jipitec

3 | 2015

Volume 6 (2015)
Issue 3
ISSN 2190-3387

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

www.jipitec.eu

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 6 Issue 3 December 2015
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.,
Humboldt-Universität zu
Berlin, Unter den Linden 6,
10099 Berlin

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

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

ISSN 2190-3387

Funded by

DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Table Of Contents

Editorial

Articles

Case Comment

Editorial

New Cooperation with DGRI

Since its launch in 2010, JIPITEC has been funded by a grant of the German Research Council (Deutsche Forschungsgemeinschaft - DFG). The aim of JIPITEC is to provide a forum for in-depth legal analysis of current issues of intellectual property, information technology and E-commerce law with a key emphasis on European law. Unlike the more traditional law reviews, JIPITEC seeks to develop an information platform that allows authors and users to work closer together. JIPITEC is a peer-reviewed Open Access journal, which connects academics and legal practitioners from all EU Member States, as well as from contributors world-wide.

In order to financially secure the continuation of JIPITEC, the decision was taken to team up with a scientific association in the field of IT. The ideal partner for this cooperative endeavor was found in the German Association for Law and Informatics (Deutsche Gesellschaft für Recht und Informatik - DGRI).

DGRI is the leading professional association in the area of IT law in Germany. It addresses issues that lie at the intersection of informatics and computer technology on the one hand, and law and business, on the other hand. The objective of DGRI is to promote interaction between academia, research, and practice in the following areas: legal issues relating to the processing of information; the use of information technology within the legal system; and shaping the legal framework conditions for information technology. Within its area of interest, DGRI attracts both academics and practitioners seeking an exchange of knowledge, experiences and views.

DGRI resulted from a merger of the German Association for Informatics and Law (DGIR) and the Association for legal and administrative informatics (Gesellschaft für Rechts- und Verwaltungsinformatik - GRVI). After 40 years of existence, DGRI currently has some 750 individual and corporate Members. Further information is available at http://www.dgri.eu/.

Beyond benefitting from a greater array of contributors through this partnership, JIPITEC shall become even more European. To this effect, it is planned as a first step to enlarge the board of editors – already international in its composition – by including an editor from the United Kingdom. Furthermore, JIPITEC could serve as a participatory platform for scientific associations from other EU Member States. At the same time, JIPITEC will assist the DGRI in broadening its contact base within Europe.

The cooperation between JIPITEC and DGRI is initially limited for a trial period of two years. It is, of course, very much hoped that this cooperation will prove to be a solid basis for a flourishing future for both JIPITEC and DGRI as well as for IT law as such.

On behalf of the editors

Thomas Dreier

Axel Metzger

Cultural Heritage Online? Settle it in the Country of Origin of the Work

by **Lucie Guibault***

Abstract: This article examines the conditions under which a system of extended collective licensing (ECL) for the use of works contained in the collections of cultural heritage institutions (CHIs) participating in Europeana could function within a cross-border basis. ECL is understood as a form of collective rights management whereby the application of freely negotiated copyright licensing agreements between a user and a collective management organisation ("CMO"), is extended by law to non-members of the organisation. ECL regimes have already been put in place in a few Member States and so far, all have the ability to apply only on a national basis. This article proposes a mechanism that would allow works licensed under an ECL system in one territory of the European Union to be made available in all the territories of the Union. The proposal rests on the statutory recognition of the "country of origin" principle, as necessary and sufficient territory for the negotiation and application of an ECL solution for the rights clearance of works contained in the collection of a cultural heritage institution, including orphan works.

Keywords: copyright; cultural heritage; extended collective licensing; cross-border access

Recommended citation: Lucie Guibault, Cultural Heritage Online? Settle It in the Country of Origin of the Work, 6 (2015) JIPITEC 173 para 1.

A. Introduction

1 After almost a decade of efforts towards the digitisation of the content of their collections, cultural heritage institutions ("CHIs") across Europe are still in search of a workable solution to the astronomical transaction costs related to the rights clearance for making these works available to the public. In the same time, several legal initiatives at the European level have been put forward in an attempt to address the problem. First, the representatives of rights holders and user organisations, signed in September 2011 the Memorandum of Understanding (MoU) on Key Principles on the Digitisation and Making Available of Out-of-Commerce Works.[1] This MoU concerns the digitisation and dissemination of books and learned journals that are no longer available in commerce. Second, the European Parliament and the Council adopted Directive 2012/28/EC on certain permitted uses of orphan works ("OWD" or "Directive 2012/28/EC"), e.g. works for which the rights holder cannot be identified or located.[2] And third, at the beginning of 2014, the European Commission launched a vast public consultation on the reform of the European copyright regime, enquiring about the public's view on issues such as the rights relevant for digital transmissions, the territoriality of exceptions and the mass-digitisation of works and other subject matter[3] by CHIs[4]. Until the time comes when the European Commission puts forth a proposal for a broader reform of the copyright system, solutions

1 Memorandum of Understanding on Key Principles on the Digitisation and Making Available of Out-of-Commerce Works, Brussels, 20 September 2011, available at: ec.europa.eu/internal_market/copyright/out-of-commerce/index_en.htm.

2 Directive 2012/28/EU of the European Parliament and of the Council of 25 October 2012 on certain permitted uses of orphan works (2012 OJ L 299/5). See: A.M. Beunen & L. Guibault, 'Brussels Memorandum of Understanding inzake digitalisering en online beschikbaarstelling van out-of-commerce boeken en tijdschriften', AMI 2011-6, p. 221-226.

3 For ease of reading, the expression 'work' will be deemed in the remainder of this article to encompass other subject matter covered by neighbouring rights, such as first fixations of performances, phonograms, first fixation of films and broadcast signals.

4 European Commission, DG Internal Market, Report on the responses to the public consultation on the Review of EU Copyright Rules, Brussels, July 2014.

for lawful dissemination of cultural heritage must emerge within the existing legal framework.[5]

2 As Directive 2012/28/EC is rather limited in scope (covering only orphan works) and involves a diligent search process that can be very cumbersome for institutions with larger collections[6], several Member States are looking for a more encompassing solution beyond the transposition of the provisions of the Directive. Among a number of solutions considered as having the potential to address the broader and more general problem of rights clearance of works is the extended collective licensing ("ECL") system. ECL is a form of collective rights management whereby the application of freely negotiated copyright licensing agreements between a user and a collective management organisation ("CMO"), is extended by law to non-members of the organisation. Compared to standard collective rights management, the "extension" of agreements to non-members of a CMO significantly facilitates the licensing process to the benefit of rights owners and users alike: even if not all rights owners are identified, license agreements can still be concluded and remuneration paid, allowing the use to take place under specific conditions. In principle, non-members retain the right to withdraw their rights from the scope of the agreement and to obtain remuneration for the use made of their works at all times.

3 The Scandinavian countries (Norway, Denmark, Sweden and Finland) have a long tradition with the use of ECL for the licensing of mass uses, including for the digitisation and making available of works contained in the collections of CHIs.[7] ECL-type systems were recently introduced in one form or another in France,[8] Germany[9], Slovakia[10], and the United Kingdom.[11] Other Member States, like Estonia[12] and the Netherlands[13], are seriously considering this option upon transposing the provisions of Directive 2012/28/EC in their national legal order.

4 Directive 2012/28/EC does not regulate the adoption of ECL systems, but it does leave the possibility open for Member States to do so. Knowing that the MoU is implicitly based on the establishment of an ECL regime, it is not surprising that Member States look towards this direction for a solution to rights clearance in the context of mass-digitisation projects. From a European perspective, the situation becomes highly problematic however, by the fact that some of the national solutions in place expressly restrict online access to works licensed under these regimes to citizens residing within their national territories. Among the few mass-digitisation initiatives based on ECL, the Norwegian "Bookshelf" project is perhaps the most well-known, since it has been online already for a few years.[14] But anyone accessing the Bokhylla website from outside Norway will see the following notice appear on their computer screen: "Bokhylla.no is a web service that provides users with Norwegian IP addresses access to all books published in Norway until 2000, according to the agreement with Kopinor that underlies the service, users without Norwegian IP address must apply for access for specific uses, primarily research, education and professional translation business. Access is usually granted for a period of 6 months with possibility of extension".[15]

5 The 2011 Commission Staff Working Paper "Impact Assessment On The Cross-Border Online Access To Orphan Works"[16] may not be a stranger to the position adopted by the national legislators to restrict access beyond their borders or at the very

5 European Commission's Report on Digitisation, Online Accessibility and Digital Preservation of Cultural Material, Brussels, September 2014, p. 33.

6 Study 'Assessing the economic impacts of adapting certain limitations and exceptions to copyright and related rights in the EU – Analysis of specific policy options', Brussels, 23.06.2014, p. 18.

7 R. Tryggvadottir, 'Digital Libraries, the Nordic system of extended collective licensing and cross-border use', Auteurs & Media 2014/5, pp. 314-325.

8 Loi No. 2012-287 du 1er mars 2012 relative à l'exploitation numérique des livres indisponibles du XXe siècle, available at : http://www.legifrance.gouv.fr/affichLoiPubliee.do;jsessionid=8327BDD080F8720E7E999784A16219C1.tpdila24v_1?idDocument=JORFDOLE000024946198&type=general&legislature=13.

9 Gesetz zur Nutzung verwaister und vergriffener Werke, Bundesgesetzblatt 8.10.2013, entered into force on 1st April 2014, available at: http://www.dpma.de/service/e_dienstleistungen/register_vergriffener_werke/index.html.

10 Act 283/2014 of 12 September 2014, amending Act No 618/2003 on copyright and rights related to copyright (the Copyright Act), as amended, art. 12c, entered into force on 29 October 2014, available at: http://www.ifrro.org/sites/default/files/2014-283_copyright_act_amendment_orphanooc_works.pdf.

11 Enterprise and Regulatory Reform Act 2013, 2013, c. 24, art. 77; Copyright and Rights in Performances (Extended Collective Licensing) Regulations 2014, No. 2588, available at: http://www.legislation.gov.uk/ukdsi/2014/9780111116890.

12 E. Vasamäe, 'Sustainable Collective Management of Copyrights and Related rights', Dissertation, University of Tartu, 2014.

13 Wijziging van de Auteurswet en de Wet op de naburige rechten in verband met de implementatie van de Richtlijn nr. 2012/28/EU inzake bepaalde toegestane gebruikswijzen van verweesde werken, Tweede Kamer, vergaderjaar 2013–2014, 33 892, nr. 6.

14 V.M. Skarstein, 'The Bookshelf: digitisation and access to copyright items in Norway', Program: electronic library and information systems (44) 2010, p. 48-58.

15 Translation via Google Translate - http://www.nb.no/Tilbud/Lese-lytte-se/Bruk-av-bokhylla.no-i-utlandet.

16 Commission Staff Working Paper Impact Assessment On The Cross-Border Online Access To Orphan Works and Accompanying the document Proposal for a Directive Of The European Parliament And Of The Council on certain permitted uses of orphan works, SEC(2011) 615/2.

least to keep silent on the issue. In this document, the European Commission clearly discards the ECL system as a valid solution for the making available of works throughout the European Union.[17] In the context of the adoption of Directive 2012/28/EC, it is true that an ECL solution does not require an upfront diligent search, and that as such, it does not allow for the positive determination of an orphan works status or the mutual recognition thereof across Europe. However, by choosing the path of ECL instead of the more burdensome orphan works route, CHIs appear to be resolving the problem of rights clearance for contemporary cultural heritage material by blocking access to people located outside of their own territories. Alleviating the transaction costs associated with the rights clearance of works in the collections of CHIs should not be at the expense of cross-border access to digitised material, as this would have negative consequences for projects such as Europeana, and most importantly for European society as a whole.[18]

6 A pragmatic solution to rights clearance should not come at the expense of cross-border access to the digitised material, as emphasised in the fourth recital of Directive 2012/28/EC, "this Directive is without prejudice to that Memorandum of Understanding, which calls on Member States and the Commission to ensure that voluntary agreements concluded between users, rightholders and collective rights management organisations to license the use of out-of-commerce works on the basis of the principles contained therein benefit from the requisite legal certainty in a national and cross-border context". How can this statement be reconciled with reality and how can the last part of the sentence be applied practically?

7 Admittedly, the means of broadening this type of licence scheme to other territories not covered by the national law that prescribes the "extension effect" have yet to be found.[19] This question therefore forms the central focus of this paper: can the application of the principle of "country of origin" constitute a workable basis for the cross-border use of copyright protected works contained in the collections of CHIs in the context of Europeana which is licensed under an extended collective licensing system?

8 To answer this question, this study will compare in section B each element constituting the ECL system in the light of the imperatives of a multi-territorial application. These elements include an analysis of nature of the extension mechanism, requirement of representativeness of CMOs, the opt-out option, the subject matter covered by the agreements, the definition of user groups, the scope of the licence and the conditions of use. Other important characteristics of an ECL regime, such as the need for a CMO to obtain governmental approval for its operations, or the existence of a mediation mechanism for the negotiation of agreements, will not be examined here because of their less immediate consequences on cross-border rights clearance. For the purpose of this study, we will rely heavily on the relevant regulations adopted and in force in Scandinavia, France, Germany, Slovakia and the UK.[20] In the absence of any relevant case law and literature, the analysis will essentially take the legislative documents as a starting point for an examination of the similarities and discrepancies between the constituent elements of the ECL provisions in each Member State, in order to see how they can be reconciled with each other.

9 This comparative analysis will allow us, in section C, to make a proposal for a mechanism that would allow works licensed under an ECL system in one territory of the European Union to be made available in all the territories of the Union. The proposal rests on the statutory recognition of the "country of origin" principle, as necessary and sufficient territory for the negotiation and application of an ECL solution for the rights clearance of works contained in the collection of a cultural heritage institution, including orphan works. To set this proposal into context, section C. I briefly highlights the advantages and drawbacks of two alternative options to the recognition of the "country of origin" principle, namely the full harmonisation of exceptions to the benefit of cultural heritage institutions and the multi-territorial licensing of works. The following section explains how the principle of "country of origin" could be applied on a cross-border basis so as to give every European citizen access to cultural material that is licensed by the CMO of the country that first published the material. Section C.II.1 briefly examines how this proposal would fit within the existing legal framework, both international and European, while section C. II. 2 looks into the practical aspects of the application of the country of origin principle for ECLs. This proposal would need to be implemented at the European level and be accompanied by transparency measures to ensure that potential users have the necessary information

17 Id., p. 18.

18 See recital 23 of Directive 2012/24/EC : 'In order to foster access by the Union's citizens to Europe's cultural heritage, it is also necessary to ensure that orphan works which have been digitised and made available to the public in one Member State may also be made available to the public in other Member States'.

19 Id., p. 27. See also : Study 'Assessing the economic impacts of adapting certain limitations and exceptions to copyright and related rights in the EU – Analysis of specific policy options', Brussels, 23.06.2014, p. 19.

20 The texts of the relevant legislative provisions of Denmark, Finland, France, Norway, Sweden and the United Kingdom can be found in Annex to this report.

for a legitimate and secure cross-border use of the copyright protected material.

10 It is important to note at the outset that the analysis of the possible cross-border applicability of an ECL system and the proposals made in the following pages are designed to apply strictly to the specific purpose of allowing the mass-digitisation and online making available of works by CHIs. It is not our intention to extend the analysis of the cross-border application of an ECL system to any other area than this one, as the respective stakeholder interests may play out quite differently in the context of other types of uses. This article builds on prior studies carried out for Europeana,[21] on the workings of ECL systems and their main characteristics, and the compatibility of the ECL regime with the relevant European legal framework.[22] Because the issue is not directly related to the cross-border application of ECL systems, the article will not discuss the applicability or non-applicability of the Directive on Services to the services offered by CMOs in the European Union.[23]

B. Main characteristics of ECL systems

11 In order to answer the research question, e.g. under which conditions could an ECL system for the use of works contained in the collections of CHIs be workable on a cross-border basis, we must first examine which essential characteristics of an ECL system would likely be significant in a transnational setting in order to allow effective cross border use of cultural heritage collections. This section provides a comparative law analysis of the main characteristics of ECL systems, in particular, the nature of the extension mechanism, the requirement of representativeness of CMOs, the opt-out option, the subject matter covered by the agreement, the definition of user groups, the scope of the licence and the conditions of use. To this end, we will consider the relevant regulations adopted and in force in Scandinavia (namely Norway, Denmark, Sweden and Finland), France, Germany, Slovakia and the UK. As it will become clear below, some of these characteristics have been regulated by law, while others are left to be determined by the parties to the agreement, with the potential of increasing the occurrence of discrepancies between systems.

I. Extension mechanisms

12 Following the Scandinavian model, ECL is a form of collective rights management whereby the application of freely negotiated copyright licensing agreements between a user and a CMO, is extended by law to non-members of the organisation. Therefore, this mechanism of ECL functions in a two-tiered manner: 1) the law recognises the "extended" application of agreements concluded between a CMO and a user to non-members of the CMO; and 2) the parties freely negotiate the content of the agreement. With respect to ECL systems created for the purpose of allowing the mass-digitisation and online making available of works by CHIs, this can be achieved either through a general provision in the copyright act or through a specific provision detailing the purpose and intended beneficiaries. With the adoption of its new provision in the Enterprise and Regulatory Act 2013, the United Kingdom will follow the first approach.[24] Denmark and Sweden have a mix of specific and generic provisions, the latter of which states for example that "[e]xtended collective license may also be invoked by users who, within a specified field, have made an agreement on the exploitation of works with an organisation comprising a substantial number of authors of a certain type of works which are used in [the country] within the specified field".[25]

13 In Finland and Norway, the extension is operated through a more specific provision in the copyright act, which allows an archive, a library or a museum open to the public by virtue of extended collective licence to reproduce and communicate the works in its collections to the public in cases other those specified in the act.[26] Section 26(1) of the Finnish Copyright Act provides that "extended collective licences shall apply when the use of a work has been agreed upon between the user and the organisation which is approved by the Ministry of Education and which represents, in a given field, numerous authors of works used in Finland. A licensee authorised by virtue of extended collective licence may, under terms determined in the licence, use a work in the same field whose author the organisation does not

21 J. Axhamn and L. Guibault, 'Cross-border extended collective licensing: a solution to online dissemination of Europe's cultural heritage?', EuropeanaConnect, Milestone M.4.1.9, 2011; M. Oostveen and L. Guibault, Summary report on IPR issues faced by Europeana and its partners, Europeana Awareness, Deliverable D5.2, June 2013.

22 See also: A. Vuopala, 'Extended Collective Licensing – A solution for facilitating licensing of works through Europeana, including orphans?', Finnish Copyright Society, Helsinki, 2013.

23 See : T. Riis, 'Collecting Societies, competition, and the Services Directive', Oxford Journal of Intellectual Property Law and Practice (2011) 6, pp. 482-493 ; Case C-351/12, Judgment of the Court of Justice of the European Union, 27 February 2014 (OSA vs. Czech Republic).

24 E. Rosati, The orphan works provisions of the ERR Act: are they compatible with UK and EU laws?, E.I.P.R. 2013, 35(12), 724-740.

25 Danish Copyright Act 2010, art. 50(2).

26 Finnish Copyright Act 2005, art. 16d. See Norwegian Copyright Act, art. 16a.

represent".

14 The Slovakian system follows a similar system, as article 12c(6)(6) of the Slovakian Copyright Act states that:

> *If an author has not explicitly opted out of collective management of his rights, the user is entitled to use the out-of-commerce work by making copies, making the work available to the public or publicly distributing copies by sale or other forms of assignment of title under an agreement concluded with the relevant collective management organisation representing a significant number of authors for works under paragraph (1), even if the collective management organisation does not represent the author for the out-of-commerce work.*

15 By contrast, the systems established in Germany and Slovakia do not explicitly extend the application of collective licensing agreements concluded between the CMO and the user to non-members. Section 13d(1) of the Collective Administration Act establishes an ECL-type system for the licensing of out-of-commerce books by extending the CMO's mandate to represent non-members. Through this provision, a collecting society entrusted with the exploitation of the rights of reproduction (§ 16 of the Copyright Act) and making available to the public (§ 19a of the Copyright Act) of out-of-print books, is presumed authorised to license to third parties within the scope of their activities the rights of right holders who have not entrusted the collecting society with the exercise of their rights.

16 The French mechanism mandates the *Société française des intérêts des auteurs de l'écrit* (SOFIA) with respect to the rights of authors and publishers on unavailable books published in France before 1st January 2001 on the basis of article L. 134-3 and adherence to the Intellectual Property Code. Books are unavailable if they are no longer subject to commercial distribution by a publisher and are not currently the subject of a publication in print or digital. The Sofia is entrusted with administering the rights on the unavailable books that are placed on a list drawn up annually and held by the National Library of France. The Sofia was established in 1999 by the merger of the *Société des Gens de Lettres* (SGDL) and the *Syndicat National de l'Édition* (SNE). As such, the Sofia is likely to partly represent the rights of the authors and publishers of these unavailable books, but most likely also of non-members.

17 Whether the extension is effectuated at the level of the licensing agreement or at the level of the CMO's mandate, the effect on a non-member is presumably the same as long as the conditions of representativeness of CMOs, the right to opt-out, and the right to obtain separate remuneration are guaranteed.

II. Representativeness of CMOs

18 Arguably, the primary requirement of the entire ECL system is that the CMO be representative of the group of rights holders in the same category as the rights of whom it administers.[27] According to this requirement, a CMO can only negotiate an agreement with a cultural heritage institution with a degree of certainty if it can demonstrate that it does administer the rights on behalf of a "substantial" amount of rights owners in the same category than those it administers.[28] In the impact assessment to Directive 2012/28/EC, the Commission stressed that "[b]ecause the legal presumptions that a representative collecting societies also represents orphan works only applies in the national territories that introduce such a presumption, this option only allows the display of orphan works within the territory of a Member State. Digital libraries operating with an extended collective licence would therefore only be accessible at national level".[29]

19 The representative character of the CMO is a question of legitimacy towards the non-members and of legal certainty towards the users: 1) a "representative" CMO will speak on behalf of a large enough number of rights holders to legitimise the application of the agreement to all rights owners, including non-members; 2) a representative CMO will be able to grant a licence with broad coverage of the repertoire, which increases the legal certainty for the users. A CMO with a low representation rate cannot feign negotiating a legitimate agreement with users on behalf of all rights holders, nor can it give any assurance to the user that the repertoire covered is sufficiently important to reduce the risk of having a (large number of) non-members opt-out from the agreement.

20 When one examines the body of works and performances that qualify as "cultural heritage" and are contained in the institutions' collections, an important part of these may be quite old. How is the representative character of a CMO to be established? Which criteria should it follow? Is a CMO deemed representative if it represents the rights of a substantial portion of rights holders whose works are currently being managed? Or should the representative character be determined in relation

27 Tryggvadottir 2014, p. 317.

28 P.B. Hugenholtz, S. van Gompel, L. Guibault and R. Obradovic, 'Extended Collective Licensing: panacee voor massadigitalisering?', Report commissioned by the Dutch, Ministry of Education, Culture and Science, Amsterdam: Institute for Information Law, August 2014, p. 16.

29 Commission Staff Working Paper Impact Assessment On The Cross-Border Online Access To Orphan Works and Accompanying the document Proposal for a Directive Of The European Parliament And Of The Council on certain permitted uses of orphan works, SEC(2011) 615/2, p. 27.

to the amount of rights holders whose works make up the body of the "cultural heritage"? While the latter option would in theory be more logical in terms of legitimacy and legal certainty, it would entail an almost insurmountable burden of proof on the part of the CMO who would need to establish that it represents a sufficiently high number of heirs and other assignees on the old works and performances. This, in our opinion, would not reflect the intention of the legislator.

1. Assessment of representative character

21 There is no clear criterion for the assessment of the representative character of a CMO. Neither the French nor the German copyright acts contain any specific requirements regarding the representative character of a CMO entrusted with licensing works under an ECL regime. However, in both countries the CMO engaged in ECL licensing must be authorised by a competent public authority: in France, by the Minister of Culture and in Germany, by the Patents and Trademark Office (Bundespatentamt). The French Code requires that the mandate to manage the rights on unavailable books be given to a collective management organisation that can attest to a diversity of the members of the organisation as well as of an equal representation of authors and publishers among the partners and within the governing bodies of the organisation. The Sofia declares that it brings together nearly 8,000 authors and 400 publishers representing 85% of sales of the French edition.[30] Pursuant to article 3 of the German Copyright Administration Act (UrheberWarhnehmungsgesetz), the Patents and Trademark Office must grant such authorisation upon submission of evidence of the amount of rights owners represented by the organisation. The consequence of a lack of proper evidence regarding this point is not clear from the Act, but it is reasonable to assume that should the Patents and Trademarks Office entertain doubt as to the representative character of a CMO, it would withhold or withdraw the authorisation.[31]

22 Arguably, as the "extension effect" is operated at the level of the CMO's mandate, rather than at the level of the agreement, the requirement of representativeness is perhaps less important. But even if the CMO is the only one active in the specific territory, it would be an error, in my opinion, to take the representative character of that CMO for granted: in the interest of legitimacy towards non-members and legal certainty towards users, a CMO should at all times be able to establish its representative character. Being the sole CMO in the territory is no guarantee.

