-314/12, *UPC Telekabel Wien*, judgment of 27 Mar. 2014, nyr, para. 47; Case C-70/10, *Scarlet Extended*, [2011] ECR I-11959, paras. 45-46, 50-53. In addition, the typically neglected website operator's rights - for example, the right to fair trial, freedom of expression and freedom to conduct a business - are also relevant. See Husovec (n 3), paras. 33-38. More generally on IPR protection and its relation to fundamental rights, see e.g. Griffiths, "Constitutionalising or harmonising? The Court of Justice, the right to property and European copyright law", 28 ELR (2013) 65; Peukert, "Intellectual Property as an End in Itself?", 33 EIPR (2011), 67; 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", 31 EIPR (2009) 113, Mylly, "Intellectual property and fundamental rights: Do they interoperate?" in Bruun (ed.), *Intellectual Property Beyond Rights* (WSOY, 2005) 185, pp. 206-207.
- 13 See e.g. Sandfeld Jacobsen - Salung Petersen (n 3), pp. 176-180; Geiger - Izuymenko, "Copyright on the Human Rights' Trial: Redefining the Boundaries of Exclusivity Through Freedom of Expression", 45 IIC (2014) 316; Jones, "Internet Pirates Walk the Plank with Article 10 kept at Bay: Neij and Sunde Kolmisoppi v Sweden", 35 EIPR (2013) 695; ECtHR *Kolmisoppi v Sweden*, Appl. No. 40397/12, decision of 19 Feb. 2013, 4 EHRLR (2013) 425. On blocking, see cases listed in note 73. Cf. Peukert (n 11), pp. 4-6, 10 (criticising both CJEU and ECtHR for the lack of normative criteria, weighting without a scale and unforeseeability, and also that limitations require justification rather than balancing).
- 14 For a critique of the CJEU's succinct reasoning, see e.g. Mylly (n 12), pp. 210-213; Griffiths (n 12), pp. 74, 76-78; Peukert (n 11), p. 4.
- 15 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. O.J. 2001, L 167/10.
- 16 Corrigendum to the Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights. O.J. 2004, L 195/16. The former Article governs interlocutory injunctions, the latter injunctions awarded after infringement has been established in court. The Infosoc Directive does not explicitly require interlocutory injunctions; see Leistner, "Structural aspects of secondary (provider) liability in Europe", 9 JIPLP (2014) 75, p. 76. The Enforcement Directive explicitly notes

- that injunctions are ordered by a judicial authority, while “injunction” seems to imply that also in the Infosoc Directive.
- 17 Articles 12–14 of E-Commerce Directive; Husovec (n 3), paras. 4–6.
 - 18 On these differences, see Opinion in *L’Oréal v eBay*, paras. 138–146, correctly questioning applying the liability exemptions of connectivity providers to hosting providers in Joined cases C-236–238/08, *Google France*, [2010] ECR I-2417, paras. 113–114. Also see Van Eecke (n 1), pp. 1481–1483.
 - 19 Recitals 42–44 and Art 12 of E-Commerce Directive.
 - 20 Recital 46 and Art 14 of E-Commerce Directive.
 - 21 For a summary, see references in Savola (n 9), p. 285. This will have impact in a proportionality evaluation. See also e.g. Matulionyte – Lankauskas, “Bittorrent Loses Again: A Recent Lithuanian BitTorrent Case and What It Means for the Construction of E-commerce Directive”, 4 JIPITEC (2013) 179; Dimita, “Six Characters in Search of Infringement: Potential Liability for Creating, Downloading and Disseminating .Torrent Files”, 7 JIPLP (2012) 466.
 - 22 On reinterpretation of neutrality to imply awareness, see note 18.
 - 23 Case C-324/09, *L’Oréal v eBay*, [2011] ECR I-6011, paras. 120–123. Van Eecke’s reading of this is that any diligent economic operator should have been able to note the illegality, implying a threshold slightly lower than “manifestly illegal content” (n 1, p. 1467). For similar earlier trends, see Verbiest et al., “Study on the Liability of Internet Intermediaries”, Final report (Markt/2006/09/E) of 12 Nov. 2007, pp. 36–47.
 - 24 Cf. Rizzuto, “The liability of online intermediary service providers for infringements of intellectual property rights”, 18 CTLR (2012) 4, pp. 13–14, submits the opposite argument by generalization and analogous interpretation. For the stated reasons, this seems unconvincing. Indeed, since the E-Commerce Directive, there have been few serious claims (and no rulings) to establish a connectivity provider’s liability for transmitted information.
 - 25 Similarly in *Newzbin2* [2011] EWHC 1981 (Ch), para. 145.
 - 26 Such duties exist in close to 10 EU states, for example, Belgium and Italy. See Verbiest et al. (n 23), pp. 72–73. At least in Italy, failure to comply has also led to finding the connectivity provider liable. See Bellan, “Intellectual Property Liability of Consumers, Facilitators and Intermediaries: The Position in Italy” in Heath – Kamperman Sanders (eds.), *Consumers, Facilitators, and Intermediaries: IP Infringers or Innocent Bystanders?* (Kluwer Law International, 2012) 87, pp. 92, 96–97.
 - 27 Recital 47 and Art 15(1) of E-Commerce Directive. Art 18 also requires providing court measures “designed to terminate any alleged infringement and to prevent any further impairment of the interests involved”. See Montero – Van Enis (n 1), pp. 28–29. An example of “specific monitoring” is a targeted, temporary request to tackle a specific illegal activity. See *ibid.*, p. 30 footnote 69.
 - 28 Recital 45 and Arts 12(3), 13(3), and 14(3) of E-Commerce Directive.
 - 29 This might re-ignite debate on which generic orders would constitute a monitoring obligation. See Husovec, “CJEU Allowed Website Blocking Injunctions With Some Reservations” 9 JIPLP (2014) 631, p. 634.
 - 30 Opinion in *UPC Telekabel Wien* (n 12), para. 78. The A.G. did note that if the connectivity provider needed to search for duplicate DNS entries for the same site, this would amount to forbidden monitoring.
 - 31 Recital 48 of E-Commerce Directive. These also cannot amount to general monitoring but rather refer to notification systems, for example. See Montero – Van Enis (n 1), p. 29. Also, see generally e.g. Nordemann, “Liability for Copyright Infringements on the Internet: Host Providers (Content Providers) – The German Approach”, 2 JIPITEC (2011) 37. Cf. Leistner (n 16, pp. 88–89) who seems to consider the violation of reasonable duties of care to prevent infringements a significant European factor and standard for providers’ secondary liability. His discussion seems to have an implicit hosting provider focus.
 - 32 Last part of Article 14(3) of E-Commerce Directive. See Van Eecke (n 1), pp. 1484–1485.
 - 33 *L’Oréal v eBay* (n 23), paras. 139, 141.
 - 34 *Gema v Rapidshare* (BGH I ZR 80/12), *Atari v Rapidshare* (BGH I ZR 18/11). See Gärtner – Jauch, “GEMA v RapidShare: German Federal Supreme Court extends monitoring obligations for online file hosting providers”, 36 EIPR (2014) 197, pp. 198–199; Ginsburg, “Take Down/Stay Down: RIP in France? But Little Solace for Google...”, Intellectual property issues, The Media Institute (6.8.2012). Cf. Opinion in *L’Oréal v eBay* (n 23), paras. 166–168, 178–182, which suggested a double identity requirement for preventing future infringements: that a person could be prevented from repeating infringement of a specific trademark. This was not explicitly addressed by the CJEU, but the restrictions seemed to point towards that direction; see Van Eecke (n 1), pp. 1477–1478. On potential issues of “stay down” orders, see *ibid.*, pp. 1479–1480.
 - 35 *Scarlet Extended* (n 12), para. 43, affirmed in *UPC Telekabel Wien* (n 12), para. 61. Also similarly in Opinion in *UPC Telekabel Wien*, paras. 75–76, 79–81. For an earlier discussion, see e.g. Mylly (n 12), p. 200.
 - 36 See e.g. Feiler (n 3), pp. 74–75. One way to answer this is to conclude that rights are in some cases practically unenforceable. Alternatively, it must be evaluated whether the extension to enforcement is justified. See Husovec (n 3), para. 26.
 - 37 *UPC Telekabel Wien* (n 12), paras. 54, 57.
 - 38 Opinion in *UPC Telekabel Wien* (n 12), paras. 66, 81–86, 88. This was also submitted by the Commission.
 - 39 While Art 8(1) requires effective, providing and dissuasive sanctions against infringers (emphasis added), these do not apply to faultless intermediaries.
 - 40 Cf. a case on trademark infringement, in which the A.G. did not see that EU law would impose any specific requirements beyond efficacy, dissuasiveness and proportionality required by Article 3(2). Opinion in *L’Oréal v eBay* (n 23), para. 180.
 - 41 See Recital 17 of Enforcement Directive on case-by-case consideration.
 - 42 The interpretations have been taken mainly from *Scarlet Extended* (n 12). For example, “not unnecessarily costly or complicated” could also be construed to mean that the procedure should be easy and cheap for the right holder. Similarly, it could be argued that it would be disproportionate for the right holder to be denied an injunction. On the other hand, the “effectiveness” requirement could also be read in a negative fashion (see Feiler (n 3), pp. 61–62). That is, non-effective mechanisms must be rejected. A positive and widely accepted reading seems to be that effective mechanisms should be provided, but ineffective ones are also acceptable (*maius includit minus*). Likewise, “no barrier to legitimate trade” could also be construed to imply reluctance against intra-EU market fragmentation by imposing requirements to website operators in all jurisdictions. See Feiler (n 3), pp. 68–69 and note 9.
 - 43 See also Norrgård, “The Role Conferred on the National Judge by Directive 2004/48/EC on the Enforcement of Intellectual Property Rights”, ERA Forum 4/2005 at 503, p. 506.
 - 44 Norrgård (n 43), pp. 507–511.
 - 45 Norrgård (n 43), pp. 511–514.
 - 46 Ohly, “Three principles of European IP enforcement law: Effectiveness, proportionality, dissuasiveness”, prepublication

version of article published in Drexl et al. (eds.), *Technology and Competition, Contributions in honour of Hanns Ullrich* (Larcier, 2009), pp. 7–8, 11, 15.

- 47 Cf. Headdon, “Beyond liability: On the availability and scope of injunctions against online intermediaries after *L’Oréal v eBay*”, 34 EIPR (2012) 137, p. 139, seems to implicitly accept dissuasiveness with respect to intermediaries, interpreting it as being in contempt of the court for disobeying the court order.
- 48 Opinion in *L’Oréal v eBay* (n 23), paras. 176–177.
- 49 Norrgård (n 43), p. 514. Actually, Norrgård lists only four types of infringers (and not third parties at all) as imposing considerations for the context. The omission is striking and calls for a specific reminder of third-party scenarios.
- 50 For examples, see Husovec (n 3), paras. 15–19.
- 51 In particular, according to the German Constitutional Court (1 BvL 3/08), a preliminary reference to the CJEU is required if a national court needs to determine the exact scope of discretion of the Member State implementing EU law. See Sarmiento (n 10), p. 1301 fn 128.
- 52 For more examples, see e.g. Verbiest et al. (n 23), pp. 53–56.
- 53 Further details are provided in this and a number of subsections.
- 54 This is the case at least in the UK, Ireland, The Netherlands, Belgium and Austria.
- 55 Feiler (n 3), pp. 27–30. Generally on IPR injunctions in Member States, see European Observatory on Counterfeiting and Piracy, “Injunctions in Intellectual Property Rights” (2011), <http://ec.europa.eu/internal_market/iprenforcement/docs/injunctions_en.pdf> (Observatory Report).
- 56 There have also been cases which relate to Internet connectivity providers and also discussed proportionality, but where the context has been *inter alia* disclosing the subscriber whose IP address was used in copyright infringement. It is not necessary or possible to discuss these in detail. See Case C-275/06, *Promusicae*, [2008] ECR I-271, Case C-557/07, *LSG v Tele2*, [2009] ECR I-1227, Case C-461/10, *Bonnier Audio*, judgment of 19 Apr. 2012, nyr, and Joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, judgment of 8 Apr. 2014, nyr.
- 57 *L’Oréal v eBay* (n 23), paras. 134, 139–144. The criteria established in *Google France* (n 18) were apparently superseded in *L’Oréal v eBay*.
- 58 In another case, a social media site benefited from the Article 14 defence. The judgment was essentially identical to *Scarlet Extended* (n 12), so it is not necessary to cover it here. See Case C-360/12, *NETLOG*, judgment of 16 Feb. 2012, nyr.
- 59 *Scarlet Extended* (n 12), para. 40. Because such an injunction is prohibited, it is not clear why the CJEU continued to consider the fundamental rights balance at all. The CJEU possibly wanted to provide for criteria for evaluation for subsequent cases instead of just addressing the issue at hand.
- 60 *Scarlet Extended* (n 12), paras. 44, 48–49. Also see Kulk – Zuiderveen Borgesius, “Filtering for Copyright Enforcement in Europe after the Sabam Cases”, 34 EIPR (2012) 791.
- 61 *Scarlet Extended* (n 12), paras. 50–52.
- 62 The Opinion in *Scarlet Extended* is of less relevance. The key point was the argument that the national law was vague and broad, and could be used to issue essentially arbitrary orders. The quality of the law as required by fundamental rights limitations should prevent issuing such orders. This aspect was not addressed in the CJEU judgment. See e.g. Van Eecke (n 1), pp. 1494–1495; Husovec (n 3), paras. 40–41.
- 63 *UPC Telekabel Wien* (n 12), paras. 54–62.
- 64 The unfortunate side-effect was that the answer to the fourth question on specific orders was not given and no explicit guidance was provided. It would have been crucial for a proportionality evaluation.
- 65 *Ibid.*, para. 46. The CJEU referred to *Promusicae* (n 56); also see Coudert – Werkers, “In The Aftermath of the *Promusicae* Case: How to Strike the Balance?”, 18 JLLIT (2008) 50.
- 66 *UPC Telekabel Wien* (n 12), para. 47. A.G. had opined (paras. 94–98) on the Charter, limitations and the rights at issue in much the same manner. It is notable that users’ right to data protection was not at issue, as with *Scarlet Extended* (n 12), paras. 50–51, 53.
- 67 *UPC Telekabel Wien* (n 12), paras. 48–51. This latter means that injunctions are not completely forbidden, merely restricted.
- 68 *Ibid.*, paras. 52–53. A.G. had opined (paras. 84–86) that “prohibition of outcome” would not be compatible with the fair balance requirement, as it might require the use of very complicated mechanisms, and the intensity of interference with a provider’s fundamental rights varied. Prevention could also be impossible.
- 69 *Ibid.*, para. 54. The A.G. had opined (paras. 87–88) that a defence at the execution stage would be non-compliant, because the provider does not know which actions it must perform. Similarly in *L’Oréal v eBay* (n 23), the A.G. had opined (para. 181) that it is crucial that the intermediary can know for certain what is required of it, and that the injunction does not impose impossible, disproportionate or illegal duties like the general monitoring obligation.
- 70 See Savola, “Website blocking in copyright injunctions: A further perspective” (28.3.2014), <<http://the1709blog.blogspot.fi/2014/03/website-blocking-in-copyright.html>>. Alternatively, this would imply orders which specify, for the avoidance of doubt, a sufficient implementation as in the early UK injunctions; see *Newzbin2* (No 2) [2011] EWHC 2714 (Ch), para. 56.
- 71 Opinion in *UPC Telekabel Wien* (n 12), paras. 88–89. Intrusive means could also incur significant expenses to the provider.
- 72 *UPC Telekabel Wien* (n 12), paras. 55–56. The A.G. also emphasised (para. 82) that blocking (emphasis added) *actually affects* infringing material and there is no danger of blocking access to lawful material. “Actually affects” could be read to disallow ineffective or misdirected means.
- 73 ECtHR *Yildirim v Turkey*, Appl. No. 3111/10, judgment of 18 Dec. 2012, paras. 65–69. In contrast, in *Akdeniz v Turkey*, Appl. No. 20877/10, inadmissibility decision of 11 Mar. 2014, an Internet user was deemed not to be a ‘victim’ of website blocking.
- 74 *UPC Telekabel Wien* (n 12), para. 57. This may be unattractive for national courts; see Savola (n 70).
- 75 As will be seen, in some countries such a review has not been conducted or it has been superficial.
- 76 *Ibid.*, paras. 58–61. Indeed, on impossibility, see section B.IV.
- 77 *Ibid.*, para. 62.
- 78 *Ibid.*, para. 63.
- 79 Opinion in *UPC Telekabel Wien* (n 12), paras. 99–102. This “users will not bother” argument is similar to the one used by Arnold J; see notes 91 and 101 and accompanying text.
- 80 *Ibid.*, paras. 103–108.
- 81 *UPC Telekabel Wien* (n 12), paras. 34–35. Notably here the context differs from a connectivity provider ordered to reveal the identity of the subscriber using an IP address, as with the referred (para. 32) *LSG v Tele* (n 56), para. 44. In that case, there is only one provider having the required information; here, blocking can be implemented by others as well, and it is a matter of convenience and other considerations.
- 82 *UPC Telekabel Wien* (n 12), paras. 34–35; A.G. Opinion, paras. 58, 107.
- 83 Opinion in *UPC Telekabel Wien* (n 12), para. 57. Similarly, Lodder and van der Meulen (n 1, para. 71) suggest that the problem

- should be addressed at its source and only as the last resort on the user end. While injunctions may be ordered without prejudice to the other actions available to the right holder (Recital 59 of Infosoc Directive, and respectively, Recital 23 of Enforcement Directive), the novel part is taking this into account in the proportionality evaluation. Subsidiarity has been applied at least in France and The Netherlands. On the other hand, some courts in e.g. Germany and Belgium have held that such a subsidiarity requirement does not exist in Article 8(3) of the Infosoc Directive. See Feiler (n 3), pp. 47–52; Van Eecke (n 1), p. 1490; Verbiest et al. (n 23), pp. 49–50.
- 84 See Savola (n 5) pp. 305, 312; Feiler (n 3), p. 53.
- 85 IPR holders have typically claimed that the user end provider benefits, e.g. due to increased demand for high-speed connectivity. This is not obvious. Typically the provider's own audio-visual additional services suffer, and high-volume users that use disproportionate amount of capacity are not ideal customers.
- 86 For example, in the UK it has been held that affecting even a “minority” of users is sufficient; see notes 91 and 101 and corresponding text.
- 87 *Newzbin2* (n 25), paras. 43, 151. Cf. *Newzbin* [2010] EWHC 608 (Ch), paras. 133–135 where Kitchin J was more hesitant and did not initially grant a broader injunction.
- 88 *Newzbin2* (n 25), paras. 157 ff.
- 89 *Ibid.*, paras. 185–186.
- 90 *Ibid.*, paras. 189–190. Cf. Schellekens, “Liability of internet intermediaries: A slippery slope?” 8 SCRIPT-ed (2011) 154.
- 91 *Newzbin2* (n 25), paras. 194, 197–198. For a critique of the research, see note 101.
- 92 *Ibid.*, paras. 199–201. In this case, BT's Cleanfeed system would also have supported URL blocking. In a later ruling, Arnold J also noted that the final *Scarlet Extended* judgment would not have made any difference to his consideration. See *Dramatico Entertainment (No 2)* [2012] EWHC 1152 (Ch), para. 8.
- 93 *Newzbin2 (No 2)* (n 70). It is somewhat strange that an operational requirement of doing emergency service maintenance to the system was rejected.
- 94 See references in *Dramatico Entertainment* [2012] EWHC 268 (Ch), paras. 3–4.
- 95 *Ibid.*, para. 7 and below *Emi v Sky* (n 98), para. 90; *Paramount v Sky* (n 103), para. 3. Reasons may be saving legal expenses, adopting a neutral stance in order to avoid having to reimburse claimants' legal fees, and emphasising that it is not their role to argue for the users and the website but the court's. On saving costs, see Senfleben (n 6), para. 67.
- 96 *Dramatico Entertainment (No 2)* (n 92).
- 97 *Ibid.*, para. 13. This approach could be questioned from the perspective of guarding the interests of parties not represented in the proceedings.
- 98 *Emi v Sky* [2013] EWHC 379 (Ch), paras. 91–93, referring to *Golden Eye* [2012] EWHC 723 (Ch), para. 117: “... That approach is as follows: (i) neither Article as such has precedence over the other; (ii) where the values under the two Articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary; (iii) the justifications for interfering with or restricting each right must be taken into account; (iv) finally, the proportionality test – or ‘ultimate balancing test’ – must be applied to each.” On these developments, including *Golden Eye* [2012] EWCA Civ 1740, see Hyland, “The seductive interface between adult entertainment and Norwich Pharmacal relief”, 18 Comms L (2013) 56; Daly, “Is there an entitlement to anonymity? A European and international analysis”, 35 EIPR (2013) 198. Arnold's test is essentially similar to the balancing considered here, except it lacks an explicit suitability and necessity part.
- 99 *Emi v Sky* (n 98), paras. 7, 95–97.
- 100 *Ibid.*, paras. 99–100.
- 101 *Ibid.*, paras. 102–106. As will be discussed, the more important feature of efficacy is users', not operators', possibility to circumvent blocking. Also, there was no critical assessment of the methodology or bias of these measurements.
- 102 *Ibid.*, para. 107. Again, freedom to conduct a business was not specifically addressed.
- 103 See e.g. *Paramount v Sky* [2013] EWHC 3479 (Ch), para. 42. The number of blocked sites appears to be around 40 as of this writing. See e.g. TorrentFreak, “UK Piracy Blocklist Expands With Megashare, Viooz, Watch32 and Zmovie” (11.3.2014), <<http://torrentfreak.com/megashare-viooz-watch32-zmovie-blocked-140311/>>.
- 104 *FAPL v Sky* [2013] EWHC 2058 (Ch), para. 55. It is notable, however, that there is no requirement to provide an effective remedy in the jurisdiction of the claimant's choosing.
- 105 *FAPL v Sky* (n 104), para. 56; “Premier League piracy fight brings down Radio Times site” (15.8.2013, World IP Review), <<http://www.worldipreview.com/news/premier-league-piracy-fight-brings-down-radio-times-site>>. Also in *Dramatico Entertainment (No 2)* (n 92), para. 13, Arnold J stated that blocking an IP address was only appropriate when it is not shared with anyone else.
- 106 *FAPL v Sky* (n 104), paras. 57–58.
- 107 *TDC*, Supreme Court decision of 10.2.2006 (59/2005). See Sandfeld Jacobsen – Salung Petersen (n 3), pp. 159–160.
- 108 *Allofmp3.com*, Copenhagen City Court decision of 25.10.2006 (F1-15124/2006). See Sandfeld Jacobsen – Salung Petersen (n 3), pp. 161–162; Verbiest et al. (n 23), p. 57.
- 109 *Telenor*, Supreme Court decision of 27.5.2010 (153/2009). See Sandfeld Jacobsen – Salung Petersen (n 3), pp. 162–163.
- 110 Swedish Copyright Act, Section 53 b. Preparatory materials explicitly stated that operating the network does not as such constitute contributory infringement and that injunctions of Article 8(3) are not always available in this context. See Sandfeld Jacobsen – Salung Petersen (n 3), pp. 156–157, 164, 167, 170; Verbiest et al. (n 23), p. 53.
- 111 *Black Internet*, Svea Court of Appeal decision of 21.5.2010 (Ö 7131-09 and Ö 8773-09). See Sandfeld Jacobsen – Salung Petersen (n 3), pp. 163–164.
- 112 *Portlane*, Svea Court of Appeal decision of 21.5.2010 (Ö 10146-09). See Sandfeld Jacobsen – Salung Petersen (n 3), pp. 164–165.
- 113 See TorrentFreak, “Pirate Bay Bandwidth Supplier Disconnected, But the Ship Sails On” (13.2.2013), <<http://torrentfreak.com/pirate-bay-bandwidth-supplier-disconnected-but-the-ship-sails-on-130221/>>.
- 114 *Telenor*, Borgarting Court of Appeal decision of 9.2.2010 (10-00654ASK-BORG/04). See Sandfeld Jacobsen – Salung Petersen (n 3), pp. 165–167; Manner – Flythstrom, “Bonnier Amigo Music Norway AS v Telenor ASA – another flag in the Pirate Bay – internet service provider not responsible for blocking Bittorrent file sharing services in Norway”, 21 EntLR (2010) 237, pp. 239–240. On Iceland, see TorrentFreak, “Pirate Bay Blockade Dismissed by Icelandic Supreme Court” (3.5.2014). <<http://torrentfreak.com/pirate-bay-blockade-dismissed-by-icelandic-supreme-court-140503/>>. The substance was not evaluated and therefore it is not listed in the table.
- 115 See e.g. TorrentFreak, “Anti-Piracy Group Will Use New Law to Block The Pirate Bay” (24.7.2013). <<http://torrentfreak.com/anti-piracy-group-will-use-new-law-to-block-the-pirate-bay-130724/>>.
- 116 Sandfeld Jacobsen – Salung Petersen (n 3), pp. 171–172.
- 117 However, there is a separate provision on not disturbing third parties, so the lack of “users” here seems irrelevant.