23 By contrast, representativeness of CMOs is an important aspect of ECL regimes in Scandinavia, where the CMOs must represent a "significant" (Sweden)[32] or "substantial part of the authors" (Norway) or even "numerous authors" (Finland)[33], "of a certain type of works which are used in [the country] within the specified field".[34] The Danish Copyright Act, for example, requires that the CMO engaging in ECL agreements present a "substantial number of authors of a certain type of works which are used in Denmark within the specified field". The law does not further specify what "substantial number" means in practice.[35] The legislative history of this provision indicates that the requirement of "a substantial number of authors" does not mean that the CMO must represent a "majority" of rights owners within the specified field. Rather, the amount of rights owners represented should be "important" or refer to a "plurality" of authors. The Danish Ministry of Culture assesses the representativeness of the CMO upon giving its approval to the agreement, as required by law, on the basis of the evidence submitted by the CMO. In Norway the law was modified in 2005 from its original text, which obliged CMOs to represent a "substantial part of Norwegian authors of a certain type of works". This formulation was deemed to be in conflict with the EU Treaty as a form of non-acceptable discrimination on the basis of nationality.[36]

24 On the model of the Scandinavian provisions, the Slovakian Copyright Act also refers to a "relevant collective management organisation representing a significant number of authors for works". As this provision has only recently been introduced in the Copyright Act, little information is known regarding

30 http://www.la-sofialivresindisponibles.org/2015/index.php.

31 P.B. Hugenholtz, S. van Gompel, L. Guibault and R. Obradovic, 'Extended Collective Licensing: panacee voor massadigitalisering?', Report written to the Dutch, Ministry of Education, Culture and Science, Amsterdam: Institute for Information Law, August 2014, p. 54.

32 Swedish Copyright Act, art. 42a.

33 Article 26 of the Finnish Copyright Act requires that the organisation 'represents, in a given field, numerous authors of works used in Finland'.

34 Tryggvadottir 'Digital Libraries, the Nordic system of extended collective licensing and cross-border use', Auteurs & Media 2014/5, p. 318.

35 Freudenberg 2014, WahrnG § 2, Rn. 6, in: H. Ahlberg & H.-P. Götting, Urheberrecht, Beck'scher Online Kommentar (ed. 4, 1 juli 2014).; Hugenholtz et al. 2014, p. 25.

36 J. Axhamn & L. Guibault, 'Cross-border extended collective licensing: a solution to online dissemination of Europe's cultural heritage?', final report prepared for Europeana-Connect, Amsterdam: Institute for Information Law, August 2011, p. 30-31; A. Vuopala, Extended Collective Licensing – A solution for facilitating licensing of works through Europeana, including orphans?, Finnish Copyright Society, Helsinki, 2013, p. 14.

its actual workings.

25 The UK Copyright and Rights in Performances (Extended Collective Licensing) Regulations 2014[37] establish a system of government approval of ECL licences. Pursuant to article 4(4) of the Regulations, "[t]he Secretary of State may only grant an authorisation to a relevant licensing body if the Secretary of State is satisfied that — (b) the relevant licensing body's representation in the type of relevant works which are to be the subject of the proposed Extended Collective Licensing Scheme is significant". This provision must be read in conjunction with the definition in article 2 of the Regulation of "representation", which means the extent to which the relevant licensing body currently — (a) acts on behalf of right holders in respect of relevant works of the type which will be the subject of the proposed Extended Collective Licensing Scheme; and (b) holds right holders' rights in relevant works of the type which will be the subject of the proposed Extended Collective Licensing Scheme.

26 Questions regarding the topic of representativeness were put to the public in a consultation prior to the adoption of the Regulations. In its response to the consultation, the UK government were of the opinion that the representativeness test should be flexible, since requiring absolute thresholds could prevent ECL schemes from emerging where they are needed most. The government added that "Collecting societies must show that they made all reasonable efforts to find out total numbers of rights holders and works, using a transparent methodology. A poor understanding of the total numbers of rights holders and works will necessarily entail an incomplete publicity campaign, which in turn will mean that rights holders who might want to opt out may not be able to."[38] According to the Regulations, the CMO must also show that it has the support of a significant proportion of its members for the application ECL scheme.

27 How would one calculate the degree of representativeness of a CMO at the European level? Admittedly, it would be very difficult and depend on a few factors. Among the most important factors to help determine the representative character of a CMO is whether the CMO has signed reciprocal agreements with sister organisations abroad to represent their foreign repertoire on the CMO's own territory.[39]

28 In the case where the CMO has signed no reciprocal arrangement with sister societies, it would be virtually impossible to determine the representative character of the CMO outside of its own boundaries. There would likely be an overlap between the potential non-members of two organisations that do not have a reciprocal representation agreement. This essentially means in practice that non-members would be entitled to opt-out separately from both organisations and claim remuneration for the use of their works at both organisations.

2. Scope of mandate of CMO

29 For the purposes of authorising an ECL regime, the representative character of a CMO is generally assessed in relation to the "number of authors of a certain type of works which are used in [the country] within the specified field". Article 50(3) of the Danish Copyright Act specifies that "[t]he extended collective licence gives the user right to exploit other works of the same nature even though the authors of those works are not represented by the organisation". The part of the representativeness criterion relating to the user's "right to exploit other works of the same nature" directly concerns the CMOs mandate and its capacity to grant licences with respect to the rights it administers. This aspect of the representative character of the CMO must be neither overlooked nor underestimated, because it is at the core of the ECL system: to be entitled to grant licences in the first place, whether on behalf of non-members or not, the CMO must be entrusted by its members with an explicit mandate to represent specific rights. Although this question is not specific to the cross-border application of ECL arrangements, the issue of the mandate of a CMO is as crucial for the good functioning of an ECL scheme as the number of authors represented is. In the context of the digitisation and dissemination of presumably old(er) cultural heritage material, the question whether the CMO has obtained from the rights owners, their heirs or assignees, the necessary mandate to administer the digital rights on these older works is very relevant.

30 This problem arose in a particularly acute way in Germany where, prior to 2008, the Copyright Act expressly prohibited the transfer of rights in relation to new types of exploitation. It was therefore clear that there was a significant gap in the mandate of the German CMOs in terms of digital exploitation

37 The Copyright and Rights in Performances (Extended Collective Licensing) Regulations 2014, available at: http://www.legislation.gov.uk/ukdsi/2014/9780111116890.

38 Intellectual Property Office, Government response to the technical consultation on draft secondary legislation for extended collective licensing (ECL) schemes, UK, May 2014, p. 5.

39 Tryggvadottir 'Digital Libraries, the Nordic system of extended collective licensing and cross-border use', Auteurs & Media 2014/5, p. 317.

rights on old(er) works.[40] This was solved in Germany with the adoption of section 137L of the German Copyright Act, which states:

> *(1) Where between 1 January 1966 and 1 January 2008, the author has granted another person all essential exploitation rights, exclusively as well as without limitation of place and time, the exploitation rights which were not known at the time the contract was concluded shall be deemed also to have been granted to the other person, so far as the author does not indicate to the other person that he objects to such exploitation. In respect of types of exploitation that were already known on 1 January 2008 the objection may be made only within one year. Otherwise the right of objection shall expire after three months have elapsed since the other person sent the author, at the address last known to the sender, the information concerning the intended commencement of the new type of exploitation of the author's work. The first to third sentences shall not apply to exploitation rights which have become known in the meantime and which the author has already granted to a third person.*[41]

31 Since the laws of the other countries examined in this paper did not expressly prohibit the transfer of rights relating to new forms of exploitation, the ownership of digital rights remains unclear. The French Government chose a rather controversial route to solve the problem: pursuant to article L. 134-6 of the Intellectual Property Code, as introduced by Act No. 2012-287, the burden of proof lies on the authors to establish that they are the sole rights owners of digital rights on non-available works.[42] While the legal validity of the French scheme established by Act No. 2012-287 was upheld by the Conseil Constitutionnel,[43] two French authors pursued the litigation by presenting the case to the Conseil d'état, who then filed a request for preliminary ruling with the Court of Justice of the EU. The case is still pending.[44] The UK legislator foresaw the possible occurrence of doubt regarding the mandate of a CMO and this is why the Regulations (Extended Collective Licensing) 2014 demand that the CMO has obtained the required consent from its members to the proposed Extended Collective Licensing Scheme.[45] In view of the potential difficulties arising from a dubious mandate at the national level, the problem becomes unpalatable if amplified at the European level.

32 Another area of possible friction for the cross-border application of an ECL scheme concerns not the number of rights owners represented, nor the rights included in the mandate, but the category of rights owners represented. In the Netherlands, for example, the CMO in charge of administering the rights of authors of writings (books, newspaper/magazine articles, screenplays etc.) LIRA, exercises the rights of literary authors, but not those of publishers. The latter prefer exercising their rights individually. What would this mean in a cross-border setting? It would certainly not indicate that foreign publishers would be able to be considered as non-members, even if in other countries' CMOs do administer the rights of publishers in this field. With respect to LIRA, only foreign authors would be able to claim this status. This example demonstrates how fragmented the administration of rights is and how difficult it would be to extend the application of a particular ECL scheme beyond the boundaries of the national territory.

III. Opt-out option

33 A second key element of a legitimate ECL regime is the possibility for non-member rights holders to withdraw from the scheme at will. Not all existing ECL schemes in Scandinavia offer this option to rights owners. In particular cases, such as broadcasting and cable retransmission, the legislator considered that it would be unwise to give non-members a right of withdrawal as it would create important holes in the repertoire of the CMO and hinder the operations of the cable distributors.[46] Nevertheless, together with the free negotiation of ECL agreements between the CMO and the user(s), the opt-out option is recognised as the element that makes the difference between a mandatory licence and an ECL system. Without the possibility to withdraw from the regime, the non-members would lose control over the use of their

40 N. Klass, 'Die deutsche Gesetzesnovelle zur "Nutzung verwaister und vergriffener Werke und einer weiteren Änderung des Urheberrechtsgesetzes" im Kontext der Retro-digitalisierung in Europa', GRUR Int. 2013, p. 881-894; U. Fälsch, 'Verträge über unbekannte Nutzungsarten nach dem Zweiten Korb: die neuen Vorschriften § 31 a UrhG und § 137 l UrhG', Bibliotheksdienst 2008-4, p. 411-419.

41 Zweites Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft" vom 26. Oktober 2007 (BGBl. I/2007, S. 2513 ff.); in force as of 1st January 2008.

42 Loi No. 2012-287 du 1er mars 2012 relative à l'exploitation numérique des livres indisponibles du XXe siècle.

43 Conseil Constitutionnel Decision No. 2013-370 QPC of 28 February 2014.

44 Case C-301/15, Court of Justice of the EU, pending - where the French Conseil d'état asked: 'Do the provisions, referred to above, of Directive 2001/29/EC of 22 May 2001, 1 preclude legislation, such as that analysed in paragraph 1 of this decision, that gives approved collecting societies the right to authorise the reproduction and the representation in digital form of 'out-of-print books', while allowing the authors of those books, or their successors in title, to oppose or put an end to that practice, on the conditions that it lays down?'.

45 The Copyright and Rights in Performances (Extended Collective Licensing) Regulations 2014, art. 4(4)f).

46 J. Axhamn & L. Guibault, 'Cross-border extended collective licensing: a solution to online dissemination of Europe's cultural heritage?', final report prepared for Europeana-Connect, Amsterdam: Institute for Information Law, August 2011, p. 28.

works, meaning that they would no longer be able to exercise their exclusive rights. An ECL system without the possibility to opt-out would be akin to a mandatory licence.

34 With respect to ECL systems that are used for the digitisation and dissemination of cultural heritage, the law of all countries under review in this article do grant non-members a right to opt-out. This is the case in Sweden and Denmark, where the ECL agreement concluded for this special purpose, is based on a generic ECL provision in the Copyright Act. Articles 42a and 42d of the Swedish Copyright Act states that "the provisions of the first Paragraph do not apply if the author has filed a prohibition against the making of copies or the making available with any of the contracting parties or if there are otherwise specific reasons to assume that the author would object to the exploitation". The Danish Copyright Act is to the same effect.[47] This observation is also the case in Finland, where the ECL agreement is based on a specific provision in the Copyright Act, which expressly declares that the provisions are not applicable "to a work whose author has prohibited the reproduction or communication of the work". In Norway, by contrast, the possibility to opt-out from an ECL arrangement is left to the determination of the contracting parties.[48]

35 The Slovakian provision also specifically sets as a condition for the application of the regime for out-of-commerce books, that the author has not explicitly opted out of collective management of his rights. Authors must object within three months of the filing of the proposal for insertion into the Slovak National Library list. At all times, an author may request to remove an out-of-commerce work from the list. The Slovak National Library shall remove an out-of-commerce work without undue delay from delivery of the written request from an author pursuant to the first sentence, or after delivery of notification by a collective management organisation on an author's opting out of collective rights management pursuant to paragraph (6).

36 The French and German ECL schemes for the digitisation and dissemination of out-of-commerce books also grant rights owners the possibility to withdraw from the regime. In both countries, authors have the right to oppose the inscription of their work in the register of out-of-commerce works. However, in France the permissible time-frame is within six months from the date of inscription, while in Germany it is six weeks. In addition, the rights owner has the right to withdraw their works from the repertoire at all times in France and Germany, although the procedure to be followed under French law appears to be more complex and detailed than in Germany.[49]

37 The UK Enterprise and Regulatory Reform Act 2013, confers on the copyright owner the right to limit or exclude the grant of licences by virtue of the regulations. The (Extended Collective Licensing) Regulations 2014 defines "opt out arrangements" as the steps to be followed by a right holder to limit or exclude the grant of licences under an Extended Collective Licensing Scheme.[50] This statement is completed by two provisions in the Regulations: article 5 (1)(g), according to which "the opt out arrangements that the relevant licensing body will adopt including the steps which a non-member right holder is required to take to opt out of a proposed Extended Collective Licensing Scheme before the scheme commences and whether the consent of the Secretary of State is sought as described in regulation 16(5)(b)"; and article 16 of the same Regulation, which set out in great detail when and how a copyright owner may opt-out of an ECL scheme.

38 To sum-up, an opt-out option for non-members is available in virtually all countries examined here, albeit not for every ECL scheme in force. All opt-outs must be recorded, either by the CMO itself (like in Germany) or by a competent authority (like in France), which in principle should ease cross-border consultation by users, as long as this information is publicly accessible.

IV. Subject matter

39 Depending on the country examined, the subject matter covered by an ECL system is determined either in the law or by the parties to an ECL agreement. Of the eight countries studied here, France, Germany and Slovakia have the ECL system with the narrowest scope of application in terms of works covered, since by law these systems apply only to works that are no longer available in commerce, in line with the MoU. Hence, the German provision on out-of-commerce works, § 13d) of the Collective Administration Act exclusively concerns books, journals, newspapers, magazines or other writings published before 1966. The French Act No. 2012-287 on non-available works applies even more strictly to books (excluding any other print material) published

47 P.B. Hugenholtz, S. van Gompel, L. Guibault and R. Obradovic, 'Extended Collective Licensing: panacee voor massadigitalisering?', Report written to the Dutch, Ministry of Education, Culture and Science, Amsterdam: Institute for Information Law, August 2014, p. 25.

48 Id. p. 39.

49 Urheberwahrnehmungsgesetz, section 13d (2) ; Code de la propriété intellectuelle, art. L.134-6.

50 The Copyright and Rights in Performances (Extended Collective Licensing) Regulations 2014 No. 2588.

in France before 2001. The Slovakian ECL system applies, like the German and French mechanisms, to "out-of-commerce works", defined in article 12c(1) as a published literary work in written form, in particular a book, magazine or newspaper, copies of which can no longer be acquired through paid transfer of ownership rights and are held by a library, archive or museum, and are inscribed in the publicly accessible list of out-of-commerce works kept by the Slovak National Library.

40 By contrast, where the ECL schemes in other countries are based on a generic ECL provision in the Copyright Act, the determination of the subject matter covered by the scheme is left up to negotiation by the parties. For example, this will be the case of any ECL scheme that will be established pursuant to the recently adopted UK (Extended Collective Licensing) Regulations 2014. The contracting parties to an ECL arrangement based on article 50(2) of the Danish Copyright Act or article 42h of the Swedish act would also need to identify the subject matter covered by the extended licence. On the other hand, an ECL agreement concluded on the basis of article 16b of the Danish Act would only concern articles from newspapers, magazines and composite works, brief excerpts of books and other published literary works, as well as illustrations and music reproduced in connection with the text; while an ECL agreement based on article 30a of the act would cover works, which have been made public and are part of the own TV productions of the public broadcasters, provided these works were integrated in the broadcast productions before January 1, 2007.[51] Of course, the list of works can be shortened by the parties if necessary. In Norway the Bokhylla project is the result of an agreement between the Norwegian CMO, Kopinor, and the National Library, based on article 16a of the Norwegian Copyright Act. Since the provision does not specify the exact type of works falling under the provision, the parties have concluded an agreement covering Norwegian books published in the periods between 1790-1799, 1890-1899, 1990-1999.

41 The diversity of provisions existing in the several jurisdictions leads in practice to the negotiation and conclusion of a variety of arrangements covering different types of works. Moreover, through law or contractual arrangements, the coverage of certain subject matter under certain ECL schemes is dependent on a particular cut off date.

V. Definition of user group

42 The general or specific character of the ECL enabling legal provision also affects the definition of the user group. The French Act No. 2012-287 creates a unique regime among the ones discussed in this paper, for it allows publishers to obtain a licence from the designated CMO to digitise and commercialise books that have been inscribed in the special register for "unavailable" works maintained by the Bibliothèque nationale de France.

43 Where the digitisation and making available of works is made possible on the basis of a generic ECL provision, the user group will be determined by the contracting parties to the ECL agreement as part of the negotiations. The UK (Extended Collective Licensing) Regulations 2014 actually says nothing about the potential recipients of the licence – all rules and measures included therein are directed at the licensing body, e.g. the CMO, and the protection of the rights holders. As the UK Regulations have only been very recently adopted, no ECL regime has been put in place yet. Nonetheless, the user group will inevitably have to be defined inside a future ECL arrangement. The same holds true in Slovakia and Germany, where the identity of the user group is unclear. The user group may or may not be identical to the institutions that keep the works. These would include libraries, educational institutions, museums, archives and in the field of audiovisual, film or audio heritage institutions. This enumeration would coincide with the list of beneficiaries with the exception of the use of orphan works under Directive 2012/28/EC; however, the Slovakian Act speaks of an undefined "user".

44 As Danish and Swedish law contain both specific and generic provisions allowing the extension of negotiated agreements, the definition of the user group will depend on the provision used as a basis for the agreement. Only small-scale digitisation projects have so far been set up in Denmark on the basis of the generic ECL provision. These concern the digitisation of the Danish Biographic Lexicon, of a dictionary of old Norwegian prose, of issues of the scientific journal KRITIK published between 1967-2011, and of older versions of the journal "IngeniØren".[52] The user groups in these cases were defined per agreement. Specific ECL provisions will tend to provide some indication of the intended user group: article 16b of the Danish Copyright Act, for example, is aimed at "public libraries and other libraries financed in whole or in part by the public authorities". In the case of article 30a of the Danish act the user group consists of the public broadcasting archives. Article 42d of the Swedish Copyright Act provides for the possibility to negotiate an extended collective licence for certain archives and libraries. But this provision refers back to article 16 of the

51 P.B. Hugenholtz, S. van Gompel, L. Guibault and R. Obradovic, 'Extended Collective Licensing: panacee voor massadigitalisering?', Report written for the Dutch, Ministry of Education, Culture and Science, Amsterdam: Institute for Information Law, August 2014, p. 28.

52 Id., p. 30.

same act for further specification of the intended user group, where paragraphs 3 and 4 state:

> *Entitled to the making of copies, and to the distribution, pursuant to the provisions of this Article are*
>
> *1. governmental and municipal archival authorities,*
>
> *2. such scientific and research libraries that are operated by public authorities, and*
>
> *3. public libraries.*
>
> *The Government may in specific cases decide that also certain archives and libraries other than those mentioned in the third Paragraph shall be entitled to make copies pursuant to this Article. (Act 2013:691).*

45 Article 16a of the Norwegian Copyright Act is perhaps much less detailed than its Swedish counterpart – simply speaking of "archives, libraries and museums" – but it is broader than the Swedish provision as it also includes museums. Article 16b of the Finnish Act is comparable to the Swedish provision in terms of detail but, like the Norwegian Act, it counts museums among the potential users:

> *provisions may be issued by Government Decree regarding the archives and the libraries and museums open to the public which are authorised under these sections to use works, or who may apply the provisions on extended collective license, if*
>
> *1. the activities or mission of the institution has been enacted by an Act;*
>
> *2. the institution has been assigned a specific archival, preservation or service function in legislation;*
>
> *3. the activities of the institution serve scientific research to a significant degree; or*
>
> *4. the institution is owned by the State.*

46 It is clear from the above description of the different ECL provisions in the national legislation that some overlap exists in the definition of the user groups benefitting from the application of ECL agreements for the digitisation and making available of works held in the collections of CHIs. But the overlap is not flawless and some jurisdictions set greater restrictions than others with respect to the same categories of users, while other jurisdictions choose to exclude certain categories of CHIs from the application of the ECL arrangements all together (Sweden for example). Also worth bearing in mind is that some copyright acts leave the definition of the user group up to the negotiation of the parties.

VI. Scope of licence

47 Under the ECL regimes created on the basis of the generic ECL provision in the Danish, Swedish and British copyright act, it is up to the parties of the ECL agreement to negotiate the scope of the licences for the use of works by CHIs. Indeed, according to the UK Regulations, "permitted use" means the acts restricted by copyright or protected by neighbouring rights. This formulation can support a very broad application, depending on what the contracting parties agree to. At the extreme opposite of this spectrum is the French Act that allows publishers who have obtained a licence from the designated CMO to digitise and make digitised books available to the public under specific conditions.

48 In between these two extremes lies the legislation of the other Member States. In Finland an ECL agreement based on article 16d authorises the licensee to make a copy of a work in its collections and to communicate that work in cases other than those referred to in sections 16a-c. This essentially means that parties to an ECL arrangement will be able to conclude an agreement on a broad range of acts, including once digitised making available to the public of the works held in the archive, library or publicly accessible museum. The specific ECL provisions of Denmark, Norway and Sweden are to the same effect.[53] In Germany, a licence obtained from a CMO pursuant to § 13d) of the Collective Administration Act will allow the licensee to replicate and make the works available to the public. Any other specific restrictions on these acts will need to be negotiated by the parties.

VII. Conditions of use

49 Conditions of use of works are commonly defined through negotiation, the most important conditions being the payment of a fee by the CHIs or other user group, the purpose of the use – whether commercial use is allowed or not – and the duration of the agreement.

1. Payment of a fee

50 Determining the appropriate level of remuneration for acts of digitisation and making available of works contained in the collections of CHIs is by no means a straightforward task. As Hugenholtz and Korteweg explain, there are essentially two modes of calculation for fixing the level of remuneration in this case: either the fee is based upon the actual use by end users of the material made available online, or it is based upon the expected usage by

53 Id., p. 26.

end users and the expected (social) value of that use.[54] In practice, it is not uncommon to see that the amount of remuneration is determined on the basis of the operating budget of the user institution. The remuneration can be established on the basis of a one-time payment or an annual fee. The amount of money collected by the CMO from the payment of fees by the CHIs will be distributed to rights owners according to the usual distribution key.[55] Non-members have in principle the same rights and obligations as authors represented by the organisation. This principle is in fact confirmed by article 7 of Directive 2014/28/EC on the collective management of copyright and related rights.[56]

51 The only reference in the national legislation to the aspect of remuneration in an ECL scheme concerns the rights of non-members.[57] The Norwegian and Swedish acts expressly recognise the right of the non-members to claim remuneration for the exploitation, provided he or she forwards the claims within three years from the year in which the work was exploited. Claims for remuneration may be directed only towards the organisation. The UK (Extended Collective Licensing) Regulations 2014 are essentially to the same effect.

52 Leaving the French regime aside since it concerns the commercial exploitation of out-of-commerce books by publishers, a digitisation project based on an ECL provision must still be established in the UK and Slovakia. The two relevant German collective rights management organisations, VG Wort and VG Bild-Kunst, signed a collective agreement at the end of 2014 with the Federal Government and the government of every local state.[58] According to this agreement, the public libraries concerned must pay remuneration for the use of the books once, following an upwards scale starting at € 5 for books published before 31st December 1920, € 10 for books published between 1st January 1921 and 31st December 1945 and € 15 for books published between 1st January 1946 and 31st December 1965 (excluding 7% tax). Works in the public domain are exempt from payment.

53 Apart from the smaller-size projects set up in other Scandinavian countries, the main exception is the Norwegian Bokhylla project. In this project, Kopinor receives an annual fee based on the number of digital pages made available. The actual degree of use by end users plays no role in the determination of the fee. Initially set at NOK 0,56 (for 2011) per page, the fee has been reduced constantly in subsequent agreements to NOL 0,36 (for 2013), NOK 0,35 (for 2014) and NOK 0,34 (for 2015 and following). For CHIs with very large collections, this amount may appear excessive. Even for smaller-size collections, this fee structure may be very expensive, if the institution has little financial means at its disposal. Taking the Bokhylla project as an (only) example, the European Commission discarded ECL as a viable option in the Impact Assessment accompanying Directive 2012/28/EC in no unequivocal terms: "it would be extremely costly for the libraries to purchase such a licence".[59] One important element that the European Commission overlooked is that the Norwegian fee structure need not be the only fee structure for all digitisation and dissemination projects in every Member State and that parties to ECL agreements may very well come to different arrangements.