- An amendment to add users (and make a number of other revisions) is in progress, however.
- 118 *Elisa*, Helsinki Court of Appeals decision of 15.6.2012 (S 11/3097), Supreme Court denied leave to appeal on 29.10.2012; *DNA*, Helsinki Court of Appeals decision of 8.2.2013 (S 12/1850); *TeliaSonera Finland*, Helsinki Court of Appeals decision of 11.2.2013 (S 12/2223). All court of appeals decisions upheld Helsinki district court decisions, though in the *Elisa* case (p. 21) with a tightened precision of orders. Only the first lower court decision has been elaborated in English; see Norrgård, “Blocking Web Sites – Experiences from Finland” in Axhamn (ed.), *Copyright in a Borderless Online Environment* (Norstedts Juridik, 2012) 171. The most extensive commentary in Finnish is Savola, *Copyright Injunctions against Internet Connectivity Providers Especially with Regard to Peer-to-peer Networking* (Aalto University Licentiate Thesis, 2013).
- 119 By adopting Cleanfeed, some of these were excluded in *Newzbin2* (n 25); see note 93 and corresponding text. Savola has submitted (n 5) that blocking international transit communications would likely be inappropriate, and as such the wording was too broad.
- 120 *DNA* (n 118), pp. 1, 8–9. In contrast, in The Netherlands, the expenses for two providers were 326,000 euro (n 125).
- 121 *Elisa* (n 118), pp. 17–18.
- 122 *Ziggo*, District Court of The Hague, 19.7.2010 (KG ZA 10-573). See Lodder – van der Meulen (n 1), paras. 31–34; Feiler (n 3), p. 28.
- 123 *Ziggo and XS4ALL*, District Court of The Hague, 11.1.2012 (HA ZA 10-3184). See Lodder – van der Meulen (n 1), paras. 35–42.
- 124 *UPC etc.*, District Court of the Hague, 10.5.2012 (KG ZA 12-156). See Lodder – van der Meulen (n 1), paras. 43–44. NB. the case number there is incorrect.
- 125 *Ziggo and XS4ALL*, The Hague Court of Appeals ruling of 28.1.2014 (200.105.418-01). An appeal to the Supreme Court is pending.
- 126 Poort et al., “Baywatch: Two approaches to measure the effects of blocking access to the Pirate Bay”, 38 *Telecom Policy* (2014) 383; *Ziggo and XS4ALL* (n 125), paras. 5:17–5:22. Previous versions of research were available during court proceedings.
- 127 *Ibid.*, paras. 5:25–5:26. The alternative ground that the providers were obliged to act against their infringing customers in this manner was also rejected (paras. 6:1–6:2).
- 128 *Ibid.*, paras. 5:23–5:24.
- 129 *Telenet and Belgacom*, Antwerp Commercial Court, 8.7.2010 (A/10/05374). See TorrentFreak, “ISP’s Don’t Have to Block The Pirate Bay, Court Rules” (10.7.2010), <http://torrentfreak.com/isps-dont-have-to-block-the-pirate-bay-court-rules-100710/>. This justification did not preclude issuing preliminary blocking orders in Finland; see note 118.
- 130 Antwerp Court of Appeal, 26.9.2011 (2011/8314). The court rejected IP-address-based blocking due to its greater potential for over-blocking.
- 131 Van Bael – Bellis, “Belgian Supreme Court Confirms Order Obliging Internet Providers To Block Access To Pirate Bay Websites” (20.12.2013), <http://bit.ly/1uF4bPn>. Cf. confusing the ruling to be related to the earlier cases; see TorrentFreak, “Court Orders ISPs to Police the Internet for Pirate Bay Proxies” (20.11.2013), <http://torrentfreak.com/court-orders-isps-to-police-the-internet-for-pirate-bay-proxies-131120/>.
- 132 *EMI v UPC* [2010] IEHC 377, paras. 133–134. Earlier ex-tempore judgment, *EMI v Eircom* [2009] IEHC 108, where the blocking had been granted, was here admitted to have been wrong; see *EMI v UPC*, paras. 136–137.
- 133 *UPC etc.* [2013] IEHC 274.
- 134 *Ibid.*, paras. 5–8, 21.
- 135 Supreme Court decision of 23.12.2009 (49437/09); TorrentFreak, “Supreme Court Opens Door For Pirate Bay Block” (1.10.2009), <http://torrentfreak.com/supreme-court-opens-door-for-pirate-bay-block-091001/>; Rinaldi, “Italian Supreme Court explains reasons for ordering blocking of Swedish Pirate Bay website” (10.5.2010), <http://www.twobirds.com/en/news/articles/2012/italian-supreme-court-blocking-swedish-pirate-bay-website-050510>; Bellan (n 26), pp. 107–108; Feiler (n 3), p. 26.
- 136 Bellan (n 26), pp. 91, 97; Verbiest et al. (n 23), p. 54.
- 137 See e.g. TorrentFreak, “Italian Court Orders ISPs To Block Several Major Torrent Sites” (17.10.2013), <http://torrentfreak.com/court-orders-isps-to-block-several-major-torrent-sites-131017/>. Also as a rejection of blocking the whole site instead of infringing URL, see TorrentFreak, “Court Orders ISPs to Unblock ‘Pirate’ Site” (3.4.2014), <http://torrentfreak.com/court-orders-isps-to-unblock-pirate-site-140403/>.
- 138 EDRI, “Italian authority gets the power to block websites” (18.12.2013), <https://edri.org/italian-telecom-authority-gets-power-block-websites/>; Rosati, “BREAKING NEWS: EU Commission had serious doubts about Italian Communication Authority draft online copyright enforcement regulation” (15.1.2014), <http://the1709blog.blogspot.com/2014/01/breaking-news-eu-commission-had-serious.html>.
- 139 See Hoeren – Yankova, “The liability of internet intermediaries – the German perspective”, 43 *IIC* (2012) 501, pp. 517–518; Verbiest et al. (n 23), pp. 54–55. Cf. Hoeren on German law misconceiving the goals of EU legislation in Angelopoulos, “Beyond the safe harbours: Harmonising substantive intermediary liability for copyright infringement in Europe”, (2013) *IPQ* 253, p. 269 fn 123; Observatory Report (n 55), pp. (PDF page numbers) 10, 24. Generally on Störerhaftung liability, see e.g. Leistner (n 16), pp. 78–81; Angelopoulos, pp. 266–270.
- 140 *Deutsche Telecom*, Hamburg District Court decision of 12.3.2010 (308 O 640/08), para. 42; Feiler (n 3), p. 27.
- 141 *G-Stream.in*, Hamburg Court of Appeals decision of 22.12.2010 (5 U 36/09); Feiler (n 3), p. 27.
- 142 *Hansenet*, Cologne District Court decision of 31.8.2011 (28 O 362/10), paras. 115–122. See Feiler (n 3), pp. 26–27.
- 143 *CB3ROB*, District Court of Hamburg decision of 6.5.2010 (310 O 154/10).
- 144 TorrentFreak, “Portugal Next in Line to Block The Pirate Bay” (26.9.2013), <http://torrentfreak.com/portugal-next-in-line-to-block-the-pirate-bay-130926/>.
- 145 Bright – Agustina (n 1), pp. 129–130; TorrentFreak, “Website Blocking Law Implemented by New Spanish Government” (2.1.2012), <http://torrentfreak.com/website-blocking-law-implemented-by-new-spanish-government-120102/>. Cf. TorrentFreak, “Court Jails Torrent Site Owner and Issues Three Year Website Work Ban” (8.11.2013), <http://torrentfreak.com/court-jails-torrent-site-owner-and-issues-three-year-website-work-ban-131108/>. TorrentFreak, “‘Pirate’ Site ISP Blockades Reversed by Court (17.7.2014), <http://torrentfreak.com/pirate-site-isp-blockades-reversed-by-court-140717/>. It is reported that the judge deemed that there were insufficient grounds for blocking “especially when it is not absolutely necessary for the continuation of the investigation. For earlier discussion of injunctions, see Verbiest et al. (n 23), pp. 49, 59.
- 146 See e.g. Liard – Hainsdorf, “French Courts Ordered to Block and Delist 16 Streaming Websites” (10.1.2014), <http://www.whitecase.com/articles-01102014/>. *Allostreaming*, TGI Paris decision of 28.11.2013 (11/60013). Website blocking after meeting the requirement of subsidiarity should be possible, however. See Verbiest et al. (n 23), p. 54.
- 147 *Grammo v Internet Service Providers*, Protodikeio (16.5.2012), see 44 *IIC* (2013) 468; TorrentFreak, “Court Orders ISP Blockades of ‘Pirate’ Music Sites” (21.5.2012), <http://torrentfreak.com/court-orders-isp-blockades-of-pirate-music-sites-120521/>.

- com/greek-court-orders-isp-blockades-of-pirate-music-sites-120521/>.
- 148 In Slovakia and Czech Republic, injunctions against intermediaries are not possible due to the lack of legal basis. See Observatory Report (n 55), pp. 10–11, 24–25.
- 149 See section B.IV and in particular the table therein.
- 150 It is submitted that the court must consider the absent operator's rights (to some degree) on its own motion; see Husovec (n 3), paras. 33–38.
- 151 Other recurring themes include specificity of the order, the procedure for updating the blocking list, and applicability of interlocutory injunctions, but these are less relevant from a proportionality perspective.
- 152 In slightly different words, six criteria were submitted: 1) subsidiarity, 2) effectiveness, 3) costs, 4) expansion of existing means, 5) duration and reactive/preventive nature and 6) various adequate safeguards. See Lodder – van der Meulen (n 1), paras. 70–76, 79.
- 153 Husovec (n 3, paras. 27–50) does not specifically propose criteria for proportionality, but some guidelines can be gleaned from general observations: 1) effectiveness, 2) method of implementation, 3) collateral damage to innovation, 4) operator's right to fair trial, 5) abusive use, 6) legality of blocking (out-of-court private agreements), 7) degree of illegality, 8) subsidiarity and 9) shifting of costs.
- 154 Considerations are 1) the goal of blocking and targeting, 2) effectiveness and suitability, 3) impact on users and third party communications, 4) subsidiarity i.e. alternatives and 5) costs and other burdens. These were initially submitted in Savola (n 118), pp. 183–199, and further refined in Savola, "Internet connectivity provider and fundamental rights" in Lohi (ed.), *Oikeustiede–Jurisprudentia XLVI:2013* (Suomalainen Lakimiesyhdistys, 2013) 127, pp. 195–199.
- 155 In the conflict between users and IPR holders: 1) preventive/reactive nature, 2) impact on legal material, 3) IPR holder's financial losses, 4) the extent of material and means, 5) subsidiarity and 6) communications of political or societal nature. Between provider and IPR holder: 1) IPR holder's financial losses and subsidiarity, 2) burden on the provider and 3) specific characteristics of the service. See Pihlajarinne, *Internetvälittäjä ja tekijänoikeuden loukkaus* (Lakimiesliiton Kustannus, 2012), pp. 51–61, 140–148.
- 156 See e.g. Lodder – van der Meulen (n 1), para. 76; Husovec (n 3), paras. 37–40.
- 157 This was done in Sweden. However, it is worth noting that the site has changed slightly since then. For example, instead of torrent files, it's serving only "magnet links", i.e. it is even one step further from the infringing act. See note 21. In contrast, in the Netherlands, only the artworks on the site were held to be infringing. See note 127 and corresponding text.
- 158 Examples of analysis are the UK injunctions in *Dramatico Entertainment* (No 2) (n 92), and *FAPL v Sky* (n 104). Some of the grounds could also be contested, however. See Angelopoulos (n 139), p. 257; Savola (n 9), p. 286.
- 159 On finding website operators liable, even though the site does not have any infringing content, see Savola (n 9), p. 285. On the inapplicability of hosting defences, also see note 21.
- 160 See Savola (n 118), pp. 170–173, 179–181.
- 161 For example, in *Newzbin2* (n 25), Arnold J noted that URL blocking might have been appropriate if the site had substantial legal uses (n 92). The A.G. in his Opinion in *UPC Telekabel Wien* (n 12), was also sensitive to this by referring to *Yildirim v Turkey* (n 73), where blocking the whole Google Sites site to block one site violated Article 10 ECHR in various ways. For example, Rome Court of Appeals rejected blocking the whole site (n 137).
- 162 See note 9. Husovec (n 3, paras. 37–39) notes that website blocking as a substitute for proceedings against infringers might lead to abusive or inappropriate use of blocking, citing an example of blocking a Spanish "HomeLifeSpain.com" site in Denmark due to allegations of trademark violation.
- 163 For example, Lodder and van der Meulen (n 1, para. 72) suggest that symbolic or insignificant mechanisms should not be used, but that normally means could be used when costs are not disproportionate. Pihlajarinne (n 155, pp. 135–136) observes optimism in effectiveness and converting wilfully infringing users to legal consumers, and (p. 145) that due to unavoidable negative externalities, sufficient effectiveness should be required. Husovec (n 3, paras. 27–29) calls for evaluation using the so-called Kaldor Hicks improvement test.
- 164 On users' and operators' possibilities to evade the blocking, see Savola (n 118), pp. 99–106 and Opinion in *UPC Telekabel Wien* (n 12), para. 99. On distinguishing accuracy and completeness (in information theory, "precision" and "recall", respectively), see Savola (n 118), pp. 106–108.
- 165 See e.g. note 101 and corresponding text. On further critical analysis, see note 167.
- 166 Poort et al. (n 126), pp. 387, 391. Wesselingh et al., "To Block or Not to Block?" (Work in progress, 4.6.2014). <<http://ssrn.com/abstract=2273453>> (also citing another University of Amsterdam study, where no significant measurable effect on infringement was discerned). Cf. IFPI, "Digital Music Report 2014", <<http://www.ifpi.org/downloads/Digital-Music-Report-2014.pdf>>, p. 41, claim an 11% reduction of peer-to-peer traffic in EU countries where blocking has been adopted, in contrast to a 15% increase in others. It is not possible to evaluate the reliability of such claims.
- 167 See e.g. Savola (n 118), pp. 104, 112–117. Also IFPI (n 166, p. 42) claims that 74% of consumers are introduced to pirate services through search. This was based on research commissioned by the IPR holder organization MPAA, see MilwardBrown Digital: "Understanding the Role of Search in Online Piracy" (17.9.2013). <<http://www.mpa.org/wp-content/uploads/2014/03/Understanding-the-role-of-search-in-online-piracy.pdf>>, p. 8. Only domain names ("navigational searches") rather than other keywords were used 37% of time for first visits and 46% for repeated visits (p. 9). The study is questionable because a visit to the site within 20 minutes of search is considered a success, and a sharp drop was noticed the shorter the time was (p. 12). Even a minute of delay would seem like a long time and only a fraction of these searches were actually successful. In contrast, using a different methodology, another study found only a ca. 20% impact of search. See Computer & Communications Industry Association, "The Search Fixation: Infringement, Search Results and Online Content" (5.8.2013), <http://www.ccia.net/wp-content/uploads/2013/08/CCIA_TheSearchFixation.pdf>. Further, according to a study, 2% of Internet users committed 74% of all infringement, see Ofcom, "High volume infringers analysis report" (11.9.2013), <<http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/high-volume-infringers/>>. These users are obviously not deterred by any mechanism. Other sources of entry include for example social media sites. Nonetheless, in this kind of use of navigational search by typically recurring users, the percentage is likely somewhere between 20% to 50%. However, there is not much that can be done about it. Completely censoring such generic phrases would seem to infringe on the very substance of the freedom of expression.
- 168 This was measured by a CCIA report (n 167), and the impact seemed rather modest.
- 169 Pihlajarinne (n 155), p. 135. On high-volume infringers, see Ofcom (n 167).
- 170 It is suspect whether blocking could even in the best case educate users, given that access blocking is not necessarily

accompanied by any clear message. For novice users, this is likely indistinguishable from an Internet connectivity or site failure. For recurring users, this has no educational value.

- 171 For example, courts have held that the illegality of The Pirate Bay should be obvious to the users merely through its name; see e.g. *Elisa* (n 118), p. 17. Pihlajarinne (n 155, pp. 135–136) also rejects blocking as an educational signal, noting that users are very well aware of the illegal nature of the site and it is optimistic to assume that they would convert to using legal sources. Hargreaves, “Digital Opportunity: A Review of Intellectual Property and Growth” (May 2011), <<http://www.ipo.gov.uk/ipreview-finalreport.pdf>>, pp. 78–79, also cites reports from an education campaign from 2009 that 69% of average users understood the illegality of downloading after watching an educational advertisement. In contrast (p. 68), a 2010 study found that 44% of peer-to-peer users believed their actions to be lawful. On the other hand, in a recent Finnish Gallup poll commissioned by IPR holders from 2013, 83% of respondents said that downloading music or movies from unauthorized sources is illegal, and respectively 94% said the same for sharing music or movies. A majority of them had done both regardless. See Tekijänoikeusbarometri 2013, <http://www.kulttuuriuutiset.net/gallupit/piratismitutkimus_2013/>. While these are somewhat contradictory, it seems obvious that the illegality of sites is indeed known, but respecting the rights is a different question.
- 172 See note 79 and corresponding text. Likewise Arnold J had similar arguments on blocking increasing the “transaction costs” of using a site; see note 91 and corresponding text. A similar argument and reference to blocking being “educational and helpful” can be found in *EMI v UPC* (n 132), para. 134.
- 173 On interpretations of the effectiveness principle, see note 42. A different reading of the “effectiveness” requirement is also possible: ineffective and merely symbolic means do not strike a fair balance.
- 174 Savola (n 154), p. 198.
- 175 Husovec (n 3), para. 47.
- 176 In *Newzbin2* (No 2) (n 70), paras. 30–34, the estimate for implementation costs was quoted (in the same ballpark as in Finland), and Arnold J noted that the distribution of costs is a national modality, and read “not excessively costly” as implying that the provider needs to cover the cost of carrying the Internet connectivity business. Other interpretations are also possible: that if costs are due, they must not be excessive; or IPR holder’s costs must not be excessive. See also Husovec (n 3), para. 49.
- 177 The principal opposition likely stems from the fear of expanding and extending blocking once “the genie is out of the bottle” and subjugating providers to the role of active web enforcers. See e.g. Schellekens (n 90). It has also been submitted that when implementation costs are minimal, it is not a good sole argument for rejecting blocking, and that it is easier to require blocking more sites once the provider has been subjected to blocking the first time. See Lodder – van der Meulen (n 1), paras. 73–74.
- 178 Feiler (n 3), p. 60.
- 179 The A.G. opined that proportionality might require that e.g. in some repeated cases IPR holders might be ordered to pay costs (n 80); Arnold J in *Newzbin2* (No 2) (n 70), also made a reservation that costs might be ordered in the future; see note 93.
- 180 Similarly on shifting business risks and liability to the provider, see Pihlajarinne (n 155), p. 147; Husovec (n 3), paras. 47–50.
- 181 This is exacerbated by *UPC Telekabel Wien* (n 12) holding that providers may also be responsible for taking into account the users’ interests. In practice this may call for legal evaluation and participation in the proceedings.
- 182 There are some signs of this at least in the UK and Ireland. In the UK, BT was reimbursed costs during refining the orders until 16 December 2010, but BT’s futile “all-out opposition” resulted in it having to compensate subsequent IPR holders’ costs; see *Newzbin2* (No 2) (n 70), paras. 53–55. In Ireland, one of the defendants that actively participated in drafting the order was compensated costs based on agreement with the claimants; see *UPC etc.* (n 133), paras. 19–22.
- 183 On the CJEU’s stance on the impact to business freedom, see notes 67–68 and corresponding text.
- 184 For example, DNS blocking increases the likelihood of users using less secure DNS resolvers, potentially leading to security problems or preventing the use of secure DNS extensions. This was also one of the reasons why the so-called SOPA/PIPA proposals failed. As a summary, see Savola (n 118), pp. 87–88. There are similar constraints with respect to other mechanisms.
- 185 Savola (n 118), p. 78.
- 186 *UPC Telekabel Wien* (n 12), para. 51.
- 187 This may be compared to industrial property rights regimes which include renewable terms that weed out those registrations that were later found out to be useless. On the requirement of regular re-assessment of preventive actions, see Lodder – van der Meulen (n 1), paras. 75, 79.
- 188 This makes more sense than imposing a monitoring duty on the provider or a third party, who have no knowledge and no reason to obtain knowledge of such changes.
- 189 See note 83 and corresponding text.
- 190 See notes 80–83 and corresponding text. Again, as the CJEU did not address the fourth question, it is impossible to conclude if it would have endorsed the A.G.’s opinion on the impact on proportionality.
- 191 In the review of the Enforcement Directive, the Commission has stated that “[a]ny amendments should have as their objective tackling the infringements at their source and, to that end, foster cooperation of intermediaries [...]”. At least in *de lege ferenda* there appears to be a priority to address the problems at their source. See COM(2011) 287 final, p. 19, “A Single Market for Intellectual Property Rights Boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe”.
- 192 National courts seem reluctant to reject requests, however, and in essence state “go seek an injunction in a court closer to the source”. For extensive discussion of international aspects, see Savola (n 5).
- 193 Within EU it might also be possible to request a court order for the infringer’s ISP to disclose subscriber identification information that relates to the anonymous website operator.
- 194 On CJEU see note 72 and on A.G., note 79.
- 195 However, according to ECtHR, even illegal communications enjoy freedom of expression subject to proportionate limitations. See note 13.
- 196 See note 105. Similarly see Feiler (n 3), p. 57.
- 197 See e.g. Savola (n 118), pp. 87–88, 91–93, 115–117; Husovec (n 3), para. 30.
- 198 Further, it could be argued that this would incentivise the creation of new works and foster culture (as a public interest), but this has been disputed; see e.g. Patry, *How to Fix Copyright* (OUP, 2011), pp. 14–27, 77–78; Hargreaves (n 171), pp. 75–76.
- 199 On difficulties of quantifying the impact of infringement, see e.g. Hargreaves (n 171), pp. 72–76. Also, it is not obvious if stronger enforcement measures have reduced piracy (*ibid.*, pp. 77–78). Careful tracking and assessing the impact of enforcement and educational initiatives was also deemed

important (*ibid.*, p. 81). Notably, emphasising enforcement as an alternative to improved licensing and modernisation of copyright law was flat-out rejected (*ibid.*).

- 200** It is unclear if CJEU's statement on "seriously discouraging" accessing the site could be read to accept educational purposes.
- 201** See discussion and references in notes 169–172 and corresponding text.
- 202** See note 166 and corresponding text.
- 203** See notes 125–128 and corresponding text.
- 204** If blocking was indeed as effective as the best claims made of it, expansion might not be worthwhile. See Savola (n 118), pp. 112–113.
- 205** See notes 91 and 101 corresponding text. Arnold likely referred to the minority of infringing users. Likewise, Charleton J felt that blocking would be educational and helpful. See note 172.
- 206** It can be estimated that both providers and IPR holders have used at least 5 million euro in Europe on legal expenses in trying to block The Pirate Bay alone. This estimate is based on the number of countries, ISPs and the proceedings involved when the cost for one provider for one proceedings through appeals instances has been reported (where the information is available) to run at ca. 100,000 to 300,000 euro (see eg. note 120). It seems obvious that such expenses cannot be motivated by blocking (or resistance thereto) just one site, but both parties have more general agenda.
- 207** In *EMI v UPC* (n 132), para. 62, a reference was made to an attempt to educate the public with campaigns. The impact of reducing infringements lasted for only several months before returning to the previous level. As noted in the context of the research of blocking, there appears to be no evidence to suggest that attempts to educate already cognisant persons with inefficient blocking is any more useful. A key difference is that it shifts some expenses and responsibility to providers.
- 208** Unfortunately, such measurements and research are also often biased, so it may be of limited usefulness, especially if the connectivity provider does not wish to expend its resources to fighting it.
- 209** This has also been the only case where detailed public research has been notably part of the proceedings. In some other cases, this could also have made a difference.

Social Networking Sites' Terms of Use

Addressing Imbalances in the User-Provider Relationship through Ex Ante and Ex Post Mechanisms*

by Ellen Wauters, Eva Lievens & Peggy Valcke, Interdisciplinary Centre for Law & ICT (ICRI) – KU Leuven – iMinds

© 2014 Ellen Wauters, Eva Lievens & Peggy Valcke

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Ellen Wauters, Eva Lievens & Peggy Valcke, Social Networking Sites' Terms of Use: Addressing Imbalances in the User-Provider Relationship through Ex Ante and Ex Post Mechanisms 5 (2014) JIPITEC 139, para 1.

A. Introduction

- 1 Legislative instruments that impose information obligations on market actors when offering products and services or closing transactions with users currently exist at various levels and in different sectors. The idea underpinning these legal obligations is that informed users or consumers will make the right choices, and by doing so, will serve not only their own personal interests, but also promote wider public policy objectives (healthy food, green energy, safe investments, privacy-friendly information services, etc.). However, the idea of an informed user does not take into account the heterogeneity of the users nor individual preferences or behavioural constraints. This finding is reflected in the Terms of Use (ToU) of a Social Network Site (SNS), which are meant to inform the user about the rights and responsibilities that membership of such a network entails. Research suggests that these ToU are rarely read by users before agreeing to them. Also, even if users were to actually read the ToU, they would probably not be able to correctly assess the possible implications of these documents. Despite their legal duty to draft contract terms in plain and intelligible language, or obtain “informed” consent for the processing of personal data, market actors continue publishing highly unattractive and complex terms of service or privacy policies which rarely take into consideration the various needs and rights of different types of users.
- 2 Aside from issues regarding the lack of awareness and understanding of ToU, an analysis of several provisions of ToU of SNS has shown that there is cause to be concerned about the imbalance of rights and responsibilities between the SNS provider and its users.¹ It is likely that certain clauses (e.g. with regard to the transfer of copyright or exemption of liability) will not be upheld before European courts, based on consumer protection arguments (e.g. because they “*cause[...] a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer*”; Article 3 of the Unfair Terms Directive).
- 3 On the basis of contract or consumer rights legislation, users may challenge an SNS provider in court when they feel that their rights are being violated. However, a single user will often not be inclined to start a procedure because such procedures are time-consuming and expensive. Also, consumer claims often have a small value in comparison to the resources of the companies that they want to bring to court. Hence, the imbalance between the effort and cost and the result will often discourage consumers from starting judicial action. It is therefore the aim of this paper to assess how this situation can be remedied. We will examine whether an *ex post* remedy such as the use of collective redress mechanisms may provide a solution for consumers or users who want to act upon certain consequences of the imbalanced ToU of SNS providers. Next to this judicial option, we will assess whether we can consider a new manner of establishing standard

contracts in a consumer environment. We will focus on whether alternative *ex ante* mechanisms may be a solution to provide users with more balanced ToU. An example is the use of pre-approved contracts where an independent third party will assess and approve or disapprove of the use of a company's ToU. If approved, the ToU are valid for a certain amount of time and immune for judicial action. Another illustration of this approach is where consumer and business organisations negotiate standard contracts that create an equal balance between business and users' interests. We will also address whether there are possibilities to take into account SNS users' individual values or preferences in such standard contracts.

I. Ex Post: Collective Redress Mechanisms

- 4 The value of goods or services in consumer contracts is often low in comparison to business contracts. It is therefore argued that consumers often do not seek redress because of the small value of the claim and the expensive and time-consuming litigation, which results in an imbalance between the efforts and the expected compensation. A study commissioned by the European Commission on consumer experiences and consumer redress showed that consumers are aware of their rights and that they do have some knowledge about the existence of redress mechanisms.² An individual court proceeding was the mechanism that most consumers recognised. Although they considered it to be beneficial because of the legally binding decision, most of them were also wary to start such a procedure because they perceived it as expensive and time-consuming. Consumers indicated they would use it only in the most serious cases.³ To improve access to justice, Member States and the European Union itself have been developing other mechanisms such as collective action, alternative dispute resolution (ADR) and small claims procedures. However, alternative or online dispute resolution⁴ and small claims procedures⁵ require action from individual users and are currently still very much theoretical options with regard to SNS ToU. Yet, depending on the developments in SNS, this could change in the (near) future, making them viable redress options for users.
- 5 At the moment there is no coherent legal definition of collective redress in the Member States or at the EU level. The Commission's Communication of June 2013 describes the concept as follows:

*Collective redress is a procedural mechanism that allows, for reasons of procedural economy and/or efficiency of enforcement, many similar legal claims to be bundled into a single court action. Collective redress facilitates access to justice in particular in cases where the individual damage is so low that potential claimants would not think it worth pursuing an individual claim. It also strengthens the negotiating power of potential claimants and contributes to the efficient administration of justice, by avoiding numerous proceedings concerning claims resulting from the same infringement of law.*⁶
- 6 The European consumer organisation BEUC (*Bureau Européen des Unions de Consommateurs*) defines the concept more simply as "a legal procedure enabling many victims of the same harm or loss to obtain compensation by way of a single group application to court".⁷
- 7 The concept of collective action is not new, and probably the most well-known is the class action system of the USA.⁸ With regard to SNS, several class actions have been filed in recent years. In April 2011, for instance, a lawsuit was filed in California with regard to the ToU of Facebook. On 26 August 2013, the case was settled and confirmed by the Court, whereby Facebook agreed to (a) establish a \$20 million dollar settlement fund and (b) amend its Statement of Rights and Responsibilities which governs the use of its site and to implement additional mechanisms giving users more information about and control over how their names and portraits are used in connection with the feature of 'Sponsored Stories'.⁹ In the aftermath of this case, Facebook announced on 29 August 2013 that it would update its Statement of Rights and Responsibilities and its Data Use Policy.
- 8 In the EU, several Member States have adopted a form of collective action that can be divided into three broad categories:¹⁰ group actions, representative actions and test procedures. In group actions, an exactly defined category of persons will bring an action to enforce their individual claims together, in one procedure, in accordance with specific rules designed for such purpose.¹¹ In a representative collective action, an organisation, a state authority or an individual on behalf of a group can start a procedure. In contrast to the collective action, the individuals that are represented are not part of the procedure.¹² Lastly, in a test procedure, an individual claim is tested that makes it a precedent for future similar cases.¹³
- 9 In total, 17 Member States have installed a collective redress procedure.¹⁴ In the context of its Consumer Policy Strategy 2007-2013, the Commission ordered two studies: one on consumer evaluation of available redress mechanisms¹⁵ and the other which evaluated the effectiveness and efficiency of collective redress mechanisms in the EU.¹⁶ These studies show that they are not widely used and that they tend to be very different, resulting in diverse results. A comparative study found that a considerable heterogeneity exists within the three broad categories (*supra*), which implies that essential features of collective actions are regulated in diverging ways.¹⁷ Overall, the studies and consultations of the Commission showed that

*the vast majority of the existing collective redress mechanisms tend to have some elements that work, and some that do not. Almost all existing collective redress mechanisms have some added value compared to individual judicial redress and alternative dispute resolution schemes. But their efficiency and effectiveness could be improved. The mechanisms have been applied in relatively few cases.*¹⁸