2. Non-commercial use

54 In a few cases, the national law will require – following the model of article 5(2)c) of Directive 2001/29/EC on copyright in the information society allowing acts of reproduction by publicly accessible libraries, archives and educational institutions – that the acts of digitisation and making available by CHIs pursuant to an ECL scheme do not pursue any commercial purpose. For example, § 13d) of the German Collective Administration Act sets as a condition that the acts of reproduction and making available of the works to the public, authorised pursuant to the ECL mechanism, serve only non-commercial purposes. The Finnish Copyright Act also limits the application of ECL mechanism to non-commercial purposes. The laws of the other Scandinavian countries, by contrast, make no reference to the commercial nature of the uses permitted on the basis of the generic or specific ECL provisions. The only consequence for the parties

54 P.B. Hugenholtz, D.A. Korteweg, with the collaboration of J. Poort, 'Digitalisering van audiovisueel materiaal door erfgoedinstellingen: Modellen voor licenties en vergoedingen', report commissioned by Images for the Future/Knowledgeland, Amsterdam, April 2011.

55 See UK (Extended Collective Licensing) Regulations 2014, art. 18.

56 Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market Text with EEA relevance, OJ L 84, 20.3.2014, p. 72–98.

57 T. Koskinen-Olsson, 'Collective management in the Nordic countries', in: D. Gervais (ed.), Collective Management of Copyright and Related Rights (2nd ed.), Alphen aan den Rijn [etc.]: Kluwer Law International 2010, pp. 283-306, at p. 294-295.

58 Rahmenvertrag zur Nutzung von Vergriffenen Werken in Büchern, 16 December 2014, available at: http://www.bibliotheksverband.de/fileadmin/user_upload/DBV/vereinbarungen/2015_01_RV_vergriffene_Werke.pdf.

59 Commission Staff Working Paper Impact Assessment On The Cross-Border Online Access To Orphan Works and Accompanying the document Proposal for a Directive Of The European Parliament And Of The Council on certain permitted uses of orphan works, SEC(2011) 615/2, p. 28.

will be regarding the determination of the level of remuneration: if the user expects to make a profit from the use of the work, then the fee should be set higher than if the use is purely for non-profit activities.

3. Duration of agreement

55 In the Impact Assessment on Directive 2012/28/EC, the European Commission identified the limited duration of ECL systems, which are often around five years, as a disadvantage against the broad application of ECLs for purposes of digitising and disseminating cultural heritage works. According to the Commission, CHIs would need licences that span over a longer period of time to be able to spread the costs and plan their collections. Although the reasons for wanting a longer period of application of an ECL agreement can hardly be disputed, it is difficult to see why this fact would weigh so much against the introduction of an ECL system in the eyes of the Commission. Indeed, a fee calculated over a specific timeframe will allow parties to anticipate the expected use. As Hugenholtz and Korteweg explain "the advantage of this method is the security it offers to both parties with regard to the duration of the licence. The cultural heritage institution can then from the very start of a digitisation project reserve the amount that reflects the practical value for the relevant period".[60]

56 As the duration of the agreement is commonly determined through negotiation, the national laws are mostly silent regarding the duration of ECL arrangements. By contrast, new article L. 134-3 of the French Intellectual Property Code allows the reproduction and making available of the unavailable work, provided remuneration is paid, that the licence is non-exclusive and that the agreement does not exceed a duration of five years. Similarly, the permission granted by the Secretary of State under the new UK (Extended Collective Licensing) Regulations 2014 is in principle valid for a maximum of five years.

60 P.B. Hugenholtz, D.A. Korteweg, with the collaboration of J. Poort, 'Digitalisering van audiovisueel materiaal door erfgoedinstellingen: Modellen voor licenties en vergoedingen', report commissioned by Images for the Future/Knowledgeland, Amsterdam, April 2011 – English summary.

C. Making ECL systems work across the EU

57 Considering the countless differences and nuances in the already existing ECL mechanisms it is not surprising that no mechanism has been developed to broaden ECL systems to other territories, which are not covered by the national law that prescribes the "extension effect".[61] On the other hand, the problem of the cross-border application of ECL regimes partly lies in the fact that ECLs commonly cover all works "used by" or "contained in the collection" of a CHI. All works "used" or "contained in the collection" encompass not only works of which the rights are owned by the nationals of that country, but also by foreigners. The "extension" of an agreement between a CMO and a CHI therefore also applies to works of foreign rights holders who may or may not be member of that CMO, or even member of a sister CMO with which a reciprocal agreement has been concluded. This relates to the issue of the representative character of the CMO. The uncertainty arising from the possibility that "foreign non-members" could be included constitutes a calculated risk for a representative CMO when applied on a national scale; however, this risk would become too great when applied on a cross-border basis. Moreover, the cross-border application of an ECL agreement is only feasible as long as the CMO has obtained a global transfer of rights allowing it to license on a worldwide scale from the rights owner, not if the CMO is only entrusted with the management of rights within its own national territory.

58 The broadening of the "extension" of a national ECL regime may actually not be necessary to achieve the purpose of allowing CHIs to digitise and make the works contained in their collections available to the public across Europe. An alternative to existing ECL systems that encompass works "used" or "contained in the collection" would be to narrow the scope of ECL agreements to the "works first published in the country" that are contained in the collection of the CHIs. As further developed below, this proposal rests on the recognition of the "country of origin" principle, as the necessary and sufficient territory for the rights clearance of works contained in the collection of a cultural heritage institution, including orphan and out-of-commerce works. This measure would need to be accompanied by transparency measures to ensure that potential users have the necessary information for legitimate and secure cross-border use of the copyright protected material. But first, a few preliminary remarks.

61 J.-P. Triaille, S. Dusollier, et al., 'Study on the application of Directive 2001/29/EC on copyright and related rights in the information society', De Wolf and partners, PN/2009-35/D, Brussels, December 2013, p. 306.

I. General remarks

59 Before turning to the core of our proposal, it is worth mentioning two other possible options to facilitate digitisation and making available of content for Europeana use: the first is a full harmonisation of exceptions in favour of CHIs, and the second is an improved system of multi-territorial licensing of rights.

1. Full harmonisation of exceptions

60 Directive 2001/29/EC on copyright in the information society establishes the main legal framework at the European level for the protection of works. This Directive only provides for narrow limitations for the benefit of cultural institutions. The two relevant provisions directed at the activities of these institutions are the following:

- a limitation on the reproduction right for specific acts of reproduction for non-commercial purposes (article 5(2)(c) of directive 2001/29/EC), and;
- a narrowly formulated limitation on the communication to the public right and the making available right for the purpose of research or private study by means of dedicated terminals located on the premises of such establishments (article 5(3)(n) of directive 2001/29/EC).

61 Not all Member States have implemented the optional limitation of article 5(2)c) of Directive 2001/29/EC, and those that did have often chosen different ways to do it, subjecting the act of reproduction to different conditions of application and requirements. Some Member States only allow reproductions to be made in analogue format; others restrict the digitisation to certain types of works, while other Member States allow all categories of works to be reproduced in both analogue and digital form.[62] In addition, Member States have identified different beneficiaries of this limitation. The prevailing legal uncertainty regarding the manner in which digitised material may be used and reproduced, has been known to constitute a disincentive to digitisation. This works especially against cross-border exchange of material and discourages cross-border cooperation.

62 In countries that chose to implement it, article 5(3)n) was transposed almost word-for-word in the national legislation. Several Member States have, however, decided not to incorporate this article into their law; the extent to which library patrons are allowed to consult digital material on the library network in these Member States is therefore unclear. Not only is the implementation of this provision, just like the previous one, not mandatory, but even where it has been implemented, its scope remains extremely narrow: a work may only be communicated or made available to individual members of the public, if each patron establishes that the use is for their exclusive research or private study. The works may only be communicated or made available by means of dedicated terminals on the premise of non-commercial establishments, which excludes any access via an extranet or other protected network connection that users can access at a distance. However, considering the default nature of this provision and the fact that its application is most often overridden by contract, libraries advocate for specific contracts or licences, which, without creating an imbalance, would take account of their specific role in the dissemination of knowledge.

63 In view of the uncertainty around the scope and workings of article 5(3)n) of Directive 2001/29/EC, the Court of Justice of the EU was asked to give its interpretation in a request for a preliminary ruling from the German Supreme Court.[63] In the *Technische Universität Darmstadt* case, the Court ruled that where an establishment, such as a publicly accessible library, gives access to a work contained in its collection to a "public", namely all of the individual members of the public using the dedicated terminals installed on its premises for the purpose of research or private study, that must be considered to be "making [that work] available" and, therefore, an "act of communication" for the purposes of Article 3(1) of that directive. Such a right of communication of works enjoyed by the establishments covered by Article 5(3)(n) of Directive 2001/29 would risk being rendered largely meaningless, or indeed ineffective, if those establishments did not have an ancillary right to digitise the works in question. Those establishments are recognised as having such a right pursuant to Article 5(2)(c) of Directive 2001/29, provided that "specific acts of reproduction" are involved. That condition of specificity must be understood as meaning that, as a general rule, the establishments in question may not digitise their entire collections.[64]

64 Even if the CJEU decision in the *Technische Universität Darmstadt* case confers a certain leeway on libraries to digitise some works in their collections, it does not permit the digitisation of entire collections. So the need for a solution for mass-digitisation and online

62 L. Guibault, 'Why Cherry-Picking Never Leads to Harmonisation: The Case of the Limitations on Copyright under Directive 2001/29/EC', JIPITEC 2010-2.

63 Case 117-13, Decision of the Court of Justice of the EU, 11 September 2014 (Technische Universität Darmstadt/Eugen Ulmer KG).

64 Id., para. 42-45.

making available of works held in the collections of CHIs is still present.[65] A well-crafted, mandatory exception or limitation to the benefit of CHIs would in fact offer the greatest level of certainty for all parties involved in the digitisation and online making available of cultural heritage on a European-wide level. It remains to be seen, whether the ongoing European copyright reform will achieve this.

2. Multi-territorial licensing

65 Although the recently adopted Directive 2014/26/EC on collective management of rights[66] aims at increasing the general effectiveness, transparency and accountability of CMOs, it is unlikely to increase the capacity of CMOs across Europe to cater in any useful and systematic way to the needs of cross-border application of ECL schemes. While Title III of Directive 2014/26/EC is meant to cure the uncertainty that prevailed until then concerning the rights clearance for legitimate online music services, the rules on multi-territorial licensing are limited to online uses of musical works and to authors' rights, excluding neighbouring rights.[67] Even if recital 7d) of the Directive emphasises that CMOs should not be precluded from concluding representation agreements with other CMOs in order to offer multi-territorial licences also in areas other than online musical services, the reality is that the level of collective organisation varies significantly per sector of the copyright industry and per country; thus it is hardly feasible to accept multi-territorial licensing based on a network of reciprocal agreements. Without the support of the Directive, the likelihood that other sectors of the copyright industry will organise themselves to a sufficient degree as to enable effective multi-territorial licensing or even the establishment of a network of reciprocal licenses is small.

II. Country of origin principle

66 There is a distinctive interest among legislators and stakeholders in Europe towards ECL systems as a solution for the clearance of rights of the digitisation and making available of works contained in the collections of CHIs. Considering the mosaic of ECL solutions already in place, a mechanism is needed to ensure that the schemes put forward at the national level can benefit citizens across the European Union. A potential solution to the problem of extra-territorial application of ECL agreements could be to formally declare the "country of origin of the work" as necessary and sufficient territory where permission should be sought prior to disseminating the works throughout the European Union. For, as Triaille et al. summarise in their study, "if a work is digitized by a library in a given country, it should be used by another library in the same country or in another Member State in order to achieve economies of scale to foster the development of digital libraries".[68] This conclusion echoes the European Commission's Recommendation of 2011 on the digitisation and online accessibility of cultural material and digital preservation, which stressed the importance of "pooling of digitisation efforts by cultural institutions and cross-border collaboration, building on competence centres for digitisation in Europe".

1. Existing legal framework

67 The principle of country of origin is the cornerstone of the international copyright framework under the Berne Convention. Article 5 of the Convention governs the rights guaranteed under the Convention to authors, being either nationals or foreigners of the country of origin of the work for which protection is sought. This provision of the Convention specifies which rules are applicable to the enjoyment and exercise of the rights guaranteed, depending on whether the author is a national of the country of origin of the work for which protection is sought or not. The definition of the "country of origin" is therefore paramount to the grant and exercise of the rights granted by the Convention. Paragraph 4 of the Convention defines the "country of origin" as follows:

> *(a) in the case of works first published in a country of the Union, that country; in the case of works published simultaneously in several countries of the Union which grant different terms of protection, the country whose legislation grants the shortest term of protection.*

65 See: European Commission, Report on the responses to the Public Consultation on the Review of the EU Copyright Rules, Directorate General Internal Market and Services Directorate D – Intellectual property D1 – Copyright July 2014.

66 Directive 2014/26/EU of the European Parliament and of the Council on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online uses in the internal market.

67 Explanatory Memorandum to Proposal for a Directive on collective management, 8.

68 J.-P. Triaille, S. Dusollier, et al., 'Study on the application of Directive 2001/29/EC on copyright and related rights in the information society', De Wolf and partners, PN/2009-35/D, Brussels, December 2013, p. 283; see also: European Commission, Study 'Assessing the economic impacts of adapting certain limitations and exceptions to copyright and related rights in the EU – Analysis of specific policy options', Brussels, 23.06.2014, p. 20.

(b) in the case of works published simultaneously in a country outside the Union and in a country of the Union, the latter country;

(c) in the case of unpublished works or of works first published in a country outside the Union, without simultaneous publication in a country of the Union, the country of the Union of which the author is a national, provided that:

(i) when these are cinematographic works the maker of which has his headquarters or his habitual residence in a country of the Union, the country of origin shall be that country, and

(ii) when these are works of architecture erected in a country of the Union or other artistic works incorporated in a building or other structure located in a country of the Union, the country of origin shall be that country.

68 The definition should be read in conjunction with article 3(3) of the Convention which defines the expression "published works" as meaning works published with the consent of their authors, whatever may be the means of manufacture of the copies, provided that the availability of such copies has been such as to satisfy the reasonable requirements of the public, having regard to the nature of the work. According to the same provision however, "the performance of a dramatic, dramatico-musical, cinematographic or musical work, the public recitation of a literary work, the communication by wire or the broadcasting of literary or artistic works, the exhibition of a work of art and the construction of a work of architecture shall not constitute publication". Acts of communication to the public in principle do not qualify as acts of publication under the Berne Convention, but as we shall see in the context of Directive 2012/28/EC on certain permitted uses of orphan works, the legislator can specify otherwise.

69 The determination of the principle of the "country of origin" as a unique point of attachment for the exercise of rights is not entirely without precedent in European copyright law. A similar principle, "country of emission", was already laid down in Directive 1993/83/EC based on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission.[69] According to the emission theory, the law of the country of emission of the satellite signal applies for the clearance of rights within the European Union. This theory was developed by analogy with the law applicable to terrestrial broadcasting, which allows broadcasting organisations to easily obtain licences for use of works from one country.[70]

70 In the specific context of the digitisation and making available of works held by CHIs, two other sets of rules are particularly relevant: the MoU on out-of-commerce works and Directive 2012/28/EC on certain permitted uses of orphan works. It is worth pointing out that, in its Recommendation of 2011, the Commission also had emphasised that the MoU should serve as a model for other sectors.[71] Admittedly the cross-border effect of voluntarily developed licensing solutions for the mass-digitisation of out-of-commerce works may necessitate legislative intervention. As would the application of a "country of origin" principle. According to the MoU, conditions of use of the works are negotiated within a predefined framework. The collecting societies will issue collective licences to libraries and other concerned institutions. These collective agreements are to be negotiated in the country of first publication of the work and provide for the type of permitted uses of works.

71 The MoU does not have a crossborder effect by default: Crossborder effect will be negotiated and agreed upon in the licence. Moreover, the MoU determines in Principle No. 3 sub 1, that if an agreement has been concluded, the CMO may limit the crossborder effects of such a licence to the works of the right holders that it represents. If this is done, the CHI could for example acquire a licence for the digitisation and online dissemination for the out of commerce works that have been published for the first time in the country of CMO for the rights holders that it represents, but territorially limited for the extended effect works of non represented rights holders.[72]

72 Directive 2012/28/EC also serves - in some important respects - as a source of inspiration for this proposal. Not only does the Directive provide footing for the development of a predefined framework within which the negotiations on the relevant conditions of use of works will take place, but it also establishes the criterion of "country of origin" as the starting point for the conduct of a diligent search. With regard to the country of first publication, Recital 12 declares that:

For reasons of international comity, this Directive should apply only to works and phonograms that are first published in the territory of a Member State or, in the absence of publication, first broadcast in the territory of a Member State or, in the absence of publication or broadcast, made publicly accessible by the beneficiaries of this Directive with

69 OJ L 248, 06.10.1993, p. 15–21.

70 P.B. Hugenholtz, 'SatCab revisited: The past, present and future of the Satellite and Cable Directive', IRIS Plus 2009-8, p. 7-19.

71 Commission Recommendation of 27 October 2011 on the digitisation and online accessibility of cultural material and digital preservation, OJ, L 283 of 29 October 2011, p. 39, Recital 12.

72 Oostveen & Guibault 2013, p. 6.

the consent of the rightholders.

73 Recital 15 further states that:

> *In order to avoid duplication of search efforts, a diligent search should be carried out in the Member State where the work or phonogram was first published or, in cases where no publication has taken place, where it was first broadcast.*

74 In other words, both the legislative and the consensual instruments dealing with the digitisation and making available of cultural heritage material point to the country of first publication as valid point of attachment.

2. Application of country of origin principle to ECLs

75 As a recent study conducted on behalf of the European Commission notes in relation to ECL schemes, "(...) it is difficult to imagine that a national CMO (all are) could be seen as being sufficiently representative to authorise the use of content (beyond its domestic repertoire) in territories outside its own country".[73] We believe that by electing the "country of origin" as the criterion of reference, the problem of representativeness of the CMO would most likely be solved. It is indeed reasonable to infer that the vast majority of authors and publishers of works in a country are also members of the CMO of that same country.[74] The few exceptions, particularly with regard to CMOs that represent the rights of authors belonging to a bigger linguistic community (such as Germany, in relation to Austria and Switzerland), should not detract from the generality of the rule.

76 The application of a "country of origin" principle would also coincide with current practice where the mass-digitisation efforts of the CHIs concern the works contained in their collections, the vast majority of which are works published or broadcast nationally. The Bokhylla project concerns Norwegian books; the French Act No 2012-287 on non-available works expressly applies to French books; the Danish public broadcasting archives contain national or regional Danish television productions. The assumption that underpins this proposal is that the digitisation and making available of works contained in the collection of CHIs concerns, for the greater part, works that are no longer in commercial circulation, e.g. out-of-commerce or even orphan. We believe that an ECL agreement negotiated in the country of first publication of an out-of-commerce book (such as the ECL-type scheme set up in Germany) would not affect the normal exploitation of the work, nor would it cause prejudice to the legitimate interests of the rights owner. Should the collections of a CHI contain commercially exploitable works, then the ECL agreement could exclude these from the scope of the licence for example by fixing a cut-off date (such as the German and French regimes, e.g. 1966 and 2001). Moreover, the rights owner would, at all times, retain his right to opt-out from the regime.

77 ECL schemes rest on a system of free negotiation between CMO and users. This principle is paramount and should not be interfered with. In other words, except for the possibility for non-members to opt-out of the regime, which should be laid down in the law, a definite degree of freedom of contract should be the rule. The recognition of the "country of origin" principle would leave existing ECL regimes unaffected, except for the recognition of their validity beyond the national boundaries. Nevertheless, for Member States that might consider introducing a new ECL provision in their legislation and have a fear of heights, Directive 2012/28/EC could provide some elements of inspiration for the design of a general ECL framework within which contracting parties would be allowed to negotiate. For instance, the definition of the user group could follow that of the Directive so as to apply to "publicly accessible libraries, educational establishments and museums, as well as archives, film or audio heritage institutions and public-service broadcasting organisations, established in the Member States". On the other hand, since ECL agreements are the fruit of free negotiations, there would in principle be no need to restrict the categories of subject matter, nor the acts permitted to take place.

78 The thorniest issue deriving from the establishment of the "country of origin" principle would be the determination of the appropriate level of remuneration to be paid by CHIs for the digitisation and European-wide dissemination of the works in their collection. Recital 18 of Directive 2012/28/EC explains that "For the purposes of determining the possible level of fair compensation, due account should be taken, inter alia, of Member States' cultural promotion objectives, of the non-commercial nature of the use made by the organisations in question in order to achieve aims related to their public-interest missions, such as promoting learning and disseminating culture, and of the possible harm to rightholders." As we have seen in section B above, contracting parties to an ECL agreement may envisage different remuneration structures, based either on actual use, or on expected user or social benefit. While the first method of calculation always bears the risk of amounting to a prohibitive price,

73 Study 'Assessing the economic impacts of adapting certain limitations and exceptions to copyright and related rights in the EU – Analysis of specific policy options', Brussels, 23.06.2014, p. 19.

74 See: Tryggvadottir 'Digital Libraries, the Nordic system of extended collective licensing and cross-border use', Auteurs & Media 2014/5, p. 323.

the second may be more palatable in this context. Small linguistic communities could take account of the relatively low level of international spill-over and fix the price accordingly. For larger linguistic communities, like English, French or German, contracting parties could envisage an earlier cut-off date so that only older works would be widely accessible, with a corresponding price tag. Technical solutions could also be put in place to limit the possibilities of use of end users located in other countries, for example by allowing streaming or viewing of works rather than downloading.[75]

79 The application of the "country of origin" principle to give cross-border effect to the extended collective licensing agreements concluded between European CHIs and their national CMO would require legislative intervention from the European legislator. At the national level, the ECL provision or agreement would need to clarify that it is restricted to works first published in that country. At the European level, the legislator would need to introduce a provision, by way of a directive, to specify that an ECL agreement concluded with respect to the works first published in one Member State is valid in all Member States. A European statutory provision could read as follows:

> *(1) For the purpose of the conclusion of agreements between a collective management organisation and a user, a Member State may introduce a mechanism by which the work of a rightholder who has not transferred the management of his rights to a collective management organisation, shall be presumed to be managed by the collective management organisation which manages rights of the same category of works in that Member State, unless he has expressly advised otherwise.*
>
> *(2) Where such a mechanism has been established in a Member State for the making available by publicly accessible cultural heritage institutions of works first published in that Member State, the works may be made available to the public in all Member States.*

80 Such a provision would ensure that the key elements of the ECL systems are respected (the negotiation of agreements, the restriction to the cultural heritage sector, the extension to non-members, the possibility to opt out), while recognising the cross-border application of the agreement.

3. Transparency measures

81 In view of the diversity of regimes put in place in the Member States for the making available of works by cultural heritage institutions, an effective cross-border application of ECL agreements would need to be accompanied by transparency measures, to ensure that potential users have the necessary information for legitimate and secure cross-border use of the copyright protected material.

82 The creation of yet another Europe-wide register, in addition to the orphan works register kept by the Office of Harmonisation in the Internal Market, would be quite cumbersome and probably not even necessary to convey the required information. Most importantly, the national libraries, archives or museum wishing to conclude an ECL agreement with a CMO for the making available of works first published in their country would need to make the terms of the agreement accessible to the public. The National Library of Norway and the Association of libraries (Bibliotheksverband)[76] in Germany already do so, as the text of their governing agreement can be easily located on their respective websites.

83 Potential users would need to be informed about the subject matter covered (does the agreement relate only to books or to other types of content?), the duration and scope of the licence (what acts are allowed under the agreement?), the definition of the user group (are only CHIs targeted by the agreement or are other types of users allowed to use the works?), the conditions of use (are commercial uses permitted or not?), and exercise of the opt-out option by certain rights holders. Only if the parties to an ECL agreement are transparent about the terms, can the application of the "country of origin" principle make sense in practice and be meaningful to users outside the national territory.

D. Conclusion

84 There is currently a certain momentum among legislators and stakeholders in Europe towards the establishment of ECL systems as a solution for the clearance of rights for the digitisation and making available of works contained in the collection of a cultural heritage institution. This system has definite advantages as it significantly lowers transaction costs compared to individual right clearance or to the diligent search requirement of Directive 2012/28/EC. It can also serve as a "one-stop-shop" for digitisation projects, as CHIs may clear the

75 Tryggvadottir 'Digital Libraries, the Nordic system of extended collective licensing and cross-border use', Auteurs & Media 2014/5, p. 325.

76 http://www.bibliotheksverband.de/fileadmin/user_upload/DBV/vereinbarungen/ 2015_01_RV_vergriffene_Werke.pdf.

rights over potentially large proportions of their collections at once. Additionally, thanks to a fixed fee structure, CHIs can more easily plan expenses and operate in a more predictable environment.[77]

85 In the 2014 Commission consultation on the reform of the European copyright regime,[78] two questions were posed to the public directly concerning the issue of mass-digitisation. Question 40 asked whether legislation would be necessary to ensure that ECLs concluded as a result of the MoU on out-of-commerce works have a cross-border effect so that out of commerce works can be accessed across the EU. Question 41 enquired whether mechanisms would be necessary beyond those already agreed for other types of content (e.g. for audio- or audio-visual collections, broadcasters' archives).[79] The answers submitted were quite diverse, reflecting the diverging interests of stakeholders involved. Interestingly, not only institutional users, but also some authors and authors' organisations invoked the need to give the MoU cross-border effect and to look for solutions for mass-digitisation for other types of works.

86 Considering the mosaic of ECL solutions already in place, we believe that the only workable solution to the problem of extra-territorial application of ECL schemes would be to formally establish a "country of origin" principle. The application of the "country of origin" principle to give cross-border effect to the extended collective licensing agreements concluded between European CHIs and their national CMO would require legislative intervention from the European legislator. In principle, there would be no need for national implementation of this rule. As a result of the introduction of a statutory provision, as soon as the rights on a work contained in the collection of a CHI would be cleared in the country of first publication, broadcast, or dissemination, they would be also cleared for the entire territory of the European Union.