- 10 A briefing paper of DG for Internal Policies for the European Parliament in 2011 came to the same conclusion and stated that “[t]hese differences point to disparities between the accessibility of collective redress to European consumers in different countries and sectors. European consumers are confronted with a complex legal patchwork of solutions which are applied by some Member States but not by others.”¹⁹
- 11 Several Member States have introduced a mechanism that permits consumer organisations to start a legal procedure on behalf of the collective interests of consumers. For instance, in France, Article L421-1 of the *Code de la Consommation* (Consumer Code) stipulates that “Duly declared associations whose statutory object specifies the protection of consumer interests may, if they are approved for this purpose, exercise the rights conferred upon civil parties in respect of events directly, or indirectly, prejudicing the collective interest of consumers”. This implies that only recognised consumer organisations can start a court procedure. In 2004, the French consumer organisation *Union Fédéral de Consommateurs* (UFC) challenged the ToU of the Internet service provider AOL France. The Court judged that 31 of the 36 clauses were in breach of French law.²⁰ One of the provisions deemed illegal by the UFC was a clause whereby the client had to indemnify AOL France for all complaints and costs, including and without limitation of the reasonable legal fees. The court classified this provision as too broad because it did not define ‘reasonable costs’ and it did not give the possibility to determine the costs for the client. The ToU of AOL France also contained a cap on its own liability equal to the last six months of fees paid by the user. This was judged illegal by the court because it was in breach of the *Code de la Consommation*, which stipulates that it is inappropriate to exclude or limit the consumer’s legal rights in respect of the business or another party in the event of total, or partial, failure to perform, or defective performance by the business of any one of the contractual obligations. In March 2014, the French consumer organisation *Que Choisir?* filed a lawsuit with the *Tribunal de Grande Instance* in Paris with regard to the ToU of Google, Facebook and Twitter, and their privacy policies in particular.²¹ The judgment is expected later this year.
- 12 In Germany, certain consumer organisations can start a judicial procedure under Article 1 of the *Unterlassungsklagengesetz* for infringing standard contract terms and practices that infringe consumer protection legislation, excluding data protection regulation. A new draft bill would extend this
- competence to claims under data protection laws.²² Only qualified consumer organisations may make use of this article:
- associations with legal personality for the promotion of commercial interests, insofar as their membership includes a considerable number of businesses marketing goods or commercial services of the same or a similar type on the same market, insofar as their staffing, material and financial resources enable them actually to perform the interest promotion functions laid down in their statutes.*²³
- 13 However, the *Verbraucherzentrale Bundesverband e.V.* (VZBV), a non-governmental organisation that acts as an umbrella for 41 consumer organisations,²⁴ has successfully challenged several data protection terms. This was only possible if the privacy policy of the company could be considered part of the general ToU.²⁵ With regard to SNS in particular, the VZBV challenged several clauses of the ToU of Facebook. The Berlin District Court found the following terms to be invalid: the copyright license, the use of the name and profile picture in connection with advertising and commercial content, the vagueness in the wording of the termination clause (“violates the letter or spirit of this Statement, or otherwise creates risk or possible legal exposure for Facebook”).²⁶ In November 2013, the Berlin regional court declared 25 clauses of Google’s ToU unlawful, including the liability clause, the term that stipulated that the company reserved the right to check, change and delete all data submitted in their services; the right to directly access a device in order to remove applications; as well as the right to completely cease to provide functions and features at their will.²⁷
- 14 In Belgium, certain consumer organisations also may start a representative action on behalf of an unidentified group of people in order to defend collective consumers’ interests. For instance, the consumer organisation *Test Aankoop* sued Apple over its one-year warranty policy. *Test Aankoop* claimed it was in contradiction with European law that demands a two-year warranty for consumer electronics. In response to the claim that was filed, Apple changed its policy, now giving two years of warranty for its products.²⁸
- 15 In the last decade, the European Commission has taken several steps to adopt a coherent approach towards collective redress mechanisms. In its Consumer Policy Strategy 2007-2013, the Commission stressed the importance of consumer redress:
- If consumers are to have sufficient confidence in shopping outside their own Member State and take advantage of the internal market, they need assurance that if things go wrong they have effective mechanisms to seek redress. Consumer disputes require tailored mechanisms that do not impose costs and delays disproportionate to the value at stake.*²⁹

- 16 The studies in this domain (*supra*) showed that the situation in the EU was unsatisfactory (*supra*).³⁰ As a follow-up on the Green Paper, a consultation paper was published in 2009, presenting a first working analysis of the impact of policy options designed in the light of the replies to the Green Paper and inviting stakeholders to provide further information.³¹
- 17 In February 2012, the European Parliament adopted the resolution “Towards a Coherent European Approach to Collective Redress” in which it welcomed the Commission’s efforts to establish a coherent European approach to collective redress but at the same time stressed that the Commission “*must respect the principles of subsidiarity and proportionality with regard to any proposal that does not fall within the exclusive competence of the Union*”.³²
- 18 In June 2013 the Commission adopted a package of three documents: a Communication,³³ a Recommendation³⁴ and a proposal for a Directive on competition damages.³⁵ The Recommendation states that all Member States should install collective redress mechanisms and take the necessary measures that are set out in this Recommendation and at the latest two years after its publication. Furthermore, Member States should ensure that the collective redress procedures are fair, equitable, timely and not prohibitively expensive. The goal of the Commission is not to harmonize but “*to list some common, non-binding, principles that Member States should take into account when crafting such mechanisms*”.³⁶ The package of the Commission has been received with mixed results, with questions raised as to whether this truly is a step forward in the collective redress process.³⁷ According to Hodges, the package of proposals “*reveals severe political compromises and serious fault lines*”.³⁸ He acknowledges that the rights of all parties are respected, that it provides some robust safeguards against abusive litigation and that economic incentives to bring speculative claims. However, he considers the Recommendation’s list of safeguards to be porous and unenforceable. Moreover, the key factors that affect collective litigation are controlled at the national level. In his view, the package will not achieve a level playing field and continued diversity will promote forum shopping between jurisdictions.³⁹ For Stadler, an important gap is “*the failure to provide clear rules for cross-border cases*”.⁴⁰
- 19 Given the current fragmented situation, it seems that using a collective redress mechanism to enforce their rights is not an obvious choice for European SNS users. Not all Member States have already introduced such procedures; even in Member States that have, the procedures seem to be underused. Up until now, there have been just a few cases against SNS that were introduced by consumer organisations, mainly in Germany and France (*supra*). The underuse of collective redress mechanisms in an

SNS environment may be attributed to a general lack of awareness, not only for individual consumers but also for consumer organisations. Because of the ‘free’ nature of the services and the fact that the negative impact of certain terms is not directly tangible, both users and consumer organisations may feel that action is not immediately necessary nor possible. However, given the impact and pervasive nature of SNS on daily life, we feel that both individual users and consumer organisations should be made aware of the importance of taking action in this field in case of infringements on fundamental rights, such as privacy or consumer rights. In addition, the fact that major SNS are established outside the EU⁴¹ makes it more difficult to start proceedings against these companies. Within the EU, disputes with a cross-border element are subject to the Brussels I Regulation, which lays down the rules for the jurisdiction and enforcement in civil and commercial matters.⁴² The purpose of the Regulation is to facilitate the recognition and enforcement of judgments among Member States for internal market purposes.⁴³ In principle, when an SNS is established outside the EU, the Regulation is not applicable.⁴⁴ The revision of the Brussels I Regulation has resulted in Regulation No 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, which came into force as of 1 January 2013 and will be implemented as of 10 January 2015.⁴⁵ Of importance is Article 18 (1): “*a consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts for the place where the consumer is domiciled*.”⁴⁶ This means that a consumer, as of the beginning of 2015, can bring a company that only has offices outside the EU before the courts of his domicile on the basis of Article 18.⁴⁷ However, the Regulation does not take into account the possibility of collective action implying, according to certain scholars, that a concentration of claims can only be brought in the court of the domicile of the defendant.⁴⁸ According to Tang, the reason can be found in the fact that at the time of writing the Regulation, “*there was no consideration to provide any special jurisdiction rules for this type of action*.”⁴⁹ This makes it very difficult to start a collective procedure against an SNS in a cross-border dispute. In sum, at the moment, the use of collective redress mechanisms to enforce SNS users’ rights is still confronted with various obstacles.

II. Ex Ante: Pre-approved, Negotiated and Interactive Contracts

- 20 Given the reluctance of users to go to court if their rights are violated, the lack of awareness and questions about the practical implementation of ex post remedies to SNS-related issues, it may be

argued that other mechanisms should be introduced to protect users' interests. In this section we will assess the option of *ex ante* remedies – mechanisms that entail an intervention before the user has to agree to the ToU. First, we examine the introduction of pre-approved contracts by a public authority or private interest groups, sometimes referred to as administrative control;⁵⁰ second, we discuss the option of model form contracts that are negotiated by consumer and business interest groups.

1. Pre-approval of contracts

- 21 The idea to introduce a certain control by a third party with regard to consumer contracts is not a new one. Already in 1970 in the USA, Arthur Leff proposed a type of direct governmental quality control.⁵¹ While Leff advocated a statutory mechanism, other US scholars favoured an administrative intervention. For instance, Kaplow and Shavell suggested the idea of a legal body – possibly a regulatory agency – writing standard form contracts and even making it mandatory in certain settings.⁵² Bates was of the opinion that “a system of administrative regulation that certifies the validity of terms in form contracts (...) constitutes a better solution than one that depends on litigation (...).”⁵³ Gillette followed this line of reasoning and considered a procedure that lets consumers and sellers submit a contract to an administrative agency that would be able to evaluate the validity of the provisions in that contract.⁵⁴
- 22 Becher has developed an extensive model of pre-approved contracts and based it on the idea of allowing third parties to review and approve standard contracts.⁵⁵ The purpose of this system is to ensure that consumer contracts are drafted fairly and efficiently. He considers such an approval a quality certification, indicating that an approved contract meets both substantive (fairness, efficiency, cognitive biases) and procedural (font, colour, language, etc.) standards.⁵⁶ Companies could get an approval for the whole contract or for part of the contract. The system would be voluntary, so incentives for companies to submit their contracts for approval are necessary. A possible incentive could be the immunisation against future claims if the contract were approved. The following aspects could be taken into account: the duration of the immunity; the scope of the immunity (which claims will be basically excluded from discussion when approved); the kind of evidence that is allowed and required in order to challenge the ordinary meaning of approved terms, etc.⁵⁷ Gillette calls this immunisation a “safe harbour”.⁵⁸
- 23 Becher finds that this would relieve consumers from their “*theoretical duty to read the fine print*”, economising their time and directing their attention to crucial or problematic contracts that are not pre-approved and that could include problematic terms.⁵⁹
- 24 Although he finds that the system has many advantages, he also isolates several issues that have to be taken into account. First, he finds allowing partial approval of terms necessary. This is because consumers are a heterogeneous audience, and what might seem fair for some consumers may not be for other consumers. Also, companies will need incentives, and an “all-or-nothing” regime will likely have limited success. He argues that companies would rather accept the flexible framework of partial approval. For consumers, providing a system of “all-or-nothing” would make things simpler: they would not have to survey contracts and read non-approved parts. Second, he assesses how the contract can be approved by the independent third party: binary, meaning approved or not, or by grading contracts. Becher prefers the binary option for several reasons, such as the difficulties in reaching a consistent manner of evaluating and grading the contracts and in who will do the grading, the party responsible for approving the contract or a consumer organisation.
- 25 It is possible to make the pre-approval of contracts a mandatory system. However, Becher sees different reasons to keep it voluntary, such as the significant resources that would be needed for an independent third party and a possible violation of the freedom to contract when pre-approval would be mandatory and the (probably) fierce opposition by interest groups that represent business interests. Given the network effects of SNS,⁶⁰ we may assume that a dominant SNS provider is less likely to have an incentive to draft user-friendly ToU. In that case, a voluntary system may not be the ideal solution. Given that the reasons for opposing a mandatory system may indeed be valid, a middle course could be a co-regulatory system, which provides incentives for the providers to join the system but still attributes enough leeway for the concrete implementation and enforcement.
- 26 Finally, Becher takes into account some challenges and anticipates criticism his model may raise. He first addresses the issue of institutional identity. The system should be able to provide strong incentives to sellers to use it; hence, resources must be provided to optimise its functioning and enforcement capabilities. Becher prefers a central institution backed by governmental funds, but acknowledges that because of the drawbacks, this system has other options such as non-profit organisations that should be looked into as well. A second issue that is raised is whether a new institution is really necessary, or whether an already existing organisation could also be an option. The use of an existing organisation could significantly reduce costs and benefit from the expertise and knowledge already available. Becher proposed the US Federal Trade Commission (FTC),

an independent agency with the objective to protect consumers, as a possibility.⁶¹ In Europe, consumer organisations at the national level or European level (such as BEUC) could take up this role.

- 27 An implementation of the pre-approval of contracts can be found in Israel. In 1964, a regulatory system was established in which standard contracts were regulated directly through legislation and whereby a dual layer of judicial and administrative control was established.⁶² Individuals and businesses can submit a contract for approval. If a term is invalidated, this does not affect the validity of other terms in the contract or the enforceability of the contract as a whole.⁶³
- 28 However, the success of the system is limited. The 1964 law generated only sixty submissions. Therefore, the system was revised in 1982 with the purpose of increasing incentives for sellers. Despite the improvements, the success remains low. Gillette contends that the reasons for limited success are not clear and may not be transferable to other states.⁶⁴ However, both Becher and Gillette point to the risk of free-riding.⁶⁵
- 29 This risk of free-riding may exist because, once approved, contracts may be readily available to other parties who have not contributed to the process of obtaining approval.⁶⁶ Gillette considers the submission by a trade organisation a possible alternative to avoid the free-riding problem.
- 30 Other risks that may be identified are related to cost, more specifically that this cost would be passed on to consumers.⁶⁷ In the case of SNS, which are offered to users on a 'free' basis, we may wonder how a transfer of cost would be calculated. An option may be that users will be subjected to more advertisements. Becher disagrees that cost will be problematic and is of the opinion that the "*significance of the problems associated with the Standard Form Contracts cannot easily be exaggerated, especially when keeping in mind the more vulnerable groups of consumers*". Creating such a system would promote trust and confidence between companies and consumers and would reduce transaction costs for companies and increase public confidence. According to Becher, however, for companies, the instalment of such a system would reduce some expenses and increase profits. And though it may result in higher prices, consumers may avoid provisions that they do not know how to evaluate correctly. Finally, as the mechanism would be voluntary, if a consumer does not want to pay the higher price, he or she still can choose to use the products or services of a company that does not have an approved contract and which offers a lower price.
- 31 Another objection could be the fact that since all companies will offer the same set of approved terms, consumers would be denied the possibility

of 'shopping' for different terms. However, this argument assumes that consumers actually do shop for contract terms, which is something that is questionable, for instance in the case of SNS.

- 32 Luth points to incentives for consumers, in particular whether a contract's sign of approval, like a quality label, will be something users will base their decision on. Individual terms may not be a relevant feature for a user, but the overall quality of the ToU might be. However, because of network effects (supra), SNS markets often contain a dominant player. So even when there is a SNS that is more user-friendly in its ToU and privacy policy, it might not make sense to users to be a part of that network when all their friends are members of another SNS with less user-friendly terms.

III. Negotiated contracts

- 33 Another ex ante mechanism is the negotiating of standard terms that would eventually result in a model form contract. Consumers, including SNS users, could be involved in the drafting process, for instance through consumer organisations,⁶⁸ in this way also aiming to concretise participatory policy-making objectives that have been put forward at the European level.⁶⁹ According to Luth, this policy option would have the "*potential of improving quality of terms beyond the level of excluding onerous terms*". Also, information and expertise of both businesses and consumer groups may be used to come to a real understanding about the terms in consumer contracts.⁷⁰ The idea in itself is not new. Based on experiences in the Netherlands and Sweden, in 2000 the European Commission considered the possibility to encourage the establishment of systems that "*encourage the negotiation and discussion of terms with the professionals*".⁷¹ These kind of negotiated model contracts could be subject to self- or co-regulation.⁷²
- 34 Examples of this approach can be found in the Nordic Countries – Norway, Sweden, Finland and Denmark – which have installed a special state authority to enforce consumers' collective interests: the Consumer Ombudsman.⁷³ According to Viitanen, a typical feature of the Nordic system of consumer protection is the "*frequent use of preventive actions in the supervision of marketing and standard terms*". He distinguishes three instruments: advance opinions, marketing guidelines and negotiations with trade organisations concerning standard terms. The purpose of these instruments is to avoid infringements of law by informing traders and by negotiating with them. In addition, these instruments are not prescribed by law, but have been created through practice over the years.⁷⁴ The Nordic Ombudsmen can start negotiations in several branches of business with the respective

trade organisations. For the traders, there is the advantage that the Consumer Ombudsman is less likely to take actions against negotiated contract terms. For consumers, these negotiations could add provisions which improve consumers' contractual position compared to standard terms that were used before or even compared to the mandatory consumer contract law provisions.⁷⁵

- 35 According to Viitanen, there are several positive elements about the Nordic approach. First, the only task of Consumer Ombudsman is the enforcement of consumer protection. This means that this body has been able to focus all available resources on consumer protection without the fear that the fulfilment of other tasks would get the upper hand. Second, the wide use of preventive actions and persuasion has been very successful, and most traders have been more willing to co-operate. He considers the main reason for this willingness in the possibility of hard law sanctions when persuasion fails: *“without the possibility to use hard law sanctions if necessary, the persuasive methods would not be so successful as they have been now in practice”*.⁷⁶
- 36 In the Netherlands, the Social and Economic Council (SER) provides business and consumer organisations with an open framework to negotiate balanced ToU. One of the statutory tasks of the SER is to *“promote desirable trends in business and industry”*.⁷⁷ To achieve this goal, the SER encourages business and consumer organisations to start negotiations over ToU that are satisfactory for both parties. This is a self-regulatory process which ideally leads to the establishment of Consumer Complaints Boards composed of representatives of business and consumers.
- 37 A business organisation or consumer organisation can take the initiative to start negotiations about the ToU in a particular sector. If a bilateral agreement is reached, the business is allowed to use the standard clause of the SER which precedes the ToU.⁷⁸ This provision states that the terms were negotiated with the *Consumentenbond*, the general Dutch Consumer's organisation within the framework of the SER.⁷⁹ The number of sector consumer organisations that are involved in the negotiations is increasing.⁸⁰ In the framework of this mechanism, on the one hand, consumers know that the ToU for a particular sector have been carefully considered, hence strengthening their legal position. Businesses, on the other hand, have ToU that generate trust with consumers. In addition, balanced ToU may help to avoid conflicts between consumers and businesses.⁸¹ For the government, this kind of mechanism has the advantage that its only task is to create the basic framework in which the system will operate.⁸²
- 38 Luth finds several advantages with the mechanism of negotiated contracts.⁸³ First, the fact that both consumers and businesses are represented in the negotiations would allow for competing interests to be taken into account in the final model contract. Second, if these contracts have been negotiated under fair procedures, it can be expected that the terms will be fair and sensitive to the particular interests of the stakeholders. Third, because consumers have a voice in the negotiation through a representative, this should generate standard terms that are more likely to correspond to consumer preferences than one-sided ToU would. However, ensuring representativeness may involve some technical, financial and organisational assistance. Fourth, when consumers are given the chance to influence the content of standard terms, the quality of the ToU may rise. Finally, enforcement costs of regulatory agencies and courts to guarantee that companies use fair contract provisions will be lower.
- 39 A drawback of the system could be that starting negotiations and adopting negotiated contracts will be more costly in expense and effort for companies for whom it is cheaper to adopt low-quality ToU. Nonetheless, Luth⁸⁴ finds some incentives that can persuade companies. First, the drafting costs of ToU would be diminished because of the negotiated contract. Costs are also saved because the terms of the negotiated standard form contract are less likely to be challenged in court and even if they were challenged, the chances of being upheld by the judge are higher. Second, a negotiated contract provides predictability and certainty about the legal validity of the terms. Third, it can be regarded as a token of consumer friendliness and could enhance trust between consumers and companies. Within the same context, reputation and public goodwill could also be an important incentive for companies to adhere to the negotiated standard contract. Finally, from a business perspective, because these contracts have been negotiated by representatives of the sector, companies may rely on the fact that these documents have been developed with business interests in mind as well.
- 40 The attraction of negotiated ToU could be boosted by making the process of negotiation and obtaining the approved model not too costly and strenuous on the part of the companies. However, when the terms are easy to obtain and not all companies that use them have contributed to the negotiations, there is, again, the risk of free-riding. Therefore, Luth proposes a kind of funding mechanism for these negotiations in order to avoid free-riders. Another mechanism that could strengthen the use of negotiated terms is the enhancement of enforcement against one-sided and onerous provisions. In addition, companies could be granted a more favourable position when confronted with a claim against the model ToU, giving them a higher chance to win a dispute when they stick to a model form contract and resulting in lower legal costs.

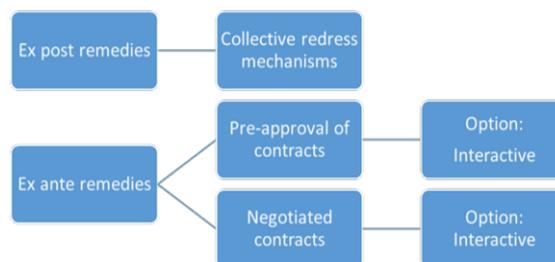
IV. The use of interactive contracts

41 A point of criticism that is voiced with regard to pre-approved or negotiated contracts is that consumers will no longer have a chance to shop for different contracts. A way of responding to this critique may be found in the use of interactive contracts. The idea is that this kind of contract will take the form of a standardised contract, but that certain parts of the agreement can be modulated by the users.⁸⁵ These modular provisions will be pre-drafted by the company. The drafting party has to decide which terms have to be customisable. For instance, an SNS could specify to its users where to store their personal data, the applicable law of the contract or the license conditions for the user's intellectual property.⁸⁶ The seller may provide these customisations for free or at a cost and must decide which will be the default setting for each modular provision. Finally, the seller must draft its interactive contract in such a way that it invites consumer interaction. If possible, the seller may also submit its contract for approval with a third party, or negotiate balanced terms with consumer organisations (*supra*).

42 According to Chen, the use of interactive contracts allows for the avoidance of efficiency losses that sellers and users may experience when using completely standardised agreements.⁸⁷ For instance, in the case of a standard contract, and in particular in the case of a pre-approved or negotiated contract, a user that is willing to pay more for a specific provision cannot do this because the terms are non-negotiable. With an interactive contract, the seller is able to offer terms that are more desirable for a user – for instance, a lower price for a shorter warranty period. Since it is known that users usually do not read ToU (*supra*), interactive contracts may provide an incentive to actually do so. ToU are traditionally offered on a take-it-or-leave-it basis, and users may feel that they have no control. In this way, users who want to shop for terms and care about what is in the ToU can exert some form of control over the contract they are agreeing to.⁸⁸

43 An objection to this kind of contracts is the cost. Devising an adjustable contract that is properly drafted will take time and effort and will hence be more expensive than traditional ToU. As Chen states: “attorneys must consider all the different variations in provisions and how these provisions will interact with each other when combined in various ways”.⁸⁹ Sellers also have to be careful to make the contract not too customisable. Users may not be given too much choice. Research has suggested that a choice overload may lead to frustration and demotivation.⁹⁰ Factors that influence the actual interactivity of the contract are the way the customisable terms are presented⁹¹ and the degree to which users interact with each other. With regard to the latter, SNS allow users to

easily communicate amongst each other about the ToU and their modularity, letting the few users that actually do read the ToU easily contact others and express their thoughts on these terms.⁹²



1.1. The role of consumer organisations

44 Given the heterogeneity and differences in preferences, organisations that represent users and consumers might be best placed to defend and promote their interests, also in the SNS environment. This would allow the voice of users being heard when SNS draw up ToU. In general, these organisations have better access to resources and expertise than individual consumers. They can also provide information and advice and can take preventive or ex post measures, like starting a collective redress procedure.



45 However, there are some elements that have to be taken into account. It is argued that consumer participation in the EU is limited and outweighed by the influence of business interest groups.⁹³ In addition, although consumer organisations express consumers' interests, their impact on policy is sometimes considered to be limited and their membership is relatively small.⁹⁴ Consumer interests themselves may be very diverse as the consumer group is large and diverse to start with. Correspondingly, differences between consumer organisations may result in various focus points between the organisations. The existence of multiple organisations which each have their own

area of expertise could make it very difficult to cooperate and could result in the lack of a coherent consumer voice, which could force regulators to approach a large number of organisations in order to obtain the correct consumer input. Another issue that consumer organisations are confronted with is the lack of resources. This is aggravated by the disparity with business organisations.⁹⁵ In order to succeed in their tasks, according to Dayag-Epstein, consumer organisations should be properly trained, properly funded and cooperate with fellow consumer organisations, not only nationally but also with other countries or on a European level. In certain legal systems, a public authority might be better or equally suited to represent consumers' interests. For instance, in the Nordic countries the Ombudsmen negotiate with trade organisations because consumer organisations in these regions are rather weak. Which party would be best placed to defend consumers will depend on the institutional arrangements and existence of competent consumer organisations in the respective legal systems.⁹⁶

- 46 Yet SNS often operate on a global level, making it difficult for national initiatives to succeed in improving SNS users position vis-à-vis SNS providers on a general level. We believe that European and international organisations that advocate consumer rights, such as the BEUC or Consumers International,⁹⁷ could play an important part in putting these concerns on the European policy agenda on the one hand, and that the European Commission could take up a mediating role between these organisations and large SNS, such as Facebook, on the other hand.

B. Conclusion

- 47 It is a general phenomenon that SNS users have a lack of awareness about and understanding of the ToU they have agreed to when creating a profile. In addition, it is possible that (parts of) these agreements may not be enforceable under European law, because they create a significant imbalance between SNS providers and their users. In this paper we assessed several mechanisms that could help to restore this imbalance.
- 48 First, there are ex post mechanisms which can be used after an issue has arisen. The most obvious one is starting a legal procedure before a court. However, because of the relatively low value of consumer claims in comparison to the costs and efforts of a judicial procedure, most consumers do not act upon complaints they may have. There are different mechanisms that try to provide alternatives to traditional individual legal proceedings, such as collective redress mechanisms. Our analysis has shown that while these mechanisms may seem

promising, they are still in their infancy, in many cases fragmented and not adapted (enough) to cross-border disputes. In addition, awareness of users and consumer organisations about these ex post mechanisms should be increased first and foremost. First, users need to be aware that they have rights and that they can actually take action when they feel that their rights have been infringed by SNS providers. Second, users need to be aware that there are different redress mechanisms that they can use. A long-term and sustainable awareness strategy should be created by the EU or national governments, in cooperation with consumer organisations, to inform users about their rights. This approach could also prove helpful with regard to other consumer protection issues where the interests of consumers are at stake.

- 49 We have also taken into account the option of ex ante schemes, which take a part of the responsibility away from the users and transfer it to the service providers and third parties such as consumer organisations.
- 50 We have discussed, first, pre-approved and, second, negotiated contracts, which may incorporate users' interests by introducing business and consumer organisations in the contract-making process. However, both mechanisms may suffer from the free-riding problem and the issue of cost. Pre-approving or negotiating will take more effort and will likely be more costly than using standard ToU that are readily available. Furthermore, there is the possibility that consumers, once aware of the existence of this type of contract, will never read ToU again because they think they are signing a user-friendly agreement each time. When not all companies in a certain sector adhere to the system, and users assume they are part of this negotiated agreement, they risk ending up with a contract that does not take the consumers' interests seriously. This implies that awareness-raising of users should be an important priority. The use of pre-approved and negotiated contracts may be criticised because it does not provide users with an opportunity to shop around for better terms. An interesting alternative may be the use of interactive contracts that allow for a certain amount of customisation. These contracts may also use pre-approved or negotiated contract terms whereby both the default terms and the modular terms can be discussed. This will allow for ToU that are balanced in the default as well as in the customised setting. Moreover, it gives users the opportunity to choose terms that reflect the values that are important to them (e.g. high or lower level of privacy). In order to decide whether such a system could be feasible in an SNS environment, more social/behavioural and legal research is necessary as well as a thorough and realistic cost-benefit analysis of the various systems.

51 To conclude, we have stressed that awareness-raising of users is a key issue, both for ex ante and ex post mechanisms. In addition, incentives should be created for SNS providers to adopt more user-friendly terms in general and, for instance, to submit them to an approval or negotiation process. To achieve this, supranational pressure, for instance from the European Commission, will be more effective than fragmented national initiatives. Action at the EU level would also lead to a more harmonised approach, and hence more legal certainty for users. Next to the Commission, consumer organisations and other civil society organisations that represent users' interests also have an important role to play in generating awareness about rights and obligations of SNS users and taking action when these rights are at stake.