87 One of the major advantages of this proposal is that it leaves Member States entirely free to decide whether or not to follow the ECL path on their own territory. The recognition of the "country of origin" principle would leave existing ECL regimes unaffected except for the recognition of their validity beyond the national boundaries. Should a Member State choose to maintain its current regime or introduce a new one, the result of the negotiations between the contracting parties to an ECL agreement would be recognised as a valid permission to digitise and make works available by a CHI throughout Europe. In practice, this would mean that there would no longer be a need to block access to visitors without a national IP address. Of course, should this become reality, the parties to an existing contract would need to revisit the conditions of use, most particularly the price paid for foreign access. Another advantage would be that this solution is presumably less far-reaching and politically sensitive, than adopting an exception on copyright to allow CHI to digitise and make the works in their collections available to the public.

88 Whether CHIs across Europe would be willing to disclose their treasures to a Europe-wide public would be a matter of setting the proper conditions of use, e.g. fixing a reasonable fee. CHIs might also be more inclined to share if there is certain degree of reciprocity among them in Europe, e.g. if more than one or two CHIs dip their toe in the system. If no one does, however, then an exception or limitation on copyright will turn out to be the only solution to allow CHIs to digitise and make available the works in their collections.

77 European Commission, Study 'Assessing the economic impacts of adapting certain limitations and exceptions to copyright and related rights in the EU – Analysis of specific policy options', Brussels, 23.06.2014, p. 19.

78 European Commission, DG Internal Market, Report on the responses to the public consultation on the Review of EU Copyright Rules, Brussels, July 2014.

79 Public Consultation on the review of the EU copyright rules, Brussels, November 2013, p. 22.

* Lucie Guibault (LL.M. Montreal, LL.D. Amsterdam) is an associate professor at the Institute for Information Law, University of Amsterdam. She is also one of the co-editors of this Journal. This research was funded by Europeana Awareness (European Commission funded eContent+ program, 2011-2014). An initial version of this paper was presented at the 3rd Europeana Licensing Workshop, held in Luxembourg on 20-21 November 2014 at the Forum da Vinci - Forum of Architecture, Engineering, Science and Technology. A later version was presented at the Conference 'Digital Frontiers – Access to Digital Archives and Libraries through Cross Border Collective Rights Management of Copyright', co-organised by the National Library of Sweden and the University of Stockholm, Stockholm, on 5-6 November 2015. The author wishes to thank all participants of both events for their invaluable contributions. Special thanks also to Felix Trumpke for asking the right questions at the right time about a previous draft.

Information as Property

by **Herbert Zech***

Abstract: Information is widely regarded as one of the key concepts of modern society. The production, distribution and use of information are some of the key aspects of modern economies. Driven by technological progress information has become a good in its own right. This established an information economy and challenged the law to provide an apt framework suitable to promote the production of information, enable its distribution and efficient allocation, and deal with the risks inherent in information technology. Property rights are a major component of such a framework. However, information as an object of property rights is not limited to intellectual property but may also occur as personality aspects or even tangible property. Accordingly, information as property can be found in the area of intellectual property, personality protection and other property rights. This essay attempts to categorize three different types of information that can be understood as a good in the economic sense and an object in the legal sense: semantic information, syntactic information and structural information. It shows how legal ownership of such information is established by different subjective rights. In addition the widespread debate regarding the justification of intellectual property rights is demonstrated from the wider perspective of informational property in general. Finally, in light of current debates, this essay explores whether "data producers" shall have a new kind of property right in data.

Keywords: information as a property good; property rights; economic good; ownership of infomation; data producers

Recommended citation: Herbert Zech, Information as Property, 6 (2015) JIPITEC 192, para 1.

A. Information as a Commodity: Semantic, Syntactic and Structural Information*

1 From a legal perspective the "nature" of information is far less important than the question of how information is treated as an object in everyday life and - closely associated with this - how information is treated as a commercial good or commodity. This is driven by and relevant to the development of information technology that not only enhanced our capabilities in handling information but also altered our view of information in everyday life. Therefore, before proposing the concept of semantic, syntactic and structural information, the influence of technological developments shall be briefly outlined.

I. How Technological Progress Influences our Perception of Information

2 The technological development of information processing has its roots in very early human history.[1] Beginning with the development of language and scripture, followed by ever advancing printing presses on to punched cards in weaving machines, photography, telegraphs, telephones, sound recording, radio, TV, photocopying, and finally information technology; multiplication, storage, transfer and automated processing of information has become increasingly easier, more powerful and widespread.

1. Easier Multiplication of Information and the Loosening of its Ties to Physical Carriers

3 Scripture provided the first means of storing information other than the human mind. As a consequence, storing information has become increasingly simplified, especially with the advent of printing presses that allowed the multiplication

1 One of the best accounts of technological and cultural developments influencing the handling of information is given by Levinson, The Soft Edge, A Natural History and Future of the Information Revolution, 1998.

of such information and eventually the development of modern information technology. The amount of information that can be stored on a physical carrier and distributed for a certain sum of money has been steadily increasing at an exponential rate. This has led to a loosening of the link between information and its physical carrier. Jon Bing wrote: "The computer has set information free. Traditionally, information has been chained in words to a page. Modern technology – especially computer based technology – has liberated the words from the medium. A text or a set of characters is more appropriately viewed as something separate, rather than a property of a page, a book, a stone slab or a film strip."[2]

4 The latest development in this respect is the advent of cloud computing. Cloud computing finally severed the link between information and one single discernible physical object as an information carrier. Although information has to be stored on a physical carrier somewhere, the practical determination of such a carrier to specific information is no longer possible.

2. Easier Multiplication and the Relation between Information and Creator

5 Not only has the link between information and a physical carrier been weakened, but also the link between information and a human creator is no longer necessary. Whereas traditional methods such as writing and drawing required a human mind to attach information to a physical carrier, this has changed with technological development. A landmark within this development was the introduction of photography and sound recording which triggered legal reactions (reactions of the lawmakers) in many countries. Subsequently, photocopying and modern data processing were introduced. Nowadays the automated registration of all kinds of phenomena and storage of the resulting data is commonplace. Ranging from scientific measurements to audio and video recording devices and special applications like Google street view, the production of information (especially data) without creativity is of increasing economic importance.

6 Finally, with the development of artificial agents, the question arises how information that was neither produced by human creativity nor by the recording of natural phenomena shall be treated. One example of this debate is the question of how "software written by software" shall be protected.[3]

3. The Unimportance of Meaning

7 A further effect of modern information technology is that information - particularly electronically stored information - is perceived as an object without any regard to its meaning. A text is still a text even if it is nonsensical, although arguably a mere mass of coincidental letters might not be regarded a text. A file is treated as a file whether it contains proper code that can be processed by computers or not and whether it contains any useful meaning that can be understood by a human being or not.

4. Information Technology and the Relation between Information and a Recipient

8 Traditionally, information is understood as something being exchanged between a sender and a recipient in the act of communication. However, with the establishment of information technology software as a new kind of data where information can be widely exchanged, the classical understanding of information has been altered. Software is a kind of information which is meant to be received only by machines (i.e. computers), not human recipients. Software is a special type of data with the function of steering machines. Data can be understood as information encoded in a way that can be processed by machines comprising software and application data alike. Neither data nor software as a special form of data need to carry any specific meaning (see above 3.) for a potential human recipient.

5. Abstraction of Information as a General Trend

9 As shown above, technological developments have led to everyday use of information as something separate from a physical carrier, a human creator, a specific meaning or a potential human recipient. This trend of seeing information as something "on its own" and therefore as an object may be called abstraction of information. However, this leaves open the theoretical and practical questions concerning how information can be defined as an object without all these references. This necessitates a closer look into semiotics.

2 Bing Journal of Media Law and Practice 1981, 219.

3 See De Wachter, CRi, 2010, 12; Paton/Morton, CRi, 2011, 8.

II. Three Levels of Talking about Information: Meaning, Signs and Medium

10 Semiotics demonstrates the exceptional importance of signs representing information.[4] Abstraction as defined above can be seen as a practical trend to accept information as an object defined only by signs. The semiotic distinction between the semantic level of information (meaning), the syntactic level of information (signs and their relation with each other) and communication channel (on the physical level) leads to the distinction between content layer, code layer and physical layer. When talking about information transfer in modern information technology as proposed by Benkler and Lessig[5] for instance, in the discussion about big data it is very important to distinguish between "raw" data and actual knowledge.[6]

11 Most importantly, from an IP lawyer's perspective (and a practical perspective in general), this distinction can be applied to the definition of information as an object too.

III. Treating Information as an Object: Semantic, Syntactic and Structural Information

12 The distinction between content layer, code layer and physical layer provides a powerful tool for defining information which can be treated as an object: it reveals that information can be defined on the semantic level (information with a certain meaning), on the syntactic level (information represented by a certain amount of signs), or even by its physical carrier (information contained in a certain physical carrier or in a wider sense information represented by the structure of a physical object).

1. Semantic, Syntactic and Structural Information

13 Each of the three types of information can be found in everyday life - when we talk about the news, a story or the "content" of a book we refer to the semantic level. Handling a text or a file refers to the syntactic level. Finally, dealing with a CD, a printed book etc. refers to the structural level. Of course the three levels are connected as meaning can be contained within a text and a text can be printed. Thus, the physical layer carries the syntactic layer and the syntactic layer the semantic layer. Nevertheless from an economic and legal perspective, each layer represents independent possibilities to define a certain amount of information.

14 In order to facilitate the description of information that is defined on the semantic, syntactic or structural level, I propose the terms semantic information, syntactic information and structural information. In economics, information is very often used in the sense of semantic information. To know something means having access to the semantic information. Accordingly, an invention (understood as applied knowledge) is also semantic information. Other examples are news, personal data, trade secrets, and genetic information. An important aspect of semantic information is that it can be correct or incorrect.

15 On a syntactic level, information is defined without meaning (i.e. abstract from any meaning) and therefore cannot be right or wrong but, when it comes to software, it can be functional or dysfunctional. Examples for syntactic information are texts, pictures (which represent whatever they depict and therefore they act as an amount of signs), sound recordings or any data (understood as information coded for machines instead of data about something which includes a semantic component). The act of translating meaning into a certain amount of signs can be called coding (code meaning the rule of translation). However, there is also a possibility of translating from the structural to the syntactic level (like in any kind of automatic measurement of recording), which can be understood as automated coding as well.

16 On the structural level, any kind of information carrier contains structural information. If a physical object carries syntactic information like a book, hard drive or a CD, its informational content is evident. However, even if a physical object does not contain any syntactic or semantic information, it nevertheless carries structural information that potentially can be detected.

2. Information Goods

17 Whenever information serves a certain use and can be transferred, it can also be addressed as a good. The definition of such goods is achieved in the same way information can be defined as an object in general. Therefore, information goods can also be divided in semantic, syntactic and structural information

4 Eco, A Theory of Semiotics, 1978.

5 Benkler, 52 Federal Communications Law Journal, 2000, 561, 562; Lessig, The Future of Ideas, The Fate of the Commons in a Connected World, 2002, 23.

6 Silver, The Signal and the Noise, 2012, 13.

goods. A news story can be sold as such, as a text containing the story or as a USB device storing the text containing the story. In the following section it will be demonstrated how this method of defining information objects and information goods can be used to analyse the construction of property rights.

B. Applying the Bundle of Rights Theory to Information

18 Since information is a much less clearly defined object than corporeal objects, property rights in information have to be carefully constructed as a bundle of rights. In addition, it should be considered that informational goods - at least semantic and syntactic information - are public goods in the sense that their use is non-exclusive and non-rival. Moreover, information as such is not depreciable, which is especially important for the justification of property rights to information.

19 Building on the standard categories of property rights: use (usus), enjoying the benefits of the use (usus fructus), changing form and substance (abusus) and transfer of the property three basic categories of rights to information can be distinguished: possessing information, using information and destroying information.[7]

I. Possessing Information: Access

20 The first category of information related activity that can be exclusively attributed to a right holder is information access. It equals the category of possession in tangible property.[8] Possessing an object enables the owner to perform any kind of activity related to this object, especially to use it. Unlike processing a corporeal object, having access to information is both non-rival and non-exclusive. Therefore property rights (as well as contracts) regarding access to information should be constructed differently.

II. Using Information

21 The second category is information use. Although access to information is a necessary requirement for using information, the two aspects can be attributed differently. An example for this would be the difference between patents and copyright: whereas patents limit the use of information without limiting access (and on the contrary aim at distributing technical information among the public), copyright limits the information by limiting access (namely prohibiting the copying and distributing of copyrighted works).

III. Destroying Information: Integrity

22 The third category is the destruction of information. This can be achieved by altering syntactic information on the code level or by falsifying semantic information. Moreover, syntactical information can be destroyed completely by deleting it, that is by destroying every existing carrier (structural information) containing the specific syntactic information. Knowledge, that is semantic information in the human mind, cannot be destroyed – or at least it cannot be destroyed without violating the integrity of the persons who have access to it.

C. Legal Ownership of Information

23 As shown above, legal ownership of information ought to be constructed according to the bundle of rights theory, as the exclusive attribution of certain aspects or activities dealing with specific information (defined as an object, i.e. as semantic, syntactic or structural information).

I. Semantic Information: Patents and Personality Protection

24 Semantic information can be defined as actual or potential knowledge regarding an individual or other objects. Information concerning other persons is the object of personality rights. Whereas personality protection has its roots in the protection of a legal subject which cannot be commoditized, information about a person can be separated from the person and therefore be treated as an object. This also led to the distinction between personality protection on the one hand and the right to publicity on the other hand, which can also be assigned to other right holders. Informational aspects of personality can be data, pictures, voice recordings or genetic information. Such information can either be defined on a semantic level (a certain fact about a certain person) or on a syntactic level (photographic pictures, voice recordings, gene sequences). Both are attributed to the original right owner on

7 The transfer of a property right is not regarded as a specific category of property like possessing, using or destroying. It belongs to a different level since it is not part of the activities exclusively assigned to the right owner but rather captures the question of the assignability of such a right on a higher level (or meta-level).

8 Cf. Rifkin, The Age of Access, 2000.

the semantic level, meaning they belong to the individual concerned.

25 A different mechanism of attribution can be found for semantic information regarding technical functioning (such information is protected in the form of inventions which are attributed to the inventor). Arguably one of the fundamental principles of classical intellectual property is that IP rights are conferred to the individual who creates information.

26 Trade secrets are another example of semantic information as an object of legal protection. Trade secrets are basically defined by their semantic connection with a company that can be embodied as a file (syntactic information) or a sheet of paper (structural information). However, the legal protection mechanism is different. Exclusivity is not established by attributing exclusive rights but pre-exists as a factual consequence of the secrecy. Trade secret protection acts as a legal intensifier of such factual exclusivity. The protection conferred is also incomplete as such secrets are not protected against independent recreation (especially in the case of technological knowledge) or in case they get disclosed.

II. Syntactic Information: Copyright and Design

27 The best example for syntactic information as an object of property rights are copyrighted works. According to the definition given in art. 9 (2) TRIPS, only expressions are protected, not ideas. These expressions are syntactic information as opposed to the free content (ideas) which qualifies as semantic information. Like patents the exclusive right is conferred upon the creator. Among the rights conferred is not only the use (excluding the mere perception of a copyrighted work) but also the granting of access to others.

28 Similarly design protection confers exclusive competences with regard to syntactic information, i.e. the design, to its creator. However, the information is not protected per se, but only when used as a design, i.e. by making articles to the design or creating a design document in order to make such articles not by distributing a design document (cf. art. 228 (6) UK-CDPA).

III. Structural Level: Tangible Property

29 Somewhat surprising also property rights in corporeal things (real property rights) confer legal exclusivity with respect to the information contained within. The possession of a data carrier ensures access to the information. Property protection for the carrier - especially the possession of the carrier - indirectly protects access to the information. Moreover the exclusive right to alter and destroy a data carrier indirectly entitles the right holder to prevent the alteration or destruction of the contained information. This mechanism is still of great importance for the protection of data although it encounters limitations when property rights and data usage divert (like working on somebody else's computer) or a specific data carrier is difficult to discern (for instance in cloud computing).

30 The practical relevance of corporeal property tends to use it as a mechanism for the attribution of incorporeal aspects. Even real estate has been used as an informational property right.[9] The question could be posed regarding whether the picture of a building belongs to the land owner, especially when the building can only be perceived from within the premises. However this has to be strongly refuted since corporeal property is tailor-made for rival and exclusive uses due to the corporality of its object. The picture of a building is classical intellectual property and may be subject to the architect's copyright. If it contains (semantic) information about the owner, its distribution may conflict with personality protection. Nevertheless, it should be strictly detached from the question regarding who the owner of the building is.

D. Justifying Legal Ownership and Creation of New Property rights

I. Justification

31 The discussion regarding the justification of IP covers a large part of information as property. The classification of information goods adds only a small argument: semantic information as a property causes greater losses to the public domain than syntactic information. Having an exclusive right to use semantic information (e.g. certain knowledge) gives a greater range of exclusive competences than having an exclusive right to use syntactic information (e.g. a certain text). A text is only one possibility to embody certain knowledge, while many others are left free. Therefore, creating property rights within semantic information requires a stronger justification than creating property rights within syntactic information. For instance, copyright becomes more

9 See the German Federal Court of Justice: BGH V ZR 44/10, V ZR 45/10, V ZR 46/10 (17 Dec 2010) Preußische Schlösser und Gärten; V ZR 14/12 (1 Mar 2013).

problematic if copyrighted works and the scope of protection shifts from mere expression (syntactic information) to content (semantic information, like the case of a novel which under the German "fabric doctrine" is protected if many details are imitated[10]).

32 Accordingly, real property rights, which assign structural information are even less detrimental to the public domain than property rights assigning syntactic information. This may be one of the reasons why the justification of real property rights is much less disputed than the justification of IP. Moreover justifying real property can be based on different arguments such as the "tragedy of the commons"[11] instead of the incentive paradigm or the creation of markets in public goods. Unlike semantic and syntactic information, structural information is identical with the physical object and therefore not a public good. Assigning structural information thus only means assigning competences that are already exclusive and rival. Factually exclusive competences are legally allocated; no new exclusivities are legally created.

II. Data Collection or Generation as a Reason for Property Protection?

33 The concept of information also allows a more precise description of the creation of information and informational goods either by a creative mind or by automated processes. Classical IP protects information created by human minds like inventions, works of art or designs. However, with the advent of big data applications, the question whether mere investments in information (like the creation of a database, Directive No. 96/9/EC) or the generation of information by automated sensors (like in smart cars or complex production machines) shall lead to exclusive rights.

34 The issue of a "data property" is currently hotly debated.[12] In fact, some good reasons exist for creating a new exclusive right to use data (defined as syntactic information generated by machines with automated sensors) for big data analyses pertaining to the person economically maintaining the machine. The reason is found not so much in an incentive to generate data or in the creation of a market for data (like in classical IP) but in ensuring a fair allocation of the profits generated by analysing the data. Instead of relying on existing factual ownership and secrecy, a clear property rule can provide the framework for a functioning data economy (as also envisaged by the EU commission[13]).

E. Trading Information Goods

35 The concept of information goods also highlights the function of exclusive rights in trading these goods. Instead of trading the carrier (like a CD) the legal framework as well as the individual contract should focus on the information good itself (like software). Therefore the CJEU's jurisprudence regarding software resales (UsedSoft[14]) is problematic. The doctrine of exhaustion serves to streamline IP rights to the free trade of corporeal goods. If no corporeal goods are involved anymore, the doctrine should be abandoned. Instead, IP law provides the means for trading exclusive competences by trading the rights or granting licenses. Therefore, if it is economically desirable to enable the resale of software, e-books or audio-books this should be achieved by adapting the legal rules on licensing and contract law. For instance, it could be argued that it is one of the main obligations of a purchase contract to deliver a resalable good. At least under German doctrine, this can be understood as one of the typical features of a purchase contract which cannot be waived using general clauses.

F. Conclusion

36 The three tier model of communication as proposed by Benkler may well be used to analyse information as an object of property rights. This analytical tool allows a clear distinction between property rights in semantic information, syntactic information and structural information (real property rights). The distinction has consequences for the construction and justification of property rights as well as the contractual exchange of information.

* Prof. Dr. iur., Dipl.-Biol., Professor of Life Sciences Law and Intellectual Property Law, Faculty of Law, University of Basel. This article summarizes the key arguments of a previously published book written in German language: Information als Schutzgegenstand, 2012.

10 Cf. Oechsler, GRUR, 2009, 1101, 1103 seqq.

11 Hardin, 162 SCIENCE, 1968, 1243, 1244.

12 Hoeren, MMR, 2013, 486; Dorner, CR, 2014, 617; Zech, CR, 2015, 137.

13 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, 6 May 2015, COM(2015) 192 final.

14 CJEU C-128/11 (3 Jul 2012) - UsedSoft v. Oracle. Cf. Zech 5 ZGE / IPJ, 2013, 368.

Scoping Electronic Communication Privacy Rules: Data, Services and Values

by **Joris van Hoboken and Frederik Zuiderveen Borgesius***

Abstract: We use electronic communication networks for more than simply traditional telecommunications: we access the news, buy goods online, file our taxes, contribute to public debate, and more. As a result, a wider array of privacy interests is implicated for users of electronic communications networks and services. This development calls into question the scope of electronic communications privacy rules. This paper analyses the scope of these rules, taking into account the rationale and the historic background of the European electronic communications privacy framework. We develop a framework for analysing the scope of electronic communications privacy rules using three approaches: (i) a service-centric approach, (ii) a data-centric approach, and (iii) a value-centric approach. We discuss the strengths and weaknesses of each approach. The current e-Privacy Directive contains a complex blend of the three approaches, which does not seem to be based on a thorough analysis of their strengths and weaknesses. The upcoming review of the directive announced by the European Commission provides an opportunity to improve the scoping of the rules.

Keywords: electronic communication; privacy rules; e-Privacy Directive; services; data; values

Recommended citation: Joris van Hoboken and Frederik Zuiderveen Borgesius, Scoping Electronic Communication Privacy Rules: Data, Services and Values, 6 (2015) JIPITEC 198, para 1.

A. Introduction

1 Sector-specific frameworks for electronic communications privacy, such as the European Union e-Privacy Directive,[1] have their historical roots in the sector-specific rules for public telecommunications networks, used for one-to-one voice communications. Nowadays, we use electronic communications networks for a wide variety of purposes beyond traditional telecommunications, including commerce, work, social interaction, media access, and interaction with government. The privacy interests of users engaged in these different activities go far beyond the interests protected in the current e-Privacy Directive. Therefore, the scope of the electronic communications privacy rules should be reassessed.

2 Currently, the e-Privacy Directive leaves considerable gaps in user protection; for instance because the rules for location and traffic data do not apply to new players in the electronic communications sector. The EU lawmaker has not systematically addressed user privacy interests related to access to online content, interactive media, and the wide variety of opportunities offered by networked communications. In 2015, the European Commission announced a review of the e-Privacy Directive.[2] In such a review, the question regarding the scope of the rules will be important.

1 Council Directive 2002/58/EC of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Council Directive 2006/24/EC and Council Directive 2009/136/EC (e-Privacy Directive).

2 See European Commission, Communication of 6 May 2015 on A Digital Single Market for Europe, COM (2015) 192 final, p. 13.

3 In this paper, we discuss three different approaches to scoping electronic communications privacy rules. Distinguishing these three approaches can aid in reaching informed decisions regarding scoping the rules. The three approaches are: (i) a service-centric approach, (ii) a data-centric approach, and (iii) a value-centric approach. (i) In a service-centric approach, the scope of the rules is delineated on the basis of different services. (ii) A data-centric approach protects privacy interests of users through the proxy of setting rules for processing types of personal data. (iii) A value-centric approach determines the scope of the rules based on the user's privacy interests at stake when using electronic communications networks.

4 We do not argue that one of the approaches is better than another – each approach has strengths and weaknesses. We provide the distinction between the three approaches as an analytical tool to assist in structuring discussions about scoping electronic privacy rules.

5 The article is structured as follows. In section two, we discuss the background and the scope of the main provisions of the e-Privacy Directive. The service-centric, data-centric, and value-centric approachs are outlined in sections three, four, and five respectively. The final section concludes that the European lawmaker should be aware of the strengths and weaknesses of the different approaches involved in scoping electronic communications privacy rules.

B. The e-Privacy Directive: background and current scope

6 In 1990, the European Commission presented a proposal for a Data Protection Directive with the aim to harmonise data privacy regimes to foster the European single market. After long and heated debates, the Data Protection Directive was finally adopted in 1995.[3] Additionally in 1990, the European Commission presented a proposal for a telecommunications privacy directive. The European Commission was planning to adopt the telecommunications privacy directive at the same time as the Data Protection Directive,[4] but it took until 1997.[5]

7 The general Data Protection Directive and the e-Privacy Directive are internal market harmonisation instruments.[6] The Data Protection Directive's dual aim is to provide a high level of data protection across the member states, and to ensure that personal data can flow across borders within Europe, uninhibited by differences in data privacy laws.[7] The e-Privacy Directive has a similar dual aim, for the electronic communications sector.[8]

8 In 2002, the 1997 telecommunications privacy directive was replaced by the e-Privacy Directive, officially the "Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector." This e-Privacy Directive was intended to be more in line with new technologies.[9] In 2009, the e-Privacy Directive was updated by the Citizens' Rights Directive.[10] Some of the key changes were the introduction of a consent requirement for tracking cookies and similar files, and an obligation to report data breaches.[11]

9 A few years earlier, in 2006, the European lawmaker had adopted the Data Retention Directive as an amendment to the e-Privacy Directive.[12] The Data Retention Directive obliged member states to require retention of electronic communications data by

3 Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).

4 See S. Simitis, 'From the market to the polis: The EU Directive on the protection of personal data', Iowa Law Review 1994, vol. 80, pp. 445-470.

5 Council Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (ISDN Directive).

6 The Data protection Directive is based on the (old) Article 100a of the Treaty establishing the European Community; the e-Privacy Directive is based on the (old) Article 95 of the Treaty establishing the European Community. See the current Article 114 of the Treaty on the Functioning of the European Union. See also: A. Arnbak, 'Securing Private Communications' (PhD thesis University of Amsterdam, academic version), http://hdl.handle.net/11245/1.492674 (accessed 15 November 2015), pp. 28-79.

7 Article 1 of the Data Protection Directive.

8 Article 1 of the e-Privacy Directive.

9 See recital 4 of the e-Privacy Directive.

10 Council Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Citizen's Rights Directive).

11 See P. De Hert & V. Papakonstantinou, 'The Amended EU Law on ePrivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights', John Marshall Journal of Information Technology & Privacy Law 2011, 29; B. Van der Sloot & F.J. Zuiderveen Borgesius, 'De amendementen van de Richtlijn Burgerrechten op de e-Priv'acyrichtlijn' [The Amendments of the Citizens' Rights Directive on the e-Privacy Directive], Privacy & Informatie 2010, Vol. 13, No. 4, pp. 162-172.

12 Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive).

related service providers for a period of 6-24 months, to enable government agencies to access these data. In 2014, the Court of Justice of the European Union declared this directive invalid.[13]

10 The e-Privacy Directive is a sector-specific regulatory instrument, adopted as part of the EU regulatory package for the telecommunications sector.[14] The directive's full title illustrates the goal of sector-specificity; the directive concerns "the processing of personal data and the protection of privacy in the electronic communications sector" [emphasis added].

11 Most of the provisions in the e-Privacy Directive contain rules applicable to "providers of publicly available electronic communications services", and "providers of public communications networks".[15] The scope of these e-Privacy Directive provisions is thus narrower than the scope of the general Data Protection Directive. The latter applies, in short, as soon as "personal data" are processed, regardless of the sector (with exceptions).[16]

12 For its material scope, the e-Privacy Directive partly relies on the definitions in the Framework Directive for electronic communications networks and services.[17] The resulting scope is not always clear, and is suboptimal from the perspective of protecting users' electronic communications privacy. As discussed below, there are many over-the-top services that are, from a user perspective, functionally equivalent to "publicly available electronic communications services" – but those over-the-top services do not fall within that definition.

13 An electronic communications network is defined in the Framework Directive as: "transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed."[18]

14 The Framework Directive defines an "electronic communications service" as "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services (...) which do not consist wholly or mainly in the conveyance of signals on electronic communications networks."[19]

15 An electronic communications service is, in short, a service that consists wholly or primarily in the conveyance of signals on electronic communications networks. This implies for instance, that the e-Privacy Directive is not applicable to voice over IP (VoIP) software services such as Skype, even though for users such services may be functionally equivalent to regulated services such as telephony. For personal data processing by services outside of the scope of the e-Privacy Directive, the general rules in the Data Protection Directive still apply.[20] From a user's privacy perspective, this difference in legal treatment does not make sense. In practice, individuals may not even be aware whether they are making a call through an electronic communications service or through a VoIP service.

16 Furthermore, as established in article 3, generally the e-Privacy Directive only applies to publicly available services and networks. This restriction has led to much debate. The Article 29 Working Party, in which European Data Protection Authorities cooperate, noted in 2008 that the distinction between private and public networks and services is difficult to draw: "Services are increasingly becoming a mixture of private and public elements and it is often difficult for regulators and for stakeholders alike to determine whether the e-Privacy Directive applies in a given situation. For example, is the provision of internet access to 30.000 students a public electronic communication system or a private one? What if the same access is provided by a multinational company, to tens of thousands of employees? What if it is provided by a cybercafé?"[21]

13 Court of Justice of the EU 8 April 2014, C-293/12 (Digital Rights Ireland).

14 See recital 4 of the e-Privacy Directive.

15 See infra Section 3 for more discussion.

16 See article 1(1) of the Data Protection Directive. Some parts of the public sector are outside the scope of the Directive (see article 3(2) and article 13). Some data processing practices in the private sector are also exempted, for purely personal purposes (article 3(2). There are also exemptions for the processing for journalistic purposes (article 9).

17 Council Directive 2002/21 of 7 March 2002 on a common regulatory framework for electronic communications networks and services as amended by Directive 2009/140/EC and Regulation 544/2009 (Framework Directive).

18 Article 2(a) of the Framework Directive.

19 Article 2(c) of the Framework Directive.

20 Recital 10 of the e-Privacy Directive.

21 Article 29 Working Party, 'Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic com-

17 Article 4 deals with the security of processing, and contains notification obligations regarding data breaches.[22] The security requirements and the data breach notification obligation in article 4 only apply to providers of publicly available electronic communications services.[23]

18 The e-Privacy Directive's specific regime for traffic and location data in article 5, 6 and 9 is roughly as follows. Unless a specified exception applies, consent of the user or subscriber is required for the processing of traffic and location data by regulated services. Traffic data, sometimes called metadata, are "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof".24 Examples of traffic data are the time of a communication, and the addressing information of those involved in a communication, such as the email address or IP address used to access the internet.25 With modern communication technology, the line between traffic data and communications content has become increasingly blurred. For instance, the subject line of an email message could be seen as traffic data or as communications content. Monitoring communications traffic data over time can provide a detailed picture of individuals' lives.26

19 Location data are data "indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service".[27] Location data can be sensitive.[28] For example, a phone's location data can disclose visits to a hospital, church, or mosque, or the location of one's bed.

20 Reflecting the telecommunications service background of the e-Privacy Directive, article 7 assumes that "subscribers" receive itemised bills, and grants them the right to receive non-itemised bills.[29] A subscriber is defined as "any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services".[30]

21 Article 8 concerns privacy interests related to calling line identification on a per-call basis. Under article 11, subscribers must be able, by request to the provider of the publicly available electronic communications service, to stop forwarded calls being passed on to them. The scope of article 8 and 11 is limited to providers of publicly available electronic communications services and networks. Article 8 and 11 apply to "calls". A call refers, in brief, to voice telephony.[31]

22 Article 5(1) emphasises member states' positive obligations regarding communications confidentiality.[32] Article 5(1) can be summarised as follows: member states must ensure the confidentiality of communications and the related traffic data by means of publicly available electronic communications services. In particular, member states must prohibit tapping, storage or other kinds of surveillance of communications, without the consent of the users or other legal authorisation.

23 The scope of these positive obligations for member states is subject to debate. If an internet access provider employs deep packet inspection

munications (e-Privacy Directive)' (WP150), Brussels, 15 May 2008, p. 4. See also: European Commission, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', Final Report (a study prepared for the European Commission DG Communications Networks, Content & Technology by Time.Lex and Spark legal network and consultancy ltd, 10 June 2015) http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9962 (accessed 15 November 2015), p. 24-32.

22 Article 4(3)-4(5) of the e-Privacy Directive. See also Recital 61 of the Citizens' Rights Directive.

23 Article 4(1) of the e-Privacy Directive.

24 Article 2(b) of the e-Privacy Directive.

25 Recital 15 of the e-Privacy Directive.

26 See e.g. B.J Koops & J.M. Smits, 'Verkeersgegevens en artikel 13 Grondwet. Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie' [Traffic data and article 13 of the Constitution. Technical and legal analysis of the distinction between traffic data and communications content], Wolf Legal Publishers 2014; P. Breyer, 'Telecommunications data retention and human rights: the compatibility of blanket traffic data retention with the ECHR', European Law Journal 2014, Vol. 11, No. 3, pp. 365-375; E. Felten, 'Written Testimony, Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act', www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf (accessed 15 November 2015); J. Mayer, & P. Mutchler, 'MetaPhone: The Sensitivity of Telephone Metadata' 2014, webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/ (accessed 15 November 2015); H. de Zwart, 'How your innocent smartphone passes on almost your entire life to the secret service' 2014, www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/ (accessed 15 November 2015); J.C. Fischer, Communications Network Traffic Data - Technical and Legal Aspects (PhD thesis University of Eindhoven), Academic version 2010 http://alexandria.tue.nl/extra2/689860.pdf accessed 15 November 2015.

27 Article 9 of the e-Privacy Directive.

28 Article 29 Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile devices' (WP 185) 16 May 2011, p. 7.

29 Article 7(1) of the e-Privacy Directive

30 Article 2(k) of the Framework Directive.

31 See article 2(s) of the Framework Directive.

32 See W. Steenbruggen, 'Publieke dimensies van privé-communicatie: een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk' [Public dimensions of private communication: an investigation into the responsibility of the government in the protection of confidential communications in the digital age], PhD thesis University of Amsterdam, Cramwinkel 2009, p. 176, p. 356.

to analyse people's internet use, including email communication, article 5(1) applies, since internet access providers are publicly available electronic communications services.

24 However, the broad formulation of article 5(1) could imply that member states' positive obligations extend to services involved in electronic communications that are not publicly available electronic communications services in the strict sense of the e-Privacy Directive. Thus, member states would have to ensure that nobody interferes with the confidentiality of communications and related traffic data flowing over public communications networks.[33] A similar general positive obligation could be based on the fundamental right to private life and private correspondence in Article 8 of the European Convention on Human Rights and Article 7 of the EU Charter of Fundamental Rights.

25 Web browsing and using online video services also fall within the legal definition of communication in the e-Privacy Directive.[34] Monitoring people's web browsing is thus only allowed after their consent, as member states must prohibit "interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned".[35] The European Data Protection Supervisor says that article 5(1) does not only apply to electronic communication service providers and networks, but has a broader scope.[36]

26 The rules for spam and cookies have a different scope than the majority of the other rules in the e-Privacy Directive. In short, article 11 only allows sending marketing emails after the receiver's prior consent is obtained (subject to exceptions for mail to existing customers).

27 Article 5(3) applies to anyone that stores or accesses information, such as a cookie, on a user's device, including if no personal data are involved. Article 5(3) is hotly debated, because it applies to tracking of internet users through cookies for online marketing.[37] The preamble shows that article 5(3) aims to protect the user's device and its contents against unauthorised access: "Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms."[38] The provision applies, for instance, to apps that access information on a user's smartphone, such as location data or a user's contact list.[39] Article 5(3) also protects the user against parties that want to store spyware on a user's device, without the user's knowledge. While article 5(3) does address privacy interests related to the use of electronic communication networks, its scope is atypical. The parties placing cookies or other information on user devices are not the parties that are generally regulated by the e-Privacy Directive.

28 In sum, the majority of the e-Privacy Directive's provisions only apply to publicly available communications networks or services. In the next section, we discuss the strengths and weaknesses of this service-centric approach to scoping electronic communications privacy rules.

C. A service-centric approach

29 In a service-centric approach to develop the scope of electronic communications privacy rules, the scope of the rules is delineated on the basis of different services. In brief, such rules only apply to certain types of companies operating in relevant electronic communications markets.

33 See European Commission, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', Final Report (a study prepared for the European Commission DG Communications Networks, Content & Technology by Time.Lex and Spark legal network and consultancy ltd, 10 June 2015) http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9962 (accessed 15 November 2015), p. 39-50.

34 Article 2(d); recital 16 of the e-Privacy Directive. See W. Steenbruggen, Publieke dimensies van privé-communicatie: een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk [Public dimensions of private communication: an investigation into the responsibility of the government in the protection of confidential communications in the digital age], PhD thesis University of Amsterdam, Cramwinkel 2009, p.181, 354; P. Traung, 'EU Law on Spyware, Web Bugs, Cookies, etc. Revisited: Article 5 of the Directive on Privacy and Electronic Communications', Business Law Review, 2010 Vol. 31, p. 227.

35 Article 5(1) of the e-Privacy Directive.

36 European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Proposal for a Directive on privacy and electronic communications', Brussels, (2008/C 181/01), 10 April 2008, par 33. See also P. Traung, 'EU Law on Spyware, Web Bugs, Cookies, etc. Revisited: Article 5 of the Directive on Privacy and Electronic Communications', Business Law Review, 2010 Vol. 31, p. 227; G. González Fuster, S. Gutwirth & P. De Hert, 'From Unsolicited Communications to Unsolicited Adjustments', in S. Gutwirth, Y. Poullet & P. De Hert (eds), Data Protection in a Profiled World, Springer 2010, pp. 105-117, p. 115.

37 Recital 24 and 25 of the e-Privacy Directive. See also S. Kierkegaard, 'How the cookies (almost) crumbled: privacy & lobbyism', Computer Law & Security Review 2005, Vol. 21, No. 4, pp. 310-322; E. Kosta, 'Peeking into the cookie jar: the European approach towards the regulation of cookies', International Journal of Law and Information Technology, 2013 Vol. 1, No. 1, pp. 1-27.

38 Recital 24 of the e-Privacy Directive.

39 Article 29 Working Party, 'Opinion 02/2013 on apps on smart devices' (WP 202) 27 February 2013, p. 10.

30 As suggested earlier, the e-Privacy Directive largely uses a service-centric approach. The main reason for this specific scoping is the directive's background as part of the regulatory framework for electronic communications markets.[40] A central feature of this regulatory framework is the recognition of the specific market characteristics of electronic communications networks and services, and their value for users and society. The framework recognises the particular market entry dynamics and network effects in the telecommunications industry. The framework aims to foster competition between relevant services, while providing for interconnection and interoperability of networks and services.[41]

31 Electronic communications networks and services constitute the electronic communications infrastructure, whereas over-the-top services merely use such infrastructure. Regulating the privacy conditions of infrastructure services also affects the privacy conditions of services that become available for use over such infrastructure, including over-the-top services, such as communications software. Hence, the focus on electronic communications services and networks involved in transmission activities can be defended on the basis of the infrastructural nature of these services for electronic communications. These services can have a more significant impact on communications privacy than other services that do not qualify as infrastructure.

32 A particular strength of a service-centric approach is that – if done right – it can be reasonably clear for a company whether it has to comply with a rule. The company must simply assess whether it is a "provider of a publicly available electronic communications service", or a "provider of a public communications network." Hence, in principle a service-centric approach can lead to rules with a relatively clear scope.

33 The key weakness of a service-centric approach is that such an approach can lead to – from a user perspective – arbitrary differences between protections for different but functionally equivalent services. For example, the e-Privacy Directive's rules for traffic and location data only apply to "providers of publicly available electronic communications services", and to "providers of public communications networks." However many companies, such as advertising networks (a type of online marketing company) and providers of smart phone apps, process data of a more sensitive nature than telecommunications providers. However, ad networks and apps providers are not subject to the e-Privacy Directive's rules for traffic and location data. Such companies are subject to the Data Protection Directive as far as they process personal data.

34 General data protection law is less stringent and less specific than the e-Privacy Directive's regime for traffic and location data. For instance, under the general Data Protection Directive, a data controller can rely on several legal bases for processing personal data – not only on the data subject's consent. An advertising network could, for instance, try to argue that for processing location data it has a legitimate interest that overrides the data subject's fundamental rights, and that therefore, it may process the data without the data subject's consent.[42] From a user's perspective, it is not logical that the rules are less strict when location data are in the hands of an advertising network, than when they are in the hands of an internet access provider.[43]

35 For other provisions in the e-Privacy Directive, such as the data breach notification requirement, the restriction to providers of publicly available electronic communications services appears also without merit. The e-Privacy Directive requires an internet access provider (a provider of a publicly available electronic communications service) to notify the authorities when an employee loses a laptop with customer data. But the e-Privacy Directive does not require a webmail provider, an online bank, or an online pharmacy to notify users and authorities of data breaches.[44]

36 Before the 2009 amendments to the e-Privacy Directive were adopted, there was ample discussion regarding the scope of the data breach notification requirements. The Article 29 Working Party, the European Data Protection Supervisor, and the European Parliament were in favour of extending the scope of the notification requirements to, at least, all providers of information society services.[45]

40 See C. Schnabel, 'Privacy and Data Protection in Electronic Communications Law', in C. Koenig, et al. (eds), EC Competition and Telecommunications Law, Kluwer Law International 2009, pp. 509-568, p. 520-522.

41 See e.g. P. Alexiadis & M. Cave, 'Regulation and Competition Law in Telecommunications and Other Network Industries', in: R. Baldwin, M. Cave & M. Lodge (eds.), The Oxford handbook of Regulation, Oxford University Press 2010.

42 See article 7(f) of the Data Protection Directive. See F.J. Zuiderveen Borgesius, 'Personal data processing for behavioural targeting: which legal basis?', International Data Privacy Law, doi: 10.1093/idpl/ipv011, 2015.

43 See also F.J. Zuiderveen Borgesius, 'Improving Privacy Protection in the area of Behavioural Targeting', Kluwer Law International 2015, pp. 282-283.

44 See F.J. Zuiderveen Borgesius, 'De Meldplicht Voor Datalekken in De Telecommunicatiewet' [The data breach notification requirement in the Dutch Telecommunications Act], Computerrecht 2011, No. 4, pp. 209-218; A. Arnbak, 'Securing Private Communications' (PhD thesis University of Amsterdam, academic version), http://hdl.handle.net/11245/1.492674 (accessed 15 November 2015), p. 48-49.

45 Article 29 Working Party, 'Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic

The European Commission did not follow that suggestion. However, in the 2012 proposal for a Data Protection Regulation, the Commission did introduce a data breach notification requirement.[46] If that proposal were adopted, it would be difficult to see why sector-specific data breach rules in the e-Privacy Directive would still be needed.

37 Indeed, recently the European Commission suggested that the narrow scope of the e-Privacy Directive should be reassessed:

> *Special rules apply to electronic communications services (e-Privacy Directive) which may need to be reassessed once the general EU rules on data protection are agreed, particularly since most of the articles of the current e-Privacy Directive apply only to providers of electronic communications services, i.e. traditional telecoms companies. Information society service providers using the Internet to provide communication services are thus generally excluded from its scope.*[47]

38 In sum, the main strength of the service-centric approach to scoping electronic communications privacy rules is the possibility of clear scoping. Another argument in favour of a service-centric approach is that it makes sense to have special rules for communications infrastructure, because they are in a position to interfere with individuals' communications privacy at a different level than services that merely use the infrastructure. The main weakness of a service-centric approach is that such an approach can lead to, from a user's perspective, arbitrary differences between the privacy protections applicable to functionally similar services.

D. A data-centric approach

39 A second approach to develop the scope of electronic communications privacy rules is data-centric. A data-centric approach protects privacy interests by setting rules for collecting and using types of personal data.[48] A data-centric approach to privacy regulation lies at the heart of at least a hundred data privacy laws around the world.[49] For instance, the general Data Protection Directive applies if "personal data" are processed.[50]

40 Another example of a data-centric approach to scoping rules is the stricter regime for "special categories" of personal data (also called sensitive data) in the Data Protection Directive. Special categories of data are defined as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and (...) data concerning health or sex life."[51] Processing such special categories of data is in principle prohibited, unless a legal exception applies such as medical necessity.[52] A member state can choose to allow data subjects to override this prohibition by giving their "explicit consent".[53]

41 At first glance, the e-Privacy Directive appears to follow a data-centric approach, regulating personal data, and providing a specific regime for location and traffic data. After all, article 3 states that the "Directive shall apply to the processing of personal data (...)." The provisions regarding traffic and location data particularise the general rules for personal data processing in the Data Protection Directive.[54]

42 However, a number of the e-Privacy Directive's provisions have a broader scope than setting rules for processing categories of personal data. For instance, article 1(1) clarifies that the directive gives "protection of the legitimate interests of subscribers who are legal persons," even though data related to legal persons generally do not qualify as personal data.[55] Similarly, article 5(3) of the e-Privacy Directive

communications (e-Privacy Directive)' (WP159). 10 February 2009; European Data Protection Supervisor. 'Opinion of the European Data Protection Supervisor on the Proposal for a Directive on privacy and electronic communications', Brussels, (2008/C 181/01), 10 April 2008, par 33; European Parliament, 2008. Position in 1st reading, COD/2007/0248, Brussels, Amendment 136.

46 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), COM (2012) 11 final, 25 January 2012, article 31 and 32.

47 European Commission, 2015. Communication of 6 May 2015 on A Digital Single Market for Europe, COM (2015) 192 final.

48 See R. Clarke 'Beyond the OECD guidelines: Privacy protection for the 21st Century', 2000, www.rogerclarke.com/DV/PP21C.html (accessed 15 November 2015).

49 See C.J. Bennett, Data Protection and Public Policy in Europe and the United States, Cornell University Press 1992; P.M. Schwartz & D.J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', New York University Law Review 2011, Vol. 86, pp. 1814-1894; G. Greenleaf, 'Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories', Journal of Law, Information & Science 2013, Vol. 23, No. 1.

50 See article 3(1) of the Data Protection Directive.

51 See article 8(1) of the Data Protection Directive.

52 See article 8(c) of the Data Protection Directive.

53 See article 8(2)(a) of the Data Protection Directive.

54 Some argue that not all traffic and location data are personal data. See C. Cuijpers, A. Roosendaal & B. J. Koops (eds), 'D11.5: The legal framework for location-based services in Europe' (Future of Identity in the Information Society, FIDIS) 12 June 2007 www.fidis.net/fileadmin/fidis/deliverables/fidis-WP11-del11.5-legal_framework_for_LBS.pdf (accessed 15 November 2015).

55 Articles 2(a) and 3(1) of the Data Protection Directive. In some cases, general data protection law can apply to data about legal persons. See B. Van der Sloot, 'Do Privacy and

applies, in short, to anyone that wishes to store or access information on a user's device, including if no personal data are involved. The provision applies to "information", and not to the narrower concept of personal data.[56]

43 The e-Privacy Directive seems primarily concerned with protecting personal data in the electronic communications sector, but the relationship with the Data Protection Directive remains murky. As Rosier says about the e-Privacy Directive: "[i]t is (...) not always clear whether the exact scope of the terms in the provision should be determined only in the light of the definitions provided within the Directive or if it is also necessary to determine the scope of the terms in the Directive in the light of the provisions of the Data Protection Directive".[57]

44 An advantage of a data-centric approach is that it can provide relative clarity. For example, general data protection law can be applied without engaging in open discussions about the scope or meaning of the right to privacy, a concept that is notoriously difficult to define. As De Hert & Gutwirth note: "[t]he strength of data protection (...) is not to be neglected. The complex question 'is this a privacy issue?' is replaced by a more neutral and objective question 'are personal data processed?'"[58]

45 Even though a data-centric approach may offer relative clarity, the scope of the personal data definition still leads to debate, also in the context of electronic communications. For example, for behavioural targeting, companies often process individual but nameless profiles. Many behavioural targeting companies suggest that they only process "anonymous" data, and that, therefore, data protection law does not apply to them.[59]

46 If personal data are within the scope of the special categories of data definition, the data controller must comply with stricter rules. For the data controller, this could be easier than assessing whether certain personal information is sensitive for a particular data subject in a particular context. At the same time, the question of whether certain data fall within the special categories of data definition can be difficult to answer. For instance, do location data revealing regular visits to specialised health clinics constitute medical data? Do images of people constitute special categories of data, because they can reveal race or ethnic origin?[60]

47 As Ohm argues, an advantage of extra protection to certain sensitive data types is that the data types can provide a rule of thumb for a more nuanced approach that takes all relevant circumstances into account.61 Simitis warns that a list of special data categories should be seen as "no more than a mere alarm device. It signals that the rules normally applicable to the processing of personal data may not secure adequate protection".[62]

48 Considering what is at stake for users from a privacy perspective, it makes sense to single out traffic and location data for more strict regulation, as currently stipulated in the e-Privacy Directive. As the Advocate General of the European Court of Justice notes, traffic data are "in a sense more than personal."[63] Traffic data are "'special' personal data, the use of which may make it possible to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity."[64] Mobile devices basically function as location tracking devices, and communications metadata over longer periods can allow for a detailed mapping of an individual's social, professional, and private life, revealing many sensitive details.[65]

49 Unfortunately, the current framework for traffic and location data has flaws. A key problem with the

Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-Tiered System' CLS Rev. 2015, Vol.31, No. 1 p.26; see also L.A. Bygrave, 'Data Protection Law: Approaching Its Rationale, Logic and Limits' (PhD thesis University of Oslo), Kluwer Law International 2002, Part III.

56 See F.J. Zuiderveen Borgesius, 'Personal data processing for behavioural targeting: which legal basis?', International Data Privacy Law 2015, doi: 10.1093/idpl/ipv011.

57 See K. Rosier, 'Comments on the Data Protection Directive', in A. Büllesbach et al. (eds), Concise European IT Law, second edition, Kluwer Law International 2010, p. 176.

58 See P. De Hert & S. Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power', in Claes et al. (eds), Privacy and the Criminal Law, Intersentia 2006, p. 94.

59 See Interactive Advertising Bureau Europe. Your Online Choices. A Guide to Online Behavioural Advertising, About www.youronlinechoices.com/uk/about-behavioural-advertising (accessed 15 November 2015); F.J. Zuiderveen Borgesius, 'Improving Privacy Protection in the area of Behavioural Targeting', Kluwer Law International 2015, chapter 5.