Ellen Wauters studied political sciences at the KU Leuven and graduated in 2002. She obtained her law degree as a working student at the Vrije Universiteit in Brussel in 2010. She worked as a contracts & licensing administrator at Sony Music and as a legal advisor for Sanoma Media before joining ICRI in February 2012. In the framework of the EMSOC project (www.emsoc.be), she is investigating the legal challenges of social network sites and, more particularly, whether these networks can be regulated in a more user-oriented environment

Prof. Dr. Eva Lievens holds a PhD in Law from KU Leuven and has been a member of the Interdisciplinary Centre for Law & ICT at KU Leuven since 2003 (www.icri.be). She is currently a postdoctoral research fellow of the Research Fund Flanders and guest professor at Ghent University where she teaches media law and copyright law. Her research addresses legal challenges posed by new media phenomena, such as the regulation of audio-visual media services, user-generated content, and social networks, with a specific focus on the protection of children, fundamental rights and alternative regulatory instruments (self- and co-regulation). Eva was involved in the establishment of the B-CCENTRE (Belgian Cybercrime Centre of Excellence for Training, Research and Education) and is the Associate Editor of the International Encyclopaedia of Laws – Media Law.

Prof. Dr. Peggy Valcke is full time research professor (BOFZAP) at KU Leuven, part-time professor at the European University Institute and visiting professor at the University of Tilburg. In 2006, she was visiting professor at Central European University in Budapest, Hungary.

Prof. Valcke joined iMinds-ICRI at KU Leuven in 1996 as a doctoral fellow of the FWO and obtained her PhD in law in 2003 with a dissertation on “Pluralism in a digital interactive media environment: Analysis of sector specific regulation and competition

law” (published by Larcier, 2004, under the title “Digital Diversity - Convergence of Media, Telecommunications and Competition Law” - in Dutch). She also holds a postgraduate diploma EC Competition Law at King's College in London (2006).

Her areas of expertise include legal aspects of media innovation, media pluralism, and the interaction between media/telecommunications regulation and competition law. In recent years, she was involved in several FWO, IWT, BOF, iMinds and FP7 research projects dealing with media power, user-generated content, Internet regulation, mobile and online television, e-publishing and online journalism, public service broadcasting and state aid, co- and self-regulation in the media, privacy in electronic communications and social networks.

* This paper is based on research is funded by the Agency for Innovation by Science and Technology (www.iwt.be; EMSOC research project; User Empowerment in a Social Media Culture) and the Research Fund Flanders (www.fwo.be; Risk-reducing regulatory strategies for illegal and harmful conduct and content in online social network sites).

- 1 WAUTERS, Ellen, LIEVENS, Eva, VALCKE, Peggy, “Towards a better protection of social media users: a legal perspective on the terms of use of social networking sites”, *International Journal of Law and Information Technology*, 25 March 2014, available at doi: 10.1093/ijlit/eau002.
- 2 EUROBAROMETER, Consumer redress in the European Union: Consumer experiences, perceptions and choices, Aggregated report, August 2009, available at http://ec.europa.eu/consumers/redress_cons/docs/cons_redress_EU_qual_study_report_en.pdf, 9.
- 3 *Ibid.*, p. 11.
- 4 Alternative dispute resolution (ADR) can be described as extra-judicial dispute resolution aimed at resolving disputes out of court through the intervention of an entity, e.g. an arbitrator, conciliator, mediator, ombudsman, complaints board. See HÖRNLE, Julia, “Encouraging Online Dispute Resolution in the EU and Beyond: Keeping Costs Low or Standards High?”, *Queen Mary School of Law Legal Studies Research Paper No. 122/2012*, available at <http://dx.doi.org/10.2139/ssrn.2154214>.
- 5 Small claims procedures have been introduced to provide a cheaper, faster and less formal alternative to traditional judicial procedures, and to allow individuals a better access to justice to resolve their disputes at a cost and burden that is not disproportionate to the amount of their claim. Cf. https://e-justice.europa.eu/content_small_claims-42-en.do.
- 6 EUROPEAN COMMISSION, Communication Towards a European Horizontal Framework for Collective Redress, COM(2013) 401 final, 11 June 2013, available at http://ec.europa.eu/consumers/redress_cons/docs/com_2013_401_en.pdf, 4.
- 7 BEUC, Collective redress. Where and how it works, May 2012, available at <http://www.beuc.eu/publications/2012-00308-01-e.pdf>, 11.
- 8 In Europe, however, there was a political consensus that the US model was not the way forward because it created highly undesirable side effects such as excessive litigation, excessive transactional costs, inadequate delivery of compensation to consumer claimants with small claims, etc. See HODGES, Christopher, “Collective Redress in Europe: The New Model”, *Oxford Legal Studies Research Paper*, No. 24/2010, 3-4.
- 9 *Fralely et al v. Facebook, Inc.*, <http://docs.justia.com/cases/federal/district-courts/california/>

- candce/5:2011cv01726/239253/360. In March 2012, in British Columbia, Canada, a similar class action lawsuit was filed against Facebook for using names and/or portraits of users in 'Sponsored Stories' without their consent (<http://facebookadsclassaction.com>). The Court has not yet decided on the matter.
- 10 STUYCK, Jules, TERRY, Evelyne, COLAERT, Veerle et al., An Analysis and Evaluation of Alternative Means of Consumer Redress Other Than Redress Through Ordinary Judicial Proceedings: Final Report, 17 January 2007, (Leuven Report), available at http://ec.europa.eu/consumers/redress/reports_studies/comparative_report_en.pdf, 12.
 - 11 *Ibid.*, p. 261.
 - 12 *Ibid.*, p. 261.
 - 13 *Ibid.*, p. 261.
 - 14 Austria, Bulgaria, Denmark, Finland, France, Germany, Greece, Hungary, Italy, Lithuania, the Netherlands, Poland, Portugal, Spain, Sweden and UK (in England and Wales). DIRECTORATE GENERAL FOR INTERNAL POLICIES, Overview of Existing Collective Redress Schemes in EU Member States, 2011, available at <http://www.europarl.europa.eu/document/activities/cont/201107/20110715ATT24242/20110715ATT24242EN.pdf>, 5. In March 2014, Belgium also introduced a collective procedure.
 - 15 EUROBAROMETER, Consumer redress in the European Union: Consumer experiences, perceptions and choices, Aggregated report, August 2009, available at http://ec.europa.eu/consumers/redress_cons/docs/cons_redress_EU_qual_study_report_en.pdf.
 - 16 STUYCK, Jules, TERRY, Evelyne, COLAERT, Veerle et al., An Analysis and Evaluation of Alternative Means of Consumer Redress Other Than Redress Through Ordinary Judicial Proceedings: Final Report, 17 January 2007, (Leuven Report), available at http://ec.europa.eu/consumers/redress/reports_studies/comparative_report_en.pdf.
 - 17 STUYCK, Jules, TERRY, Evelyne, COLAERT, Veerle et al., An Analysis and Evaluation of Alternative Means of Consumer Redress Other Than Redress Through Ordinary Judicial Proceedings: Final Report, 17 January 2007, (Leuven Report), available at http://ec.europa.eu/consumers/redress/reports_studies/comparative_report_en.pdf, 12.
 - 18 EUROPEAN COMMISSION, Green Paper on Consumer Collective Redress, COM(2008) 794 final, 27 November 2008, available at http://ec.europa.eu/consumers/redress_cons/greenpaper_en.pdf.
 - 19 DG FOR INTERNAL POLICIES, Policy Department A: Economic and Scientific Policy, Overview of existing collective redress schemes in EU Member States, IP/A/IMCO/NT/2011-16, July 2011, 5.
 - 20 Many of these clauses can also – in a more or less adapted manner – be found in certain SNSs' ToU.
 - 21 <http://www.zdnet.com/google-facebook-twitter-face-lawsuit-over-illegible-incomprehensible-privacy-policies-7000027780>.
 - 22 <http://www.privacylaws.com/Publications/enews/International-E-news/Dates/2014/2/German-consumer-organisations-to-be-empowered-to-sue-businesses-for-data-protection-law-breaches>.
 - 23 Art. 3 (1) Unterlassungsklagengesetz.
 - 24 <http://en.vzbv.de/>.
 - 25 VZBV, Press Release: Federation of German Consumer Organisations wins lawsuit against Google. 25 unlawful clauses in Google's privacy policy and terms of service, 19 November 2013, available at <http://www.vzbv.de/cps/rde/xbcr/vzbv/google-vzbv-press-release-2013-11-19.pdf>.
 - 26 Landgericht Berlin, Judgement of 6 March 2012, Az. 16 O 551/10, <<http://openjur.de/u/269310.print>>. See also DITTMANN, Marcus, German Court rules Facebook original Friendfinder and various terms and conditions to be illegal (Landgericht Berlin, Urteil vom 6. März 2012, Az. 16 O 551/10), available at http://www.onlinelaw.de/de/aktuelles/it_news.php?we_objectID=324&pid=0. The judgment was upheld in appeal; see Kammergerichts Berlin of 24 January 2014, Az. 5 U 42/12, http://www.berlin.de/imperia/md/content/senatsverwaltungen/justiz/kammergericht/presse/5_u_42_12_urteil_vom_24.1.2014_kammergericht_anonymisiert.pdf?start&start&ts=1392399485&file=5_u_42_12_urteil_vom_24.1.2014_kammergericht_anonymisiert.pdf.
 - 27 VZBV, Press Release: Federation of German Consumer Organisations wins lawsuit against Google. 25 unlawful clauses in Google's privacy policy and terms of service, 19 November 2013, available at <http://www.vzbv.de/cps/rde/xbcr/vzbv/google-vzbv-press-release-2013-11-19.pdf>.
 - 28 <http://www.zdnet.com/apple-brought-to-heel-in-fight-for-the-right-to-warranty-7000027741>.
 - 29 EUROPEAN COMMISSION, Communication EU Consumer Policy strategy 2007-2013 - Empowering consumers, enhancing their welfare, effectively protecting them, COM/2007/0099 final, 13 March 2007, available at http://ec.europa.eu/consumers/overview/cons_policy/doc/EN_99.pdf.
 - 30 EUROPEAN COMMISSION, Green Paper on Consumer Collective Redress, COM(2008) 794 final, 27 November 2008, available at http://ec.europa.eu/consumers/redress_cons/greenpaper_en.pdf.
 - 31 EUROPEAN COMMISSION, Consultation Paper on the follow-up to the Green Paper on consumer collective redress, 2009, available at http://ec.europa.eu/consumers/redress_cons/docs/consultation_paper2009.pdf.
 - 32 EUROPEAN PARLIAMENT, Resolution on 'Towards a Coherent European Approach to Collective Redress', 2011/2089(INI), 2 February 2012, available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2012-0021+0+DOC+PDF+V0//EN>.
 - 33 EUROPEAN COMMISSION, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Towards a European Horizontal Framework for Collective Redress, COM(2013) 401 final, 13 June 2013, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0401&qid=1397641648895&from=EN>
 - 34 EUROPEAN COMMISSION, RECOMMENDATION ON COMMON PRINCIPLES FOR INJUNCTIVE AND COMPENSATORY COLLECTIVE REDRESS MECHANISMS IN THE MEMBER STATES CONCERNING VIOLATIONS OF RIGHTS GRANTED UNDER UNION LAW, 2013/396/EU, 13 JUNE 2013, AVAILABLE AT http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2013_201_R_NS0013&qid=1397641648895&from=EN.
 - 35 EUROPEAN COMMISSION, Proposal for a Directive of the European Parliament and of the Council on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, COM(2013) 404 final, 2013/0185 (COD), 11 June 2013, available at http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2013/0404/COM_COM%282013%290404_EN.pdf.
 - 36 VOET, Stefaan, "European Collective Redress Developments", 31 August 2013, available at SSRN: <http://ssrn.com/abstract=2318809>.
 - 37 See HODGES, Christopher, "Collective Redress: A Breakthrough or a Damp Squibb?", J Consum Policy, 37, 2013, 67-89.
 - 38 HODGES, Christopher, "Collective Redress: A Breakthrough or a Damp Squibb?", J Consum Policy, 37, 2013, 87.