60 The Article 29 Working Party has struggled with the latter question in the context of images of individuals published online. Article 29 Working Party, 'Opinion 5/2009 on online social networking' (WP 163) 12 June 2009, p. 8.

61 P. Ohm, 'Sensitive Information', Southern California Law Review forthcoming Vol. 88, http://ssrn.com/abstract=2501002 (accessed 15 November 2015).

62 S. Simitis, 'Revisiting sensitive data', Report of the Council of Europe 1999, ETS 108, Strasbourg.

63 Opinion AG (12 December 2013) for CJEU, C-293/12 and C-594/12, Digital Rights Ireland Ltd, 8 April 2014, par. 65.

64 Idem, par. 74.

65 See H. de Zwart, 'How your innocent smartphone passes on almost your entire life to the secret service', 2014, www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/ (accessed 15 November 2015).

existing rules for traffic and location data is that those rules only apply to electronic communications networks and services. Since many other parties, including mobile application providers also process such data, it seems questionable whether rules that only apply to electronic communications networks and services add value.[66]

50 Furthermore, national data retention regimes break with the system of stricter rules for traffic and location data. The Data Retention Directive was declared invalid in a manner that leaves little room for Europe-wide blanket data retention.[67] Nonetheless, a number of member states have already adopted or proposed new data retention laws.[68] A review of the current e-Privacy Directive will have to address the question regarding which guarantees people should enjoy with respect to their electronic communications traffic and location data.

51 The data-centric approach has weaknesses. By focusing solely on regulating personal data processing, the law may neglect the ultimate goal of protecting people and social welfare. As Bennet notes, the point at which certain information becomes "personal", information is increasingly difficult to determine. In addition, the rules for the fair processing of personal data can be insensitive to the means of extraction or capture of data. Additionally, even in the case that no personal data about a specific person are captured, there may still exist power imbalances that call for regulatory intervention.[69]

52 For instance, occasionally people are shocked by the use of aggregated and anonymised data that escape data protection law.[70] To illustrate, the Dutch public reacted angrily when the police used aggregated information derived from data gathered by TomTom, a vendor of navigation and mapping products for cars. The police used the data to choose where to install speeding cameras.[71] The Dutch Data Protection Authority examined TomTom's practices, and from a data protection law perspective did not find significant issues.[72] The data obtained by the police were anonymised and aggregated, and thus outside the scope of data protection law.

53 The TomTom case illustrates a broader problem of a data-centric approach in a world of "big data" analytics. Rules for processing personal data do not address the way in which processing other information, including aggregate statistical information based on personal data, can affect a person. Furthermore, anonymisation may take data outside the scope of data protection law, but does not guarantee that people are treated fairly.[73] Furthermore, as Gürses notes, anonymisation can even disempower the individual, when it is used to prevent people "from understanding, scrutinising, and questioning the ways in which these data sets are used to organise and affect their access to resources and connections to a networked world".[74]

54 In addition, stricter rules for certain personal data types may not be nuanced enough. As Nissenbaum notes, sensitivity often depends on the context, rather than on the data type.[75] In 1976, Turn already argued: "[s]ensitivity is a highly subjective

66 See A. Klabunde, 'Datenschutz bei der Erfassung und Nutzung von Standortdaten' ['Data Protection for the Collection and Use of Location Data'], Datenschutz Nachrichten [Data Protection Updates], Vol. 2014, No. 3, pp. 98-102; F.J. Zuiderveen Borgesius, 'Improving Privacy Protection in the area of Behavioural Targeting', Kluwer Law International 2015, p. 281-283; European Commission, 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation', Final Report (a study prepared for the European Commission DG Communications Networks, Content & Technology by Time.Lex and Spark legal network and consultancy ltd, 10 June 2015) http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9962 (accessed 15 November 2015), p. 82.

67 Court of Justice of the EU 8 April 2014, C-293/12 (Digital Rights Ireland).

68 See Eurojust, 'Eurojust's analysis of EU Member States' legal framework and current challenges on data retention', 26 October 2015, http://statewatch.org/news/2015/oct/eu-eurojust-analysis-ms-data-retention-13085-15.pdf (accessed 15 November 2015), pp. 4-5: The national implementation law of the Data Retention Directive was struck down in at least eleven Member States. In 14 Member States the national law remains in force. See generally F.J. Zuiderveen Borgesius and A. Arnbak, 'New Data Security Requirements and the Proceduralization of Mass Surveillance Law after the European Data Retention Case', Amsterdam Law School Research Paper No. 2015-41. http://ssrn.com/abstract=2678860 (accessed 15 November 2015), p. 36-38.

69 See C.J. Bennett, 'In Defence of Privacy: the concept and the regime', Surveillance & Society 2011 Vol. 8, No. 4, pp. 485-496, pp. 491-493.

70 These two paragraphs on TomtTom are based on: F.J. Zuiderveen Borgesius, J. Gray, M. van Eechoud, 'Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework', Berkeley Technology Law Journal (forthcoming).

71 TomTom, 'This is what we really do with your data', www.tomtom.com/page/facts (accessed 15 November 2015).

72 Dutch Data Protection Authority, 'Following report by Dutch DPA, TomTom provides user with better information' 2012, https://cbpweb.nl/en/news/following-report-dutch-dpa-tomtom-provides-user-better-information (accessed 15 November 2015).

73 S. Barocas & H. Nissenbaum, 'Big Data's End Run around Anonymity and Consent', in J. Lane et al. (eds.), Privacy, Big Data, and the Public Good: Frameworks for Engagement, Cambridge University Press 2014.

74 S. Gürses, 'The Spectre of Anonymity', vous-etes-ici.net/wp-content/uploads/2014/02/SedaAnonymityMute.pdf (accessed 15 November 2015). See also B. Custers, The power of knowledge, Ethical, legal, and technological aspects of data mining and group profiling in epidemiology, Nijmegen: Wolf Legal Publishers 2004, p. 201.

75 H. Nissenbaum, Privacy in context: technology, policy, and the integrity of social life, Stanford Law Books 2009.

and context-dependent property of personal information – what one individual may consider very sensitive may be regarded with indifference by many others, and it is likely that there is a large range of sensitivity assessments for every information item." He adds: "[e]ven the same information item may be innocuous in one system of records, but very sensitive in another. For example, while a person's name is usually public information, it becomes sensitive when associated with a system of psychiatric treatment records".[76]

55 Such considerations lead a number of authors to criticise data protection law's stricter regime for special categories of data. McCullagh argues: "[t]he current approach of listing certain types of personal data as sensitive engages in an a priori classification exercise which is flawed. It is a fallacy. The privacy sensitivity of data cannot be pre-determined; rather it is influenced by contextual factors, and so, should be determined on a posterio basis".[77]

56 A final drawback of the existing rules for certain data categories is that the rules are seemingly based on the assumption that personal data will be generated. From a privacy perspective, it may make sense to consider the electronic communications architecture itself – and whether personal data need to be generated at all. Aiming to ensure that electronic communications networks and services are designed in a privacy-friendly manner could be more effective to protect privacy, than aiming to ensure that personal data are processed fairly after they have been generated.

57 While the data-centric approach has weaknesses, continuing the e-Privacy Directive's data centric approach has some merit. There is considerable experience with regulating personal data and with protecting privacy in electronic communications through rules for specific data types. Another argument in favour of a data-centric approach is that the e-Privacy Directive aims to complement and particularise the general data protection framework, which regulates the processing of personal data.

E. A value-centric approach

58 A third approach to develop the scope of the electronic communications privacy framework is value-centric, and focuses on the fundamental societal values that need protection. These values include the right to private life and confidentiality of communications, as well as the fair processing of communication-related personal data, as protected through the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights. As its preamble shows, the current e-Privacy Directive focuses on these fundamental values in the electronic communications context. The directive aims to protect the data protection and privacy rights from the Charter of Fundamental Rights of the European Union.[78]

59 In addition to protecting the confidentiality of private communications, the e-Privacy Directive provides for specific restrictions on the processing of communications related metadata, as discussed in the previous section. These specific protections should be seen in the light of the fundamental right to personal data protection, in the Charter of Fundamental Rights of the European Union.[79] Furthermore, electronic communications metadata fall within the scope of the right to private communications in the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union.[80]

60 The way in which the protection of these values is operationalised in the e-Privacy Directive's provisions still resonates best with the use of electronic communications for telephone calls and other types of electronically mediated conversations between individuals, such as email. As mentioned in the introduction to this paper, we use electronic communications networks for many purposes, including shopping, distance-working, accessing news, and interacting with government. Therefore, the lawmaker should consider a wider range of privacy and communications related fundamental values at stake for individuals in contemporary electronic communications.[81]

61 Values that are currently underemphasised in the e-Privacy Directive are freedom of expression and

76 R. Turn, 'Classification of personal information for privacy protection purposes', AFIPS '76 Proceedings of the June 7-10, 1976, national computer conference and exposition, pp. 301-307.

77 K. McCullagh, 'The social, cultural, epistemological and technical basis of the concept of' 'private' data', PhD thesis University of Manchester, 2012, www.escholar.manchester.ac.uk/uk-ac-man-scw:157750 (accessed 15 November 2015), pp. 189-190.

78 Recital 2 and 3 of the e-Privacy Directive.

79 Article 8 of the Charter of Fundamental Rights of the European Union.

80 Article 7 of the EU Charter of Fundamental Rights; article 8 of the European Convention on Human Rights. See also: Court of Justice of the EU 8 April 2014, C-293/12 (Digital Rights Ireland).

81 See also: A. Arnbak, 'Securing Private Communications' (PhD thesis University of Amsterdam, academic version), http://hdl.handle.net/11245/1.492674 (accessed 15 November 2015), p. 127-141.

the freedom to communicate more generally. These values are not specifically mentioned in the current e-Privacy Directive. However, the effective exercise of the right to freedom of expression is increasingly dependent on access to electronic communications networks, and on the conditions under which access can take place, including the protection of privacy and personal data.[82]

62 Privacy and freedom of expression are closely related.[83] The early history of the right to confidentiality of communications illustrates the connection between that right and the right to freedom of expression. When the right to confidentiality of correspondence was developed in the late eighteenth century, it was seen as an auxiliary right to safeguard freedom of expression.[84] Nowadays the right to confidentiality of communications is primarily regarded as a privacy-related right, but the connection remains, as is illustrated in the Digital Rights Ireland judgment by the Court of Justice of the European Union, on the Data Retention Directive:

> *It is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter.*[85]

63 A weakness of a value-centric approach to scoping electronic communications privacy rules is that the guidance from values could remain too vague. Most people would agree that we want to foster human dignity, freedom, equality and solidarity, as the EU Charter of Fundamentals Rights puts it.[86] Likewise, most would agree that living conditions should improve, and peace, liberty and democracy should be strengthened, as the preamble of the Data Protection Directive suggests.[87] However, operationalising such goals is difficult.

64 A distinction put forth by Bordewijk and Van Kaam of four communication models can help to operationalise a value-based approach.[88] Four types of communication can be distinguished: (i) the classic telecommunications model, including new forms of electronic correspondence; (ii) the consultation model, regarding access to information and electronically available resources; (iii) the registration model, regarding, for instance, tracking users for electronic marketing; (iv) the publishing model, regarding electronic publishing or broadcasting. Each communication model implicates different user interests and therefore calls for different types of privacy protection.

65 Regarding the classic telecommunications model, the rules for classic voice communication and data exchange of a similarly conversational nature in the e-Privacy Directive are the most advanced. The e-Privacy Directive focuses on protecting the privacy interests at stake in this model, including the confidentiality of communications and related traffic data. However, the e-Privacy Directive does not protect these interests for services that are functionally equivalent to telecommunication services. From a value-centric point of view, this situation is hard to defend. In addition, the underlying fundamental value of the freedom to communicate could be made more explicit in the e-Privacy Directive.

66 In the consultation model, people use electronic networks to access many informational resources, such as news, government information, medical records, educational offerings, and entertainment. This use of the network includes access to software that can be installed on the device and allows for new types of usage of the network. Here, the primary interest of the user is to access the network to enjoy these resources.

67 From a regulatory perspective, the question is under which conditions people should be able to access such resources. For instance, should it be possible to gain access to these resources without having to identify oneself or leaving an identifiable trace between different destinations? Additionally, considering the interests in societal inclusion and participation at stake with access to communications networks, should more specific provisions be adopted for the tracking and logging of network use? Currently, the

82 See Court of Justice of the EU 8 April 2014, C-293/12 (Digital Rights Ireland), par 28.

83 See Richards NM, 'Intellectual privacy' Texas Law Review 2008, Vol. 87, p.387; J.V.J. Van Hoboken, 'Search engine freedom: on the implications of the right to freedom of expression for the legal governance of search engines' (PhD thesis university of Amsterdam), Kluwer Law International 2012, p. 226.

84 See B.R. Ruiz, 'Privacy in telecommunications: a European and an American approach', Kluwer Law International 1997, p. 67; see also ECtHR 22 May 1990, Autronic AG v. Switzerland, par. 47.

85 Court of Justice of the EU 8 April 2014, C-293/12 (Digital Rights Ireland).

86 See the preamble of the Charter of Fundamentals Rights of the European Union.

87 Recital 1 of the Data Protection Directive.

88 See J.L. Bordewijk & B. van Kaam, 'Towards a new classification of tele-information services', InterMedia, 1986 Vol. 14, No. 1, pp. 16-21; J.C. Arnbak, J.J. Van Cuilenburg & E.J. Dommering, Verbinding en Ontvlechting in de Communicatie, een studie naar toekomstig overheidsbeleid voor de openbare elektronische informatievoorziening [Bundling and unbundling of communication, a study into future government policy regarding public electronic information provision], Cramwinckel 1990, pp. 7-9.

e-Privacy Directive leaves access to information mostly unaddressed.

68 The registration model concerns, for example, tracking users for electronic marketing. Electronic networks are often used to track, monitor, and reach users. Regarding such practices, the e-Privacy Directive offers some protection. First, current provisions regarding unsolicited communications aim to ensure that having an email address does not imply getting email from anyone that wants to reach a user.[89] Second, article 5(3) of the e-Privacy Directive applies to tracking users with cookies or similar technologies.

69 The publishing model concerns electronic publishing or broadcasting. Electronic communication networks enable people to publish information and ideas, including information and ideas related to matters of public concern. There is a need to consider privacy guarantees that should apply to this kind of use of electronic communications. For instance, should the possibility to publish anonymously be protected?

70 The current e-Privacy Directive does not contain rules that focus on the privacy protections connected to the use of the network for electronic publication and broadcasting purposes. Services outside the scope of the current electronic communications regulatory framework set the predominant conditions for publishing online. For instance, social media sites and other publication platforms can censor or remove individuals' contributions to online debate. Facebook sometimes censors users' posts.[90] But electronic communications networks and services could also interfere with freedom of expression. For example, access to specific publication platforms could be curtailed or compromised.[91] It may be necessary to adopt electronic communication privacy rules that protect users when they publish information for an online audience.

71 In sum, a value-centric approach could help to highlight the freedom of communication as a core value in the electronic communications context. This approach can ensure a more systematic evaluation and robust protection of the privacy interests at stake in the communications sector. The four communication models discussed above can help to identify user interests that go beyond the privacy interests at stake in traditional telecommunications networks, but that do deserve to be protected in sector-specific electronic communications privacy laws.

F. Conclusion

72 In this paper, we introduce a distinction between three approaches to electronic communication privacy rules. The scope of the rules could be developed based on (i) a service-centric approach, (ii) a data-centric approach, and (iii) a value-centric approach. Each of the approaches has strengths and weaknesses. We provide the distinction between the three approaches as an analytical tool, to assist in discussions concerning the scope of electronic privacy rules. The recently announced review of the e-Privacy Directive provides an opportunity to improve the current scope.

73 In a service-centric approach to develop the scope of electronic communications privacy rules, the scope of the rules is delineated on the basis of different services. The primary strength of the service-centric approach, which is currently dominant in the e-Privacy Directive, is clarity for market actors. The service-centric approach also conforms well to the infrastructural nature of electronic communications networks and services. The main weakness of a service-centric approach is that it can lead to different privacy rules for communication services that are functionally equivalent to users. The e-Privacy Directive should make clear that any party (rather than only "providers of publicly available electronic communications services" and "providers of public communications networks") must respect confidentiality of communications.

74 A data-centric approach protects users' privacy interests through the proxy of regulating the processing of types of personal data. The data-centric approach is also present in the e-Privacy Directive, for instance in the rules for location and traffic data. We conclude that the protective rules for traffic and location data should be extended to information society services.

75 Regulating the processing of certain data types can be a helpful proxy to protect user interests. Still, the rationale for having an electronic communications privacy framework should be protecting people – not data. A value-centric approach determines the scope of the rules based on the fundamental user interests at play. These interests go beyond the privacy interests at stake in traditional telecommunications networks. In particular, the lawmaker should more explicitly recognise freedom of expression and freedom of communication as fundamental values

89 Article 13 of the e-Privacy Directive.

90 See M. Heins, 'The Brave New World of Social Media Censorship', Harvard Law Review 2013,127 325.

91 See Citizen Lab and C. Anderson, 'The Need for Democratization of Digital Security Solutions to Ensure the Right to Freedom of Expression', Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 10 February, 2015, Appendix, p. 4, https://citizenlab.org/wp-content/uploads/2015/02/SR-FOE-submission.pdf (accessed 15 November 2015).

underlying the directive.

* Dr. Joris van Hoboken is a Postdoctoral Research Fellow at New York University, School of Law, Information Law Institute (ILI). Dr. Frederik Zuiderveen Borgesius is a Researcher at the University of Amsterdam, Faculty of Law, Institute for Information law (IViR). The authors would like to thank the participants at the EuroCPR 2015 conference, and Achim Klabunde in particular, for their comments on an earlier draft of this paper. The authors also thank Nico van Eijk and the anonymous reviewer for their useful comments. Where this paper discusses article 5.1 and article 5.3 of the e-Privacy Directive, and the concept of personal data and special categories of personal data, the paper builds on, and includes sentences from, F.J. Zuiderveen Borgesius, Improving Privacy Protection in the area of Behavioural Targeting, Kluwer Law International 2015.

Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe

by **Bart van der Sloot***

Abstract: In Europe, roughly three regimes apply to the liability of Internet intermediaries for privacy violations conducted by users through their network. These are: the e-Commerce Directive, which, under certain conditions, excludes them from liability; the Data Protection Directive, which imposes a number of duties and responsibilities on providers processing personal data; and the freedom of expression, contained inter alia in the ECHR, which, under certain conditions, grants Internet providers several privileges and freedoms. Each doctrine has its own field of application, but they also have partial overlap. In practice, this creates legal inequality and uncertainty, especially with regard to providers that host online platforms and process User Generated Content.

Keywords: liability; intermediaries; privacy violations; ECHR; freedom of expression; data protection

Recommended citation: Bart van der Sloot, Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe, 6 (2015) JIPITEC 211 para 1.

A. Introduction

1 When Internet companies and private parties started to offer Internet services in the 1980s, there was already discussion concerning the position of Internet intermediaries. Initially, the provider was often seen as the digital equivalent of a postal company, which had neither knowledge of nor control over the post that was delivered by it and therefore could not, in principle, be held liable for any illegal content. At that time however, there existed two separate doctrines regarding third party liability for copyright infringements in the United States, where the Internet experienced its initial growth. "Vicarious liability" entailed that a third party could be held liable for infringing activities if it had the right and ability to control over and gained financial profits from the activity, and "contributory liability", which regarded third parties that had knowledge of and contributed to the infringing activity.[1] These doctrines were gradually also applied to Internet service providers. This meant that if an Internet intermediary wanted to avoid liability for, for example, copyright infringements by its users, the intermediary would have to prove that it did not know of the infringing nature of the material, that it did not contribute in any way to the infringement and that it had not received any financial gain from the infringement.[2]

2 This jurisprudential doctrine was subsequently further developed in the US Digital Millennium Copyright Act (DMCA) of 1998, which makes a distinction between (1) providers that offer access to networks and data transmission via these networks (access providers/mere conduits), (2) providers temporarily storing material on their server (caching providers), (3) providers that store information or host websites (hosting providers) and (4) providers that offer links to websites or make content searchable (search engine providers).[3] The European Union (EU) has a regulation similar to the DMCA,[4]

1 A. Strowel, 'Peer-to-Peer file sharing and secondary liability in Copyright Law', Cheltenham, Edward Elgar Publishing, 2009.

2 M. B. Nimmer & D. Nimmer, 'Nimmer on copyright: a treatise on the law of literary, musical and artistic property, and the protection of ideas', New York: Bender, 1994.

3 Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998), para. 512.

4 See for a good comparison: M. Peguera, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems', Columbia Journal of Law &

laid down in the e-Commerce Directive 2000.[5] The rules therein contained form the general basis for the exclusion of liability of Internet intermediaries under European law (so called safe harbors). Although this regime applies to virtually all offenses, data protection issues are explicitly excluded.[6] In such cases, the Data Protection Directive[7] applies. There is a third regime that is increasingly applied as well, namely when an Internet intermediary relies on the freedom of expression to protect its own interests, for example under the European Convention on Human Rights (ECHR).

3 It should be borne in mind that in the early days, Internet intermediaries were predominantly of a passive nature, and that the e-Commerce Directive is written for providers that transmit or store material on behalf of users only. In the modern Internet landscape however, providers have become much more active, for example by providing the platform on which information is shared by users, by indexing this information, by making it searchable and by publishing and distributing the information over the Internet. Examples of active Internet intermediaries are platforms such as Facebook, video services such as Youtube, digital markets such as eBay and modern media such as WikiLeaks or news sites (partially or primarily) based on stories, contributions and comments written by users. In these examples, the content is still provided by the users, but the role of the Internet intermediary is no longer merely to transmit, store or publish the material on behalf of the user – rather it fulfils an active role in the organization and functioning of the websites and platforms. The question thus becomes what position these providers have with regard to material of an infringing nature uploaded by their users.

4 Recently, the Court of Justice (ECJ) ruled in its Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González verdict (hereafter: Google Spain) that Google may be required to block or delink certain information from other website in its search engine in order to respect the data subject's right to be forgotten.[8] The ECJ has also held that the obligation to monitor and store all Internet traffic, contained in the Data Retention Directive, is invalid and violates the rights to privacy and data protection.[9] In Delfi v. Estonia, the European Court of Human Rights (ECtHR) in 2013 and the Grand Chamber of the ECtHR in 2015 ruled that online news sites that facilitate user reactions can invoke the right to freedom of expression, but can also be held liable for user comments that harm third party interests.[10] The Council of Europe (CoE), in 2011, developed a new vision on modern media, proposing inter alia to apply the classic protection of journalists to bloggers and other new media.[11] In addition, there are advanced plans in the EU to introduce the General Data Protection Regulation, which will radically change the legal data protection regime laid down in the current Data Protection Directive.[12] Finally, for years now, there has been a discussion concerning the possible revision of the e-Commerce Directive, precisely as regards to the liability regime for Internet intermediaries, in which respect the European Commission in 2010 initiated a public consultation[13] and in 2012 launched a special consultation on hosting providers.[14]

5 This contribution will explain and analyze the three legal regimes in Europe that are applicable to Internet intermediaries, giving special attention to recent developments and case law. Section B discusses the liability regime under the e-Commerce Directive, the relevant case law of the ECJ and the plans to amend the directive. Section C discusses the regime under the Data Protection Directive, the relevant case law of the ECJ, including the Google Spain case, and the possible changes resulting from the pending General Data Protection Regulation. Section D discusses the doctrine on the freedom

Arts, vol. 32. no. 4, 2009.

5 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 or the e-Commerce Directive).

6 There are however authors that have rejected a literal reading of this provision. See among others: G. Sartor, "Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?' International Data Privacy Law 2013-3.

7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).

8 Court of Justice, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, case C131/12, 13 May 2014.

9 Court of Justice, Digital Rights Ireland Ltd (C293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung (C594/12), Michael Seitlinger, Christof Tschohl and others, cases C293/12 and C594/12, 08 April 2014.

10 European Court of Human Rights, Delfi AS v. Estonia, appl. no. 64569/09, 10 October 2013. European Court of Human Rights, Delfi AS v. Estonia, appl.no. 64569/09, 16 June 2015.

11 Committee of Ministers, 'A new notion of media', CM/Rec(2011)7, 21 September 2011.

12 In this contribution, for reasons of conciseness and clarity, reference shall be made only to the original proposal by the Commission. Commission, Proposal for a General Data Protection Regulation, COM(2012)11final, 25 January 2012.

13 http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm.

14 http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-Internet_en.htm.

of expression enshrined in Article 10 ECHR, the relevant case law of the ECtHR, including the case of Delfi v. Estonia, and the recommendation of the CoE. Finally, section E will provide a conclusion and an overview of the three regimes. This contribution will focus specifically on the position of hosting providers and active Internet intermediaries, as active intermediaries are increasingly dominant in the modern Internet environment, but their legal position is often vague and unclear.[15]

B. E-Commerce Directive

6 The e-Commerce Directive regulates a variety of different topics, including the liability of Internet intermediaries, providing so called safe harbors. A distinction is made between three types of services offered by providers. Firstly, Article 12 specifies that an access provider is not liable for the information transmitted, on the condition that the provider (a) does not initiate the transmission, (b) does not select the receiver of the transmission and (c) does not select or modify the information contained in the transmission. These providers are excluded from liability and have very limited additional responsibilities as long as they remain passive. Secondly, Article 13 regards providers engaged with caching. This provision has been of little importance so far and will therefore remain undiscussed in this contribution. Finally, Article 14 holds that a hosting provider is not liable for the information stored, provided that (a) the provider does not have actual knowledge of the illegal nature of the activity or information and, as regards to claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent and (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.[16]

7 In addition, Article 15 provides that Member States may not impose a general obligation on intermediaries to monitor the information that they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity. In the cases of Scarlet v. Sabam and Sabam v. Netlog,[17] the ECJ held inter alia that the e-Commerce Directive, read in conjunction with other directives, precludes "a national court from issuing an injunction against a hosting service provider which requires it to install a system for filtering information which is stored on its servers by its service users, which applies indiscriminately to all of those users, as a preventative measure, exclusively at its expense and for an unlimited period, which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright."[18]

8 Remarkably, the e-Commerce Directive, unlike the DMCA, contains no specific provision for search engines. However, Article 21 states, among others, that the report on the implementation of the Directive should examine whether proposals ought to be made to amend the Directive in order to include rules on the liability of search engines. Meanwhile, the ECJ ruled in Google v. Louis Vuitton that Google's advertising service, which is provided in conjunction with its search engine, may fall within the scope of Article 14 since that provision must "be interpreted as meaning that the rule laid down therein applies to an Internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned."[19] It is not unreasonable to argue that the search function itself, under certain conditions, may also fall under the regime of Article 14.[20]

9 The question is, however, whether active Internet

15 See further: N. van Eijk (et al.), 'Moving Towards Balance: A study into duties of care on the Internet', http://www.ivir.nl/publicaties/download/679.

16 See also consideration 42 e-Commerce Directive. Whether this recital applies to Article 14 e-Commerce Directive is a matter of debate.

17 Court of Justice, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), intervening parties: Belgian Entertainment Association Video ASBL (BEA Video), Belgian Entertainment Association Music ASBL (BEA Music), Internet Service Provider Association ASBL (ISPA), case C-70/10, 24 November 2011. Court of Justice, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, case C360/10, 16 February 2012. See further: S. Kulk and F. Borgesius, 'Filtering for copyright enforcement in Europe after the Sabam cases', European Intellectual Property Review, Vol. 34 No. 11, 2012.

18 SABAM/Netlog, para. 53.

19 Court of Justice, Google France SARL, Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA, Luteciel SARL (C-237/08), and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08), cases C-236/08, C-237/08 and C-238/08, 23 March 2010, para. 120.

20 See more in general: J. van Hoboken, 'Search engine freedom: on the implications of the right to freedom of expression for the legal governance of web search engines', Kluwer Law International, Alphen aan den Rijn, 2012.

intermediaries (such as s Facebook, Ebay, Youtube and news sites that run on User Generated Content) can also rely on Article 14. Of course, this will not be the case with, for example, news sites that publish their own material, written by their own employees on their own website.[21] They will be regarded as publishers, not as Internet providers. However, the question is more difficult to answer with respect to intermediaries such as Facebook, Ebay, Youtube and news sites that run on User Generated Content. The ECJ appears to have answered this question affirmatively in its L'Oreal v. Ebay ruling, which focused on illegal content posted by users on Ebay. The Court held in respect of Ebay that "the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability provided for by Directive 2000/31."[22] However, at the same time, it cannot "rely on the exemption from liability provided for in that provision if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously in accordance with Article 14(1)(b) of Directive 2000/31."[23]

10 The phrase "diligent economic operator" causes a new problem. As active Internet intermediaries have a greater influence on and control over the websites than traditional hosting providers, it is generally assumed that active intermediaries also have a broader duty of care to ensure that their sites and platforms remain free of infringing material, for example, by monitoring their sites, by installing filter systems or by appointing system administrators. A study from 2010 hinted towards exactly this potential vicious circle. "Checking Internet traffic for [enforcement purposes] is not effective, and it is technically unfeasible. A formal duty of care would lead to excessive intervention by Internet service providers and possibly could escalate in the creation of further duties of care in other fields. Intervention with regard to illegal content in general might be next and would result in disproportionate restrictions on (future) economic activities on the Internet."[24] Consequently, duties of care may create a Catch-22 situation.[25] Since providers are more directly involved in the design and the layout of the websites, they have a broader duty of care; the broader duty of care implies that they should exercise additional control over the content submitted by users. However, this will create a situation in which they have an even greater involvement in and control over the platform or service, which again could entail an even broader obligation to monitor, filter and control content. This is a spiral to which there is no logical end. In practice, this issue creates much legal uncertainty, as national regulators and courts differ in their approach to this topic.[26]

11 As an example a Dutch case may be referred to, in which a file sharing site did filter pornography and viruses, but did not filter with respect to possibly copyright infringing material. The judge concluded that the site, Mininova, was liable for this content because it had the capacity and the means to control the site on illegal content, but refused to do so with respect to content infringing on intellectual property.[27] This means that from the capacity to control, a duty of further control may be derived.[28] This is partly due to the fact that Europe lacks a clear Good Samaritan clause, such as, inter alia, contained in the Communications Decency Act of the United States. 47 U.S. Code § 230, on the protection for private blocking and screening of offensive material, sub C, on the protection for "Good Samaritan" blocking and screening of offensive material, provides: "(1) Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. (2) Civil liability. No provider or user of an interactive computer service shall be held liable on account of — (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)."[29]

21 See Art. 14 para. 2 e-Commerce Directive and Court of Justice, Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis, case C291/13, 11 September 2014.

22 Court of Justice, L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal (UK) Ltd v eBay International AG, eBay Europe SARL, eBay (UK) Ltd, Stephen Potts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana Bi, case C324/09, 12 July 2011, para. 115.

23 L'Oréal/eBay, para. 124. See further: B. Clark, B. and M. Schubert, 'Odysseus between Scylla and Charybdis? The ECJ rules in L'Oréal v eBay', Journal of Intellectual Property Law & Practice, Vol. 6 No. 12, 2011.

24 http://www.ivir.nl/publicaties/download/679.

25 J. Heller, 'Catch-22: a novel', New York, Simon and Schuster, 1961.

26 See also: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

27 ECLI:NL:RBUTR:2009:BJ6008.

28 See further: http://www.ivir.nl/publicaties/download/999.

29 https://www.law.cornell.edu/uscode/text/47/230.

12 In connection to this, mention should be made of the former plans to revise the system of liability under the e-Commerce Directive with regard to active Internet intermediaries and search engines. Both in 2003[30] and in 2008,[31] reports were issued, but both were very reticent about making actual proposals regarding effective changes to the liability regime. In 2010, the European Commission launched a public consultation on a possible revision, and the report, among other conclusions, states: "National jurisprudence on hyperlinking is very fragmented. A UK court considered it to be a mere conduit activity (art 12 ECD), a German court considered it to be a form of hosting (art 14 ECD), while a Belgian court considered that the ECD was not relevant for hyperlinking activities. Spain and Portugal have extended the liability exemption to hyperlinking and search engine activities."[32] This is just one example of the diversity of and imparity between the different national approaches to Internet liability. However, many respondents saw no benefit in changing the current protection regime. Reportedly, ISPs were afraid of further obligations and responsibilities; Intellectual Property organizations for a greater role for consumer rights; consumer groups for excessive lobbying by the industry, etc. For now, the current regime remains unaltered and it is left mainly to national courts and authorities to interpret the liability regime and apply it to new developments.

13 Finally, a noteworthy point regarding the application of the e-Commerce Directive to data protection matters. It follows from Article 1 paragraph 5 sub b, that the safe harbors do not apply to questions relating to information society services covered by the Data Protection Directive and the e-Privacy Directive.[33] Recital 40 of the e-Commerce Directive states that the existence of different regimes in respect of civil and criminal liability in the different countries distorts the internal market, which the directive would like to end by harmonization. The recital continues: "the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC [the Data Protection Directive] and 97/66/EC [the predecessor of the e-Privacy Directive]." These are notoriously vague statements. For example, do they mean that the e-Commerce Directive could apply to data protection issues, but should not lead to a lower level of protection, or that the e-Commerce Directive simply does not apply to data protection issues at all?

14 The ECJ case law demonstrates that a distinction should be made between three types of cases. First, cases in which intermediaries are held liable for an infringement committed by a user through its network, for example, an intellectual property right - the e-Commerce Directive is applicable. Second, cases in which intermediaries are held liable for an infringement, committed by a user via its network, of a person's right to data protection - the Data Protection Directive is applicable. Third, cases in which an infringement of an intellectual property right has been initiated by a user and an Internet service provider is asked to provide the name and address of the user (that is to provide personal data) or to effectuate a monitoring system - both directives apply. In such cases, the ECJ will assess the case by relying on various directives, such as the e-Commerce Directive, the directives on data protection and the directives regarding the protection of intellectual property. For example, this was the case in the aforementioned matter of Scarlet v. Sabam, regarding the potential monitoring obligation imposed on an Internet intermediary.[34]

15 As an illustration, reference can also be made to the case of Promusicae v. Telefonica, which concerned the request for obtaining the names and addresses of users of Telefonica, whom were suspected of having used the KaZaA P2P network.[35] When the case went to court, Telefonica objected and argued that it could only provide the data in the context of criminal proceedings or in the case that it would be necessary to safeguard public order and national security, but not in the context of civil proceedings or as an interim measure prior to such proceedings. The question of the Spanish court to the ECJ was whether it was obliged to rule that Telefonica was obliged to provide the personal data of their customers. The Court held that the e-Commerce Directive, two directives regarding the protection of intellectual property,[36] and the e-Privacy Directive

30 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0702&from=EN.

31 http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

32 http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf.

33 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 or the e-Privacy Directive). Directive 97/66/EC has been replaced by Directive 2002/58/EC and the references to the first directive must be read as a reference to the second directive.

34 See further: Court of Justice, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH, case C-557/07, 19 February 2009.

35 See also: C. Angelopoulos, 'Sketching the outline of a ghost: the fair balance between copyright and fundamental rights in intermediary third party liability', info, Vol. 17 Iss 6, 2015. X. Groussot, 'Rock the KaZaA: another clash of fundamental rights', Common Market Law Review, Vol. 45 No. 6, 2008.

36 Directive 2001/29/EC of the European Parliament and of the

had to be read in conjunction with each other and concluded that they "do not require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings."[37] How the balance between the different interests should be made depends on the circumstances of the case. Consequently, in the Promusicae v. Telefonica case, the ECJ refrained from providing a standard line of interpretation.[38]

C. The Data Protection Directive

16 The previous paragraph discussed the rules regarding the liability of Internet intermediaries with respect to infringements other than on the right to data protection. It also discussed the situation in which the right of users' data protection and the right to intellectual property of third parties clash. This section will analyze cases in which Internet intermediaries may be held liable for infringements on the right to data protection of third parties, conducted by their users through their networks. The Data Protection Directive generally applies when four criteria are met: (1) personal data, (2) are processed, (3) by a controller and (4) the territoriality principle applies. (1) Any data is personal data when a person could possibly be identified through it; importantly, "personal data" does not only revolve around private or privacy-sensitive data.[39] General and public information that can identify someone, such the phrase (indicating a person), "the man next to the lamppost", may already qualify as personal data.[40] Even if data at a given point in time does not identify anyone, but may do so over the course of time, for example by using advanced identification techniques, they will be considered "personal data". Consequently, ISPs will typically process personal data, as in almost every message, in every comment and on every website, personal data is contained.[41] (4) Additionally, the element of territoriality will usually be met, but this will not be discussed in depth in this contribution.[42]

17 (2) When something is done with personal data, it almost always falls under the legal definition of "processing", whether it denotes storing, publishing, distributing, blocking or even deleting data – it is all considered to be "processing".[43] Only the pure transmission of information provided by a user over a network will usually not fall under its scope. Consequently, access providers are in principle excluded from upholding the rights and duties under the Data Protection Directive.[44] Finally, there must be (3) a controller. The controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. The controller is contrasted to the "processor", which is the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.45 It follows, inter alia, that purely passive hosting providers, that neither determine the means nor the purpose of the data processing, will in principle not be considered the controller, but the processor of personal data. Therefore, they are not responsible for upholding the rights and duties under the Directive, the controller is. "An ISP providing hosting services is in principle a processor for the personal data published online by its customers, who use this ISP for their website hosting and maintenance. If however, the ISP further processes for its own purposes the data contained on the websites then it is the data controller with regard to that specific processing."[46]

18 To this extent, the regime with regard to the responsibilities of Internet intermediaries under the Data Protection Directive, is largely consistent with that of the e-Commerce Directive. However, a number of points should be noted in this respect. First, the e-Privacy Directive is applicable to passive

Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society and Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

37 Court of Justice, Productores de Música de España (Promusicae) v Telefónica de España SAU, case C275/06, 29 January 2008, para. 70. See also: Court of Justice, Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB, case C461/10, 19 April 2012. See further: S. Kiekegaard, 'ECJ rules on ISP disclosure of subscribers' personal data in civil copyright cases – Productores de Múrica de España (Promusicae) v Telefónica de España SAU (Case C-27/ 06)', Computer Law & Security Report, Vol. 24 No. 3, 2008. C. Kuner, 'Data protection and rights protection on the internet: the Promusicae judgment of the European Court of Justice', European Intellectual Property Review, Vol. 30 No. 5, 2008.

38 See also: Court of Justice, Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB, Case C461/10, 19 April 2012.

39 Article 2 sub a Data Protection Directive.

40 Working Party 29, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007.

41 See also: Working Party 29, Privacy on the Internet, WP 37, 21 November 2000.

42 See also: Working Party 29, Opinion 8/2010 on applicable law, WP 179, 16 December 2010.

43 Court of Justice, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy, case C73/07, 12 February 2007.

44 This also follows from the interpretation of the concept of 'controller', see inter alia consideration 47 of the Data Protection Directive.

45 Article 2 sub d and e Data Protection Directive.

46 Working Party 29, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 February 2010.

Internet intermediaries such as access providers.[47] The directive determines, among other things, that these providers need to adequately secure their networks and that they must process personal data confidentially.[48] Without the consent of the user, for example, providers may in principle not put information on or pull information from a computer device, for example, through the use of a cookie.[49] Further information may in principle only be processed if this is necessary for or related to the provision of the service requested by the user or for related services.[50] With respect to these data processing activities, the providers are responsible for processing these data.

19 Active Internet intermediaries will in principle be considered the controller of data within the context of the Data Protection Directive because they determine the goal and the means of the data processing. This also applies to search engines,[51] as recently evidenced by the Google Spain judgment of the ECJ. In its search engine, Google had referred to a story in a newspaper, that had digitalized its archive and published it online. Mr. Costeja González's name appeared in relation to a real-estate auction connected to proceedings for the recovery of social security debts. The content of the message itself was not illegal, neither was the newspaper requested to remove the announcement from its paper archive or even from its website. The question was whether Google should be obliged to delete the link to the story from its search engine and related to that, whether it could be held responsible for processing personal data because it had indexed the material and made it possible to search the contents of the material. The Court held: "It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing".[52] Consequently, there seems to be a fundamental difference in comparison to the regime under the e-Commerce Directive, because even more active Internet intermediaries can, under certain conditions, invoke the safe harbors therein contained and search engines presumably can too. To recount briefly, the ECJ held in its Google v. Louis Vuitton decision that Article 14 must "be interpreted as meaning that the rule laid down therein applies to an Internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored."[53]

20 The disparity between the two regimes is aggravated by the fact that the person responsible under the data protection regime is the one who "alone or jointly" determines the purpose and means of the processing. Since active Internet intermediaries typically provide the technical infrastructure and make the platform available, which users use to share their information, they will often be partially or wholly responsible.[54] "Social network service providers provide online communication platforms which enable individuals to publish and exchange information with other users. These service providers are data controllers, since they determine both the purposes and the means of the processing of such information. The users of such networks, uploading personal data also of third parties, would qualify as controllers provided that their activities are not subject to the so-called 'household exception'."[55]

21 The active Internet intermediaries will therefore generally be regarded as having a (shared) responsibility for the data processing. There are, however, two important exceptions, namely the household exception and the journalistic exception - the latter is linked to the protection of freedom of expression, as enshrined, among others, in Article 10 ECHR. The first exemption specifies that the provisions of the directive do not apply to the processing of personal data carried out by a natural person in the course of a purely personal or household activity.[56] In Lindqvist, the ECJ held in this regard that the household exemption in principle does not apply to personal data published on the Internet, even if a site is relatively unknown and used for private purposes only. "That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people."[57] Possibly, the exemption may still apply to webpages

47 Article 3 e-Privacy Directive.

48 Article 4 e-Privacy Directive.

49 Article 5 e-Privacy Directive.

50 Articles 6-9 e-Privacy Directive.

51 See also: Working Party 29, Opinion 1/2008 on data protection issues related to search engines, WP 148, 04 April 2008.

52 Google Spain, para. 33.

53 Court of Justice, Google France SARL, Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA, Luteciel SARL (C-237/08), and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08), cases C-236/08, C-237/08 and C-238/08, 23 March 2010, para. 120.

54 See also: Working Party 29, Opinion 5/2009 on online social networking, WP 163, 12 June 2009.

55 Working Party 29, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 February 2010, p. 25.

56 Article 3 Data Protection Directive.

57 Court of Justice, Sweden v. Bodil Lindqvist, case C-101/01, 06 November 2003, para. 47.

that can only be accessed with a password or to private profiles on social media that have a limited number of users. The exact boundary between public and private (e.g. in number of users) must be determined on a case-by-case basis. It is important to underline that Internet intermediaries cannot invoke the exception themselves because they are not natural persons.

22 Second, there is an exemption if personal data are processed solely for journalistic purposes.[58] In the Satamedia case, the ECJ stated that this exception does not only apply to media undertakings, but to all those engaged in journalism. The fact that processing is linked to a commercial business model does not mean that it is not an activity solely for journalistic purposes. According to the ECJ, each company after all, engages in undertakings for profit; commercial success may even be the sine qua non for the survival of professional journalism. Furthermore, the means by or the media-type through which the data is transmitted, whether they are conventional carriers such as paper or newer phenomena such as digits, as are used on the Internet, is of no importance. According to the Court, the concept of "journalism'" must be interpreted broadly too, so that non-traditional media companies may also rely on it.[59] This interpretation seems to pave the way for an interpretation under which modern media and active Internet intermediaries using User Generated Content, amateur journalists and bloggers may also invoke the journalistic exception.

23 In the recent Google Spain case, however, a much narrower interpretation was adopted. Although under the interpretation of the ECtHR, Internet intermediaries may also rely on the freedom of expression as protected by the ECHR, the ECJ seems far more hesitant. "Furthermore, the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' and thus benefit [] from derogations from the requirements laid down by the directive, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine."[60] It therefore follows that active Internet intermediaries usually have to be considered as the controller of personal data, but in principle cannot invoke the journalistic exception if they are not the editor of the published news story. This constellation, in which the intermediary is a "controller" and in which it cannot invoke an exception, implies that the Internet intermediary must fulfill all obligations under the Directive, such as maintaining transparency, security, confidentiality and the legitimacy of processing personal data.[61]

24 For example, the Internet intermediary needs a legitimate ground for processing personal data. If the information processed concerns data provided by a user about another person (which will often be the case), then the only possible legitimation ground is weighing the interests of the intermediary against the interests of the data subject. This balance will have to be made on a case-by-case basis, but in practice, the fundamental rights and freedoms of the data subject will often prevail.[62] Intermediaries also have to uphold other duties enshrined in the Data Protection Directive, such as the data minimization principle, which specifies that data may only be processed if they are necessary for and proportionate to a clear and specified purpose, that they cannot be further processed for another purpose, that they should be deleted when they are no longer necessary and anonymized when possible.[63] In addition, the directive specifies the right of the data subject to rectification, to have data removed or to oppose, in certain cases, further processing of those data.[64] These duties were initially applied on Internet intermediaries only very cautiously. However, in the case law of the ECJ, a far more extensive interpretation is adopted. Search engines are full-fledged "controllers", according to the court, and consequently they must fulfill all requirements and obligations specified in the Data Protection Directive. Obviously, if this holds true for search engines, there seems to be no reason why this would not also count for (other) active Internet intermediaries.

25 In general, there is a trend towards additional and stronger rights for data subjects and greater and broader obligations for data controllers in data protection law. This appears inter alia from the pending General Data Protection Regulation, which in time will replace the Directive from 1995. It contains numerous new rights such as the right to be forgotten,[65] the right to data portability,[66] which entitles data subjects to transfer their profiles from one to another social network, and the right to resist profiling.[67] The proposed regulation also contains very far-reaching obligations for controllers, such

58 Article 9 Data Protection Directive.

59 Satamedia, paras. 53-62.

60 Google Spain, para. 85.

61 See Articles 16 and 17 Data Protection Directive.

62 Article 7 sub f Data Protection Directive. See also: Google Spain. See further: Working Party 29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 09 April 2014.

63 Article 6 Data Protection Directive.

64 Articles 12, 14 and 15 Data Protection Directive.

65 Article 17 General Data Protection Regulation (Commission Proposal).

66 Article 18 General Data Protection Regulation (Commission Proposal).

67 Article 20 General Data Protection Regulation (Commission Proposal).

as the requirement to keep detailed records,[68] to undertake risk assessments[69] and to appoint an internal privacy auditor.[70] Finally, very high penalties are proposed when controllers do not abide by the rules contained in the Regulation, which amount up to 2% of worldwide annual revenue of a company.[71] This can have very serious consequences for the liability and responsibility of active Internet intermediaries. At the time of writing, however, it is still unclear if and when this regulation will be adopted and in what form.

D. Freedom of expression

26 Finally, Internet intermediaries may also rely on fundamental rights themselves. As discussed earlier, many providers do not want to supply personal data of their users to third parties or monitor the communications running through their networks. They may refuse to do so in order to protect the interests of their users, but they may also want to protect their own interests: legal persons may also invoke the right to privacy[72] and data protection to protect their own interests.[73] Alternatively, providers can rely on the freedom of expression, again either directly or indirectly, to protect their own interests or those of their users. Article 10 of the European Convention on Human Rights holds in paragraph 1: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.' Already in the case of Handyside v. UK from 1976, the ECtHR adopted a broad interpretation of this right, linking it to the protection of an open and vital democracy. 'Freedom of expression constitutes one of the essential foundations of such a society, one of the basic conditions for its progress and for the development of every man. Subject to paragraph 2 of Article 10, it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'."[74] In later judgments, the ECtHR not only adopted a broad interpretation of the freedom of speech itself, but also of those that may rely on Article 10 ECHR.[75]

27 The fact that Internet intermediaries are one of the parties that may invoke Article 10 ECtHR has recently been confirmed by the ECtHR in the case of Delfi v. Estonia, in which a news site published a critical article about a company that provided ferry services and about L., the sole shareholder. The article itself was nuanced and balanced, the comments of the users posted under the article, however, were less refined. When L. asked the website to remove 20 of these comments and to pay damages, the site removed the comments, but refused to do the latter. In the legal proceedings that followed, the question was posed to which extent the website was responsible for the user comments. A lengthy juridical procedure followed on the national level, in which the website was sometimes treated as an Internet intermediary under the rules of (the implementation of) the e-Commerce Directive and sometimes as a journalistic news medium under the doctrine of freedom of expression, because the site was considered too active to qualify as a passive Internet intermediary. Both in the national proceedings and before the ECtHR, the latter vision ultimately prevailed and the website was treated under Article 10 ECHR and not under the e-Commerce Directive.

28 The argument of the Estonian government before the ECtHR on this point is interesting, as is the rejection of it by the ECtHR: "The Government pointed out that according to the applicant company it had been neither the author nor the discloser of the defamatory comments. The Government noted that if the Court shared that view, the application was incompatible ratione materiae with the provisions of the Convention, as the Convention did not protect the freedom of expression of a person who was neither the author nor the discloser. The applicant company could not claim to be a victim of a violation of the freedom of expression of persons whose comments had been deleted. (...) The Court notes that the applicant company was sued for defamation in respect of comments posted on its Internet portal, it was deemed to be discloser (...)

68 Article 28 General Data Protection Regulation (Commission Proposal).

69 Article 33 General Data Protection Regulation (Commission Proposal).

70 Article 35 General Data Protection Regulation (Commission Proposal).

71 Article 79 General Data Protection Regulation (Commission Proposal).

72 See also: European Court of Human Rights, Colas e.a. v. France, case 37971/97, 16 April 2002.

73 See further: B. van der Sloot, 'Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system', Computer Law & Security Review, 2015-1, p. 26-45. See also the national implementations of the Data Protection Directive, such as that of Austria, and the goals of the e-Privacy Directive.

74 European Court of Human Rights, Handyside v. the United Kingdom, apll.no. 5493/72, 07 December 1976, para 49.

75 See also: http://www.echr.coe.int/Documents/Research_report_Internet_ENG.pdf.

of the comments – along with their authors – and held liable for its failure to prevent the disclosure of or remove on its own initiative the unlawful comments."[76] From this, the ECtHR concluded that the provider was curtailed in its right to freedom of expression. This was confirmed on 16 June 2015 by the Grand Chamber.[77]

29 Consequently, the ECtHR adopts a broad interpretation of the freedom of expression. Parties that remain relatively passive can also invoke Article 10 ECHR, though parties that have no involvement whatsoever, such as purely passive providers, will normally not be able to invoke this right.[78] Some activity or control is necessary; the exact interpretation will depend on the circumstances of the case. In this connection, a comparison can be made with the position of the "controller" under data protection law, although that position primarily entails duties and this one also entails numerous rights and privileges. Although Internet intermediaries, can, under certain conditions, invoke the freedom of expression, this right may be curtailed if the conditions under paragraph 2 of Article 10 of the Convention apply: "The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

30 It should be noted that Article 8 of the ECHR (right to privacy) is based on Article 12 of the Universal Declaration of Human Rights (UDHR), which states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[79] Although almost all elements of this provision are incorporated in 8 ECHR, the protection of honor and reputation is not. Article 8 ECHR, paragraph 1: "Everyone has the right to respect for his private and family life, his home and his correspondence." The protection of honour and reputation is moved to paragraph 2 of Article 10 ECHR, so that it is not a subjective right which natural persons can invoke, but one based on the grounds on which a state may legitimately curtail the right to freedom of expression.[80] Although the ECtHR has respected this choice of the drafters of the Convention for a long time; since 2007 it has abandoned this line and argued that individuals may, under certain conditions, also invoke a subjective right to the protection of their honor and reputation under Article 8 ECHR.[81] It should also be borne in mind that in general, Article 8 ECHR has been given a very wide scope by the court, which among other things entails that issues surrounding the protection of property and the dissemination of child pornography or similar material (matters that fall under the e-Commerce Directive, rather than the Data Protection Directive in EU law) are also (partially) protected under the right to privacy, under the European Convention on Human Rights of the Council of Europe.[82] Moreover, the right to data protection is also (partially) protected under the scope of Article 8 ECHR.