- 39 HODGES, Christopher, "Collective Redress: A Breakthrough or a Damp Sqibb?", *J Consum Policy*, 37, 2013, 67-87.
- 40 STADLER, Astrid, "The Commission's Recommendation on common principles of collective redress and private international law issues", *Nederlands Internationaal Privaatrecht*, 4, 2013, 484.
- 41 Some SNS offer their services in several EU languages, but this does not necessarily mean that they have offices in all EU countries. Most SNS only have offices or an official 'establishment' in a few EU countries. For a discussion on this issue, see WAUTERS, Ellen, LIEVENS, Eva, VALCKE, Peggy, "Towards a better protection of social media users: a legal perspective on the terms of use of social networking sites", *International Journal of Law and Information Technology*, 25 March 2014, available at doi: 10.1093/ijlit/eau002.
- 42 COUNCIL Regulation No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Regulation) will be replaced by the European Parliament and Council Regulation No 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.
- 43 COUNCIL Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Regulation) [2000], OJ L12/1, recital 1 and 2.
- 44 Brussels I Regulation, Art. 4 (1) 1: "If the defendant is not domiciled in a Member State, the jurisdiction of the courts of each Member State shall, subject to Articles 22 and 23, be determined by the law of that Member State." See a Notice of the European Parliament to its members: "The jurisdiction rules of the Regulation currently (with some exceptions) do not apply when the defendant is domiciled outside the EU, so that in these cases the Regulation refers to national law (so-called 'residual jurisdiction')". EUROPEAN PARLIAMENT, Notice to Members, Petition 1093/2012 by A.D. (German), on request that non-EU companies have a legal status in the EU, if they wish to trade within its confine, 27.03.2013, available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/peti/cm/932/932029/932029en.pdf.
- 45 EUROPEAN PARLIAMENT AND COUNCIL Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2012] OJ L351/1.
- 46 See Recital 14: "A defendant not domiciled in a Member State should in general be subject to the national rules of jurisdiction applicable in the territory of the Member State of the court seized. However, in order to ensure the protection of consumers and employees, to safeguard the jurisdiction of the courts of the Member States in situations where they have exclusive jurisdiction and to respect the autonomy of the parties, certain rules of jurisdiction in this Regulation should apply regardless of the defendant's domicile." See also the text of the European Parliament: "Common rules of jurisdiction: there must be a connection between proceedings to which this Regulation applies and the territory of the Member States. Common rules of jurisdiction should, in principle, apply when the defendant is domiciled in a Member State. A defendant not domiciled in a Member State should, in general, be subject to the national rules of jurisdiction applicable in the territory of the Member State of the court seized. However, in order to ensure the protection of consumers and employees, to safeguard the jurisdiction of the courts of the Member States in situations where they have exclusive jurisdiction and to respect the autonomy of the parties, certain rules of jurisdiction in this Regulation should apply regardless of the defendant's domicile." (European Parliament legislative resolution of 20 November 2012 on the proposal for a regulation of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) COM(2010)0748 – C7-0433/2010 – 2010/0383(COD), Summary, <<http://www.europarl.europa.eu/oeil/popups/summary.do?id=1234824&t=d&l=en>> accessed 9 September 2013.)
- 47 For instance, the SNS Pinterest does not have offices in the EU, so they are normally not bound by the Regulation. However, this article gives consumers the opportunity to sue Pinterest in their Member State.
- 48 LEIN, Eva, "Extraterritoriality and Collective Redress", in FAIRGRIEVE, Duncan and LEIN, Eva (eds.) *Extraterritoriality and collective redress*, Oxford University Press, Oxford, 2012, 141.
- 49 TANG, Zheng S., "Consumer Collective Redress in European Private International Law", *Journal of Private International Law*, Vol. 7 2011, 101; <http://ssrn.com/abstract=2079237>.
- 50 LUTH, Hanneke, *Behavioural economics in consumer policy, the economic analysis of standard terms in consumer contracts revisited*, Intersentia, Antwerp, 2010, 264.
- 51 LEFF, Arthur, "Contract as Thing", Faculty Scholarship Series, Paper 2827, available at http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=3809&context=fss_papers, 1970, 155.
- 52 KAPLOW, Louis and SHAVELL, Steven, *Fairness versus Welfare*, Harvard University Press, Boston, 2006, 217.
- 53 BATES, Larry, "Administrative Regulation of Terms in Form Contracts: A Comparative Analysis of Consumer Protection", *Emory International Law Review*, 16, 2002, 11.
- 54 GILLETTE, Clayton, "Pre-Approved Contracts", *Houston Law Review*, 42:4, 2005, 983.
- 55 BECHER, Shmuel I., "A 'fair contracts' approval mechanism: Reconciling consumer contracts and conventional contract law", *University of Michigan Journal of Law Reform*, Vol. 42:4, 2009, 748.
- 56 *Ibid.*, p. 750.
- 57 *Ibid.*, p. 750.
- 58 GILLETTE, Clayton, "Pre-Approved Contracts", *Houston Law Review*, 42:4, 2005, 988.
- 59 BECHER, Shmuel I., "A 'fair contracts' approval mechanism: Reconciling consumer contracts and conventional contract law", *University of Michigan Journal of Law Reform*, Vol. 42:4, 2009, 748.
- 60 Network effects imply that the value of a product or service for one user is dependent on the number of other users, or in other words, that a good or service becomes more valuable when more people use it. In the case of SNS, network effects have as a result that individuals are inclined to remain a member of the social network in which most of their friends are present. For more information, see WAUTERS, Ellen, LIEVENS, Eva and VALCKE, Peggy, "D1.2.4: A legal analysis of Terms of Use of Social Networking Sites, including a practical legal guide for users: 'Rights & obligations in a social media environment'", EMSOC Project, 2013, available on www.emsoc.be.
- 61 BECHER, Shmuel I., "A 'fair contracts' approval mechanism: Reconciling consumer contracts and conventional contract law", *University of Michigan Journal of Law Reform*, Vol. 42:4, 2009, 796.
- 62 DEUTCH, Sina, "Controlling Standard Contracts – The Israeli Version", *McGill Law Journal*, 1985, 30, 461.
- 63 BATES, Larry, "Administrative Regulation of Terms in Form Contracts: A Comparative Analysis of Consumer Protection", *Emory International Law Review*, 16, 2002, 32.
- 64 GILLETTE, Clayton, "Pre-Approved Contracts", *Houston Law Review*, 42:4, 2005, 985.

- 65 GILLETTE, Clayton, "Pre-Approved Contracts", *Houston Law Review*, 42:4, 2005, 984-9; BECHER, Shmuel I., "A 'fair contracts' approval mechanism: Reconciling consumer contracts and conventional contract law", *University of Michigan Journal of Law Reform*, Vol. 42:4, 2009, 758.
- 66 *Ibid.*, p. 989.
- 67 Gillette argues that the process of obtaining approval will most likely prove to be costly for the party that wants to obtain it. GILLETTE, Clayton, "Pre-Approved Contracts", *Houston Law Review*, 42:4, 2005, 988.
- 68 *Ibid.*, p. 269.
- 69 LIEVENS, Eva & VALCKE, Peggy, "Regulatory trends in a social media context", in: PRICE, Monroe & VERHULST, Stefaan, *Routledge Handbook of Media Law*, Routledge, Oxon, 2012, 557-580.
- 70 *Ibid.*, p. 270.
- 71 EUROPEAN COMMISSION, Report on the implementation of Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts, COM(2000) 248 final, 2000, available at http://ec.europa.eu/consumers/cons_int/safe_shop/unf_cont_terms/uct03_en.pdf, p. 25.
- 72 LIEVENS, Eva, *Protecting children in the digital era: The use of alternative regulatory instruments*, Martinus Nijhoff Publishers, Leiden / Boston, 2010.
- 73 VIITANEN, Klaus, "Enforcement of consumers' collective interests by regulatory agencies in the Nordic Countries". In: VAN BOOM, Willem, LOOS, Marco (Eds.), *Collective Enforcement of Consumer law*, Europa Law Publishing, Groningen, 2007, 84.
- 74 *Ibid.*, p. 84.
- 75 *Ibid.*, p. 85.
- 76 *Ibid.*, p. 97.
- 77 http://www.ser.nl/en/about_the_ser/responsibilities.aspx#promoting.
- 78 <http://www.ser.nl/nl/taken/zelfregulering/consumentenvoorwaarden.aspx>.
- 79 For instance, on a Dutch webshop: "AV CZ/79 4 juni 2012. Naar de algemene voorwaarden kopen bij andere verkopers / algemene voorwaarden zakelijke afnemers / couponvoorwaarden / cadeaubonvoorwaarden. Deze Algemene Voorwaarden van de Nederlandse Thuiswinkel Organisatie zijn tot stand gekomen in overleg met de Consumentenbond in het kader van de Coördinatiegroep Zelfreguleringsoverleg (CZ) van de Sociaal-Economische Raad en treden in werking per 4 juni 2012. Deze Algemene Voorwaarden zullen worden gebruikt door alle leden van de Nederlandse Thuiswinkel Organisatie met uitzondering van financiële diensten als bedoeld in de Wet Financieel Toezicht en voor zover deze diensten onder toezicht staan van de Autoriteit Financiële Markten."
- 80 VAN MIERLO, Thom, "Consumer Protection on the Single Market: Self-Regulation for Dating Services", In: BOELE-WOELKI, Katharina, GROSHEIDE, Willem (Eds.), *The Future of European Contract Law, Liber Amicorum E.H. Hondius*, Kluwer Law International, Alphen aan den Rijn, 2007, 413.
- 81 <http://www.ser.nl/nl/taken/zelfregulering/consumentenvoorwaarden.aspx>.
- 82 VAN MIERLO, Thom, "Consumer Protection on the Single Market: Self-Regulation for Dating Services", In: BOELE-WOELKI, Katharina, GROSHEIDE, Willem (Eds.), *The Future of European Contract Law, Liber Amicorum E.H. Hondius*, Kluwer Law International, Alphen aan den Rijn, 2007, 413.
- 83 LUTH, Hanneke, *Behavioural economics in consumer policy, the economic analysis of standard terms in consumer contracts revisited*, Intersentia, Antwerp, 2010, 265-266.
- 84 LUTH, Hanneke, *Behavioural economics in consumer policy, the economic analysis of standard terms in consumer contracts revisited*, Intersentia, Antwerp, 2010, 266-268.
- 85 CHEN, Mark Allen, "Interactive Contracting in Social Networks", *Cornell Law Review*, Vol. 97, 2011, 1551.
- 86 *Ibid.*, p. 1552.
- 87 *Ibid.*, p. 1553.
- 88 *Ibid.*, p. 1554.
- 89 *Ibid.*, p. 1554.
- 90 IYENGAR, Sheena and LEPPER, Mark, "When Choice is Demotivating: Can One Desire Too Much of a Good Thing?", *Journal of Personality and Social Psychology*, Vol. 79, No. 6, 2000, 995-1006; SCHWARTZ, Barry, *The Paradox of Choice - Why More Is Less*, Harper Perennial, New York, 2004.
- 91 WAUTERS, Ellen, LIEVENS, Eva and VALCKE, Peggy, "D1.2.5: Re-designing & re-modeling Social Network terms, policies, community guidelines and charters: Towards a user-centric approach", EMSOC Project, 2014, available on www.emsoc.be.
- 92 CHEN, Mark Allen, "Interactive Contracting in Social Networks", *Cornell Law Review* Vol. 97, 2011, 1555.
- 93 LUTH, Hanneke, *Behavioural economics in consumer policy, the economic analysis of standard terms in consumer contracts revisited*, Intersentia, Antwerp, 2010, 270.
- 94 LUTH, Hanneke, *Behavioural economics in consumer policy, the economic analysis of standard terms in consumer contracts revisited*, Intersentia, Antwerp, 2010, 270.
- 95 For instance, in the US the ratio between businesses' resources and consumer associations' resources stands at 300:1. See DAYAGI-EPSTEIN, Orit, "Representation of Consumer Interest by Consumer Associations - Salvation for the Masses?", *The Competition Law Review*, Volume 3, Issue 2, 2007, available at <http://www.clasf.org/ComplRev/Issues/Vol3Issue2Art3DayagiEpstein.pdf>, 211.
- 96 *Ibid.*, p. 271.
- 97 <http://www.consumersinternational.org/>.
- 98 PDF/?uri=CELEX:52013DC0401&qid=1397641648895&from=EN.
- 99 34 EUROPEAN COMMISSION, Recommendation on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law, 2013/396/EU, 13 June 2013, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2013_201_R_NS0013&qid=1397641648895&from=EN.
- 100 35 EUROPEAN COMMISSION, Proposal for a Directive of the European Parliament and of the Council on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, COM(2013) 404 final, 2013/0185 (COD), 11 June 2013, available at http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2013/0404/COM_COM%282013%290404_EN.pdf.
- 101 36 VOET, Stefaan, "European Collective Redress Developments", 31 August 2013, available at SSRN: <http://ssrn.com/abstract=2318809>.
- 102 37 See HODGES, Christopher, "Collective Redress: A Breakthrough or a *Damp Sqibb*?", *J Consum Policy*, 37, 2013, 67-89.
- 103 38 HODGES, Christopher, "Collective Redress: A Breakthrough or a *Damp Sqibb*?", *J Consum Policy*, 37, 2013, 87.
- 104 39 HODGES, Christopher, "Collective Redress: A Breakthrough or a *Damp Sqibb*?", *J Consum Policy*, 37, 2013, 67-87.
- 105 40 STADLER, Astrid, "The Commission's Recommendation on common principles of collective redress and private international law issues", *Nederlands Internationaal Privaatrecht*, 4, 2013, 484.

Sebastian Haunss, Conflicts in the Knowledge Society The Contentious Politics of Intellectual Property

Cambridge University Press 2013, ISBN 978-1-107-03642-0

Book Review

by **Axel Metzger**, Dr. iur. (Munich and Paris), LL.M. (Harvard), Professor of Law at the Leibniz University of Hannover, Institute for Legal Informatics, Germany.

© 2014 Axel Metzger

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.org/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Axel Metzger, Book Review: Sebastian Haunss, Conflicts in the Knowledge Society The Contentious Politics of Intellectual Property, 5 (2014) JIPITEC 152, para1

- 1 For a long time, intellectual property law could have been characterized as a secret science practiced by a handful of highly specialized lawyers. However, those days of mostly undisturbed discussions within the epistemic community, as social scientists would call it today, are past, at least since the 1960s when economists started to analyze the incentives and social costs associated with intellectual property rights. Their research results were neglected by the (European) intellectual property research mainstream for a long time, but in the last twenty years they have been widely recognized and discussed. Today intellectual property lawyers, at least those active in academia, are trained to understand and use arguments and models developed by economists. But what is still missing in most scientific works on intellectual property is a mindful reception of social science research efforts in the field. One of the recent studies on IP that is rooted in social science but still bite-sized for legal scholars is Sebastian Haunss' monograph on conflicts in the knowledge society.
- 2 Haunss starts from the basic assumption that IP has become more political in the last decades. This politicization is based on four broad processes: the growing economic importance of knowledge-based industries, the growing internationalization of IP issues, the growing attention towards IP issues by

non-specialists and the trend towards personalize IP. He sees this politicization of IP as part of a more fundamental process of social change that is associated with the knowledge society. The ongoing change in the social structure of the former industrial societies alters the overall structures of social conflicts. These conflicts revolve around two meta issues: inclusion/exclusion and the mode of production of knowledge. After this general part (chapters 1-3, p. 1-93), which provides the reader with a very valuable discussion of current theories of the knowledge society, the author presents four case studies on current conflicts in the knowledge society, namely software patents in Europe (chapter 4), access to medicines (chapter 5), and two shorter studies on pirate parties and creative commons (chapter 6). These case studies are again of high value – especially for readers from law departments. Haunss' reports are based on in-depth research on the actors involved, the creation of their networks and the frames shared by the actors. This analysis not only helps the reader to better understand how the initially dispersed actors have been successful in aggregating new forms of collective actions. It is also useful for legal scholars to get a glimpse into the current methodology used by political scientists. Of special interest are the illustrations of the different networks of actors (e.g. on p. 124-126, 168, 172).

- 3 In his conclusion (chapter 7), Haunss rightly emphasizes that the presented conflicts – despite their obvious differences in terms of issues, protagonists, action forms and geography – are characteristic of the knowledge society and are addressed in a consistent pattern: they all question the existing IP regime and its underlying property order of the knowledge society; they are all transnational; they did not develop along the cleavages of the industrial age, e.g. labour-capital or left-right. Still, Haunss is prudent enough to conclude that these and other similarities do not suffice to recognize the actors in the presented conflicts as the core of a real social movement within the knowledge society. The actors and networks active in the presented conflicts have failed so far to mobilize large constituencies beyond the circle of activists engaged in the specific issues.
- 4 In sum, the study is a clear “must” for all IP specialists with an interest in the political dimension of IP.

Jipitec

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

www.jipitec.eu