31 Consequently, in cases like Delfi v. Estonia, two fundamental rights clash. On the one hand the freedom of expression of Internet intermediaries and its users, and on the other hand the right to privacy of third parties. These fundamental rights must be seen as equivalent interests. Consequently, they must be weighed and balanced against each other.[83] "The Court has considered that where the right to freedom of expression is being balanced against the right to respect for private life, the relevant criteria in the balancing exercise include the following elements: contribution to a debate of general interest, how well known the person concerned is, the subject of the report, the prior conduct of the person concerned, the method of obtaining the information and its veracity, the content, form and consequences of the publication, and the severity of the sanction imposed."[84] Both

76 Delfi v. Estonia (normal chamber), paras. 48 and 50.

77 European Court of Human Rights (Grand Chamber), Delfi/Estonia, appl.no. 64569/09, 16 June 2015.

78 See further: E. Barendt, 'Freedom of Speech', Oxford, Oxford University Press, 2005.

79 See further: UN Documents: A/C.3/SR.119.

80 See in general: http://www.echr.coe.int/library/DIGDOC/Travaux/ECHRTravaux-ART8-CDH(67)5-BIL1338891.pdf.

81 See further: European Court of Human Rights, Chauvy e.a. v. France, appl.no. 64915/01, 29 June 2004. European Court of Human Rights, Pfeifer v. Austria, appl.no. 12556/03, 15 November 2007. European Court of Human Rights, Torres and Polanco v. Spain, appl.no. 34147/06, 21 September 2010. European Court of Human Rights, A. v. Norway, appl.no. 28070/06, 09 April 2009.

82 See among others: European Court of Human Rights, K.U. v. Finland, appl.no. 2872/02, 02 December 2008.

83 European Court of Human Rights, Associes v. France, appl. no. 71111/01, 14 June 2007. European Court of Human Rights, MGN Limited/UK, appl.no. 39401/04, 12 June 2012. European Court of Human Rights, Timciuc/Romania, appl.no. 28999/03, 12 October 2010. European Court of Human Rights, Mosley/UK, appl.no. 48009/08, 10 May 2011.

84 Delfi/Estonia, para. 83. See further: European Court of Human Rights, Springer v. Germany, appl.no. 39954/08, 07 February 2012. European Court of Human Rights, Von Hannover v. Germany (2), appl.nos. 40660/08 and 60641/08, 07 February 2012.

the Chamber and the Grand Chamber of the ECtHR concluded in Delfi v. Estonia that the limitation on the freedom of expression of Delfi by the conviction of the Estonian Supreme Court did not violate Article 10 ECHR.

32 In particular, the ECtHR felt that the measures taken by Delfi were insufficient, i.e. the terms and conditions which prohibited defamatory comments, the notice and takedown system, the monitoring activities and the automatic filter system it employed. Although these measures go beyond what is necessary for the duty of care under Article 14 e-Commerce Directive, they are apparently insufficient when it comes to the duty of care under Article 10 ECHR. A salient detail is that the Court ruled that it was legitimate to hold Delfi liable, while not even trying to press charges against the actual authors of the comments, because Delfi allowed them to post comments anonymously. "It notes that it was the applicant company's choice to allow comments by non-registered users, and that by doing so it must be considered to have assumed a certain responsibility for these comments."[85] This is remarkable because the ECtHR also agrees that the ability to post comments in full anonymity is an important part of both the right to privacy, the right to data protection and the right to freedom of expression; while the efforts to that end by Delfi show that in fact there runs a higher risk of being held liable for the comments of users than if it would not have allowed anonymous comments.

33 Finally, it should be noted that journalists and journalistic media enjoy enhanced protection under the regime of freedom of expression, in part because their role as "public watchdog" is deemed necessary in a democratic society.[86] Journalists also enjoy additional protection of their sources,[87] a larger freedom to engage in newsgathering and a greater protection with respect to publishing classified information,[88] including a limitation of their liability.[89] However, not everyone can invoke the status of journalist; only those who write newsworthy stories and abide by the journalistic principles.[90] With this respect, the ECtHR has chosen to adopt a functional instead of an institutional approach, which means that it does not (only) look at whether a person or company is an established journalist or an established journalistic medium,[91] but rather assesses whether a person or organization contributes to the public debate, engages in journalistic research, observes the journalistic standards, produces newsworthy stories on a more or less regular basis, etc.[92]

34 The European Court of Human Rights has recognized that the Internet-related services of a media enterprise may fall under the scope of Article 10 ECHR: "In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10."[93] To what extent this principle also applies to online platforms, news sites using UGC and amateur bloggers is unclear. Yet it seems that there are no fundamental objections or obstacles for them to rely on these principles. Consequently, sites like Delfi could rely on the journalistic position for the part of their activities that relate to journalism; for example, the story written by one of its employees, which condemned the defamatory user comments and triggered the court case.

35 This line also seems to follow from the recommendation of the Committee of Ministers of the Council of Europe regarding a "New Notion of Media" from 2011,[94] in which it suggests that even amateur bloggers can rely on the extra protection of journalists if they meet the conditions and

85 Delfi/Estland, para. 91.

86 European Court of Human Rights, Barthold/Germany, appl. no. 8734/79, 25 March 1985.

87 See for example: European Court of Human Rights, Financial Times Ltd. e.a. v. United Kingdom, appl.no. 821/03, 15 December 2009. European Court of Human Rights, Ressiot e.a. v. France, appl.nos. 15054/07 and 15066/07, 28 June 2012.

88 See among others: European Court of Human Rights, Stoll v. Switzerland, appl.no. 69698/01, 10 December 2007.

89 See among others: European Court of Human Rights, Fressoz and Roire v. France, appl.no. 29183/95, 21 January 1999.

90 Stoll/Switzerland.

91 European Court of Human Rights, Steel and Morris v. the United Kingdom, appl.no. 68416/01, 15 February 2005. European Court of Human Rights, Társaság a Szabadságjogokér v. Hungary, appl.no. 37374/05, 14 April 2009.

92 See also: http://www.ivir.nl/publications/helberger/Making_User_Created_News_Work.pdf.

93 European Court of Human Rights, Times Newspaper LTD(1 and 2)/UK. See also: European Court of Human Rights, Mosely v. UK. Again, this seems to create a tension between the approach of the ECtHR and that of the ECJ in its Google Spain decision, namely in connection to the use and protection of archives and archival functions. See also the case Wegrynowski and Smolczewski v. Poland, in which the ECtHR explicitly stated: 'The Court accepts that it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations. Furthermore, it is relevant for the assessment of the case that the legitimate interest of the public in access to the public Internet archives of the press is protected under Article 10 of the Convention.' European Court of Human Rights, Wegrynowski and Smolczewski/Poland, appl.no 33846/07, 16 July 2013, para. 65.

94 Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media.

journalistic standards. "As regards in particular new media, codes of conduct or ethical standards for bloggers have already been accepted by at least part of the online journalism community. Nonetheless, bloggers should only be considered media if they fulfil the criteria to a sufficient degree."[95] It should be noted that in order to rely on the regime for journalists under the freedom of expression, actors should abide by a number of additional duties of care and principles. Consequently, if Internet intermediaries want to rely on this position, they should abandon their traditional passivity even further.

E. Conclusion

36 The e-Commerce Directive was adopted at the beginning of this millennium to harmonize the various national approaches to the liability of Internet intermediaries for wrongful acts conducted by their users through their networks. The fear was that the existing diversity at that time would lead to legal inequality and uncertainty, which could hamper the digital economy. It was decided to exclude passive Internet intermediaries, under certain conditions, from liability for actions conducted by their users. Although this regime is still ensured for these traditional Internet providers, a number of factors have complicated this system.[96]

37 First, providers have become increasingly active, for example by indexing information and making it searchable, by creating social platforms and by creating sites which are based on User Generated Content. The question is whether they can also rely on the safe harbors for liability specified in the e-Commerce Directive. The ECJ seems to allow active Internet intermediaries to invoke these safe harbors to a relatively large extent, on the condition that these providers assume additional duties of care. This may create a Catch-22 situation. Providers that are more active have more control over the content they distribute and are thus supposed to have greater duties of care, but these duties of care imply that the Internet intermediaries gain even further control over the content. This might mean that they must adopt even further standards of care and exercise even greater control.

38 Secondly, the e-Commerce regime does not apply to issues falling under the data protection regime. For passive Internet intermediaries, the two regimes are more or less comparable. Under the Data Protection Directive, passive actors are in principle exempt from responsibilities and duties of care. For active intermediaries, however, the data protection regime is substantially different from the e-Commerce regime. The Data Protection Directive imposes many duties on active Internet intermediaries and this burden will only be intensified when the General Data Protection Regulation is adopted. Active Internet intermediaries can rely on the exclusion of liability under the e-Commerce regime much more quickly than under the data protection regime.

39 Thirdly, Internet intermediaries increasingly rely on fundamental rights themselves, to protect their own interests or those of their users. One example that has not even been discussed in this paper is the freedom to conduct a business, as enshrined in Article 16 of the EU Charter of Fundamental Rights. What has been discussed is that Internet intermediaries may rely on data protection law to protect their own data or those of its users. Internet intermediaries are sometimes asked to provide information about users (that are suspected to have carried out unlawful activities via their networks) to third party right holders (often of intellectual property), to monitor their networks and to detect or block infringing activities. Internet intermediaries often find themselves in a difficult position, having to judge the legitimacy of the claims and having to balance the rights of two different parties. As in Europe, in contrast to the DMCA in America, no legislative framework exists for the handling of such requests and these decisions are often made before a case is judged by a court of law; thus, Internet providers often have to make an assessment of the case independently and assume the role of a judge.

40 Providers additionally rely on the freedom of expression. This may be an indirect claim in order to protect the freedom of expression of users of a platform against filter obligations or against obligations to remove certain messages, information or files. More importantly, providers can also rely on the freedom of expression themselves, for the protection of their own interests, even if they are considered responsible for illegitimate actions of the users of their services through their network. This predominantly applies to active Internet intermediaries, as purely passive providers that provide storage space for third parties and mere conduits will usually not qualify as a publisher or an initiating party in the publication, distribution or gathering of information. If an active Internet intermediary successfully invokes the freedom of expression, then it is this right that should be balanced and weighed against the rights of the third party, such as his copyright. To further complicate matters, what has remained undiscussed in this

95 CM/Rec(2011)7, nr. 41-42.

96 See further: T. Synodinou, "Intermediaries' liability for online copyright infringement in the EU: evolutions and confusions',Computer Law & Security Review, Vol. 31 No. 1, 2015. P. van Eecke, 'Online service providers and liability: a plea for a balanced approach', Common Market Law Review, Vol. 48 No. 5, 2011.

contribution are third parties' rights to freedom of expression or the freedom of enterprise, for which being findable in search engines like Google may be pivotal. Moreover, third parties' claims may also revolve around privacy and data protection interests. This can also be invoked against the freedom of expression of the provider.

41 It should be stressed that in most freedom of expression regimes around the globe, a special position is reserved for journalists. Traditionally, they have more rights, wider freedoms and enjoy greater protection from liability. It seems that there are no obstacles for Internet intermediaries such as news sites that use UGC to claim such a position as well, provided that they comply with the additional safeguards and obligations that go with being a journalist. It should be remembered that in order to obtain the "status" of a journalist, the provider's passivity is put under pressure to an even greater extent. Consequently, there is a certain tension between the different regimes. The most striking consequence is perhaps that providers are encouraged to either remain fully passive (and therefore have no form of control over their services), in order to qualify for the exemption from liability under the e-Commerce and the data protection regime, or to abandon their passivity almost fully (and gain a very large form of control over the actions of their users), in order to rely on the freedom of speech and possibly even to qualify for the position of a journalistic medium.[97]

42 It follows that Internet intermediaries can rely on a variety of different positions and regimes. Each of the three regimes discussed here (the e-Commerce Directive, the Data Protection Directive and the freedom of expression contained in the ECHR) has roughly three positions.

43 Under the e-Commerce Directive:

- (1) The passive provider is normally excluded from liability if it complies with the requirements specified in the Directive.
- (2) Active providers that adopt additional measures and safeguards can also rely on the exclusion of liability.
- (3) There are providers that are so active that they simply do not qualify as an Internet intermediary; for example publishers of news-sites with respect to the stories written by their own employees and posted on their own website.

44 Under the Data Protection Directive:

- (1) The data processor who acts under the authority of the data controller has to take into account the limited safeguards specified in the e-Privacy Directive only.
- (2) Active Internet intermediaries that, for example, determine the technical infrastructure (and thus the means of processing) of a website, but depend primarily on the users of the site for the content and the material, have a shared responsibility with the users.
- (3) The Internet intermediaries that are so active that they are solely responsible for the data processing must comply with all the obligations contained in the Data Protection Directive, and in the future the General Data Protection Regulation.

45 Under the doctrine of freedom of expression:

- (1) Providers that are so passive that they cannot rely on this regime because they do not share, gather or publish any information themselves.
- (2) Active Internet intermediaries that can invoke the freedom of expression.
- (3) Providers who comply with additional safeguards and obligations may rely on the privileged status of journalist.

46 Not only does each position entail different rights and obligations, but different conditions apply to the positions as well. For example, the freedom of expression of a provider may be limited, even if it has taken measures that would be sufficient in relation to the intensified duty of care for active providers under the e-Commerce Directive. Moreover, providers will more quickly be able to rely on the exclusion of liability under the e-Commerce Directive, possibly by fulfilling additional duties of care, than to invoke the position of processor under the Data Protection Directive. Active providers have many duties and obligations under the Data Protection Directive, while they have many freedoms and privileges under the freedom of expression. It should also be noted that the regimes of the European Union, including that of the e-Commerce Directive and the Data Protection Directive, and the instruments of the Council of Europe, including the ECHR, deviate on a number of points. This is reinforced by Article 8 ECHR, which also provides partial protection to private property and against criminal acts, while these matters are treated under the e-Commerce Directive rather than the Data Protection Directive

97 See also: G. González Fuster, 'Balancing intellectual property against data protection: a new right's wavering weight', IDP: Revista de Internet, Derecho y Política, No. 14, 2012. M. Husovec, 'Injunctions against innocent third parties: case of website blocking', Journal of Intellectual Property, Information Technology and Electronic Commerce Law, Vol. 4 No. 2, 2013.

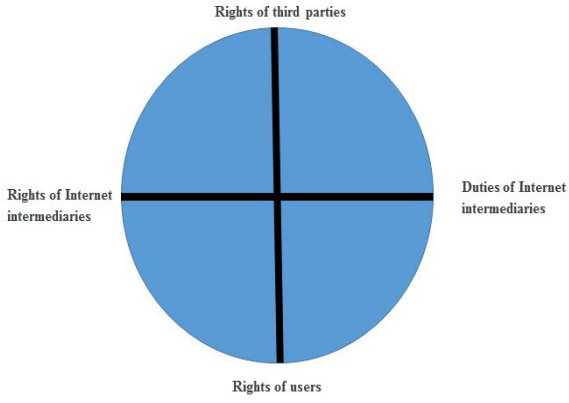
in EU law. Article 8 ECHR also covers rules on data protection, but this right is treated and explained in substantially different terms by the ECtHR than by the ECJ.[98]

47 In conclusion, while the e-Commerce Directive was installed to clarify the position of and to provide greater legal certainty to providers (given the great diversity in national rules that existed before the entry into force of the Directive), it should be acknowledged that the current situation in Europe regarding the liability of Internet intermediaries is still very diffuse and unclear. Consequently, despite the rules contained in the Directive, countries in Europe have a very different take on many of the complex questions and positions. Courts and judges will often have a very wide margin of appreciation and thus a responsibility for weighing and balancing the different interests and positions involved, while there are usually very few cases that make it to the national supreme courts, let alone the European courts. Most cases are dealt with by lower courts and the case law is often contradictory. Additionally, Internet intermediaries themselves have an important role regarding balancing the various interests and circumstances of the case and this creates an even more diffuse picture, because of the different attitudes and approaches by the various providers.[99]

48 The solution should therefore be twofold. First, a system could be implemented in which not the Internet intermediary, but a court will assess requests from third parties. This would ensure that it is not the Internet intermediary that is primarily responsible for the initial evaluation of the case, but a judge. This would simply require a rule specifying that all requests from third party rights holders should be judged by a court of law. Secondly, judges would be helped by a simplification of the rules and a harmonization of the different regimes. This requires installing one regime for determining the liability of Internet providers in Europe. Moreover, there should be clarity about the parameters that judges must take into account when establishing the liability of Internet intermediaries. Such a system would need to be adequately clear to avoid legal uncertainty, but should also allow for sufficient flexibility in order to effectively respond to new technological developments.

49 One option would be to opt for a system that does not depend on fixed positions of Internet intermediaries, with corresponding duties and freedoms, but on a more graduated approach. Specifying the exact details of such a system lies beyond the scope of this article, but with some simplification, two axes could be distinguished. The first axis contains the rights of the user in relation to the rights of third parties - they should always be balanced and weighed against each other. If a third party submits a poorly substantiated claim or provides only marginal evidence, the user's interests will usually prevail. If, however, the behavior of the user is clearly illegal and substantially harms the interests of third parties, the opposite would hold true. The second axis concerns the rights and freedoms of the Internet intermediary on the one hand and its duties and responsibilities on the other. These two sides must also be weighed and balanced by a court. Perhaps it would be advisable to choose a form of sectoral co-regulation, such as Article 27 of the Data Protection Directive, which explicitly encourages codes of conduct. For now, however, the liability regime for Internet intermediaries in Europe remains a jumble of different positions, regimes, rights, duties and exemptions. It is to be expected that for the time being, no substantial changes will be made. Welcome to the world of Internet liability, welcome to the jungle.

50 The liability of Internet intermediaries:



51 Some questions remain to be answered regarding this approach however, such as who should develop the concrete rules, what are the limits thereof, who should create or clarify the framework that judges should endeavour to apply, should they do it themselves, etc.? As mentioned, the American Digital Millennium Copyright Act might provide some leads for this alternative approach. For this reason, a brief description of this Act is given below. The DMCA specifies that a service provider shall not be liable for monetary relief, or for injunctive or other equitable

98 P. de Hert & S. Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action', in: S. Gutwirth, Y. Poullet, P. de Hert, J. Nouwt en C. De Terwangne (eds), 'Reinventing data protection?', Dordrecht, Springer Science, 2009.

99 See further: S. de Vries, 'Balancing fundamental rights with economic freedoms according to the European Court of Justice', Utrecht Law Review, Vol. 9 No. 1, 2013. L. Edwards, 'The fall and rise of intermediary liability online' In: L. Edwards, L. and C. Waelde (eds.), Law and the Internet, Hart Publishing, Oxford, 2009.

relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider does not have actual knowledge that the material or an activity using the material on the system or network is infringing, in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent, or upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material. A further condition is that the provider does not receive a financial benefit directly attributable to the infringing activity, in the case in which the service provider has the right and ability to control such activity. A final condition is that upon notification of claimed infringement, the provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity. This resembles the e-Commerce regime to a large extent.[100]

52 However, the rules regarding the notice and takedown regime are specified in further detail.[101] The DMCA specifies that the service provider should have a designated agent to receive notifications of claimed infringement, by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, the name, address, phone number, and electronic mail address of the agent and other contact information which the Register of Copyrights may deem appropriate. The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.[102]

53 The DMCA continues by specifying the elements of the notification. A notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes, first, a physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. Second, identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site. Third, identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material. Fourth, information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complainant may be contacted. Fifth, a statement that the complaining party has a good reason to believe that use of the material under scrutiny is not authorized by the copyright owner, its agent, or the law. Sixth and finally, a statement that the information in the notification is accurate, and under penalty of perjury, that the complainant is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.103

54 The DMCA explicitly states that if the copyright owner fails to comply with these provisions, the notification to the provider shall not be considered in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent. If there are minor flaws in the notification, this rule only applies if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions and requirements. Furthermore, the DMCA contains an explicit clause on misrepresentation. It holds that any person who knowingly materially misrepresents that material or activity is infringing,

100 See for comparison with EU regulation: M. Peguera, "The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems." Columbia Journal of Law & the Arts 32, 481, 2009. V. McEvedy, "The DMCA and the Ecommerce Directive." EIPR 24.2, 2002.

101 In the USA, the Communications Decency Act is also of relevance: J. Band and M. Schruers, 'Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act', Cardozo Arts & Ent. LJ 20, 295, 2002.

102 See for comments on specific cases: M. Driscoll, 'Will YouTube Sail into the DMCA's Safe Harbor or Sink for Internet Piracy', J. Marshall Rev. Intell. Prop. L. 6, 2006. T. A. Dutcher, 'Discussion of the Mechanics of the DMCA Safe Harbors and Subpoena Power, as Applied in RIAA v. Verizon Internet Services', Santa Clara Computer & High Tech. LJ 21, 493, 2004. A. Kao, 'RIAA v. Verizon: Applying the Subpoena Provision of the DMCA', Berkeley Tech. LJ 19, 405, 2004. E. C. Kim, 'YouTube: Testing the safe harbors of digital copyright law', S. Cal. Interdisc. LJ 17,139, 2007. B. White, 'Viacom v. YouTube: A Proving Ground for DMCA Safe Harbors Against Secondary Liability', John's J. Legal Comment, 24, 811, 2009.

103 See for an explanation and further discussion: L. Chang, 'Red Flag Test for Apparent Knowledge under the DMCA Sec. 512 (C) Safe Harbor', Cardozo Arts & Ent. LJ 28, 195, 2010. E. Lee, 'Decoding the DMCA safe harbors', Columbia Journal of Law & the Arts, Forthcoming, 2009. Mark A. Lemley, Mark, 'Rationalizing Internet Safe Harbors', Journal of Telecommunications and High Technology Law 6, 101, 2007. C. E. Mammen, 'File Sharing is Dead-Long Live File Sharing-Recent Developments in the Law of Secondary Liability for Copyright Infringement', Hastings Comm. & Ent. LJ 33, 443, 2010. J. M. Miller, 'Fair Use through the Lenz of Section 512 (c) of the DMCA: A Preemptive Defense to a Premature Remedy', Iowa L. Rev. 95, 1697, 2009. M. Piatek, T. Kohno and A. Krishnamurthy, 'Challenges and directions for monitoring P2P file sharing networks, or, why my printer received a DMCA takedown notice', HotSec, 2008.

or that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is ill-treated by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

55 The Act also provides rules on the replacement of removed material.[104] The DMCA specifies that a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing. This rule, however, shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice, unless the service provider, first, takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material. second, upon receipt of a counter notification, promptly provides the person who provided the notification with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and third, replaces the removed material and ceases disabling access to it not less than 10, nor more than 14 business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.[105]

56 Finally, the DMCA specifies the contents of counter notification. A counter notification must be a written communication administered to the service provider's designated agent that includes, first, a physical or electronic signature of the subscriber; second, identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled; third, a statement under penalty of perjury that the subscriber has a good reason to believe that the material was removed or disabled due to a mistake or misidentification of the material to be removed or disabled; fourth and finally, the subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification or an agent of such person.[106]

57 Thus, the advantage of the DMCA over the e-Commerce Directive is that it specifies in further detail what the obligations and rights of the different parties are. The Act describes who should issue the notification on a copyright infringement, to whom, and what information the notification should contain. Importantly, it states that if the notification is not issued in a correct manner, it shall not be considered when establishing the question of whether the Internet intermediary had knowledge of the copyright infringement. Therefore, the burden is placed on the copyright owner, not on the Internet intermediary. More importantly, the DMCA explicitly lays down sanctions for those that purposely misrepresent the truth. Thus, if a person misrepresents himself as a copyright owner or if a copyright owner notifies an Internet intermediary that his copyright has been infringed while he knows or should know that this is not the case, the costs are for that person to bear, not for the Internet intermediary. Furthermore, the third party (usually the user of the Internet provider's service) has an explicitly recognized role in the DMCA. It can issue a counter notification and argue that its use of the alleged infringing material is actually legitimate. Again, the Act specifies in detail how the counter

104 However, there is also critique on the working of the DMCA: W. Seltzer, 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment', Harv. JL & Tech. 24, 171, 2010. J. Bretan, 'Harboring Doubts about the Efficacy of 512 Immunity under the DMCA', Berkeley Tech. LJ 18, 43, 2003. J. Cobia, 'Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process', Minn. JL Sci. & Tech. 10, 387, 2008. G. Jansen, 'Whose Burden Is It Anyway: Addressing the Needs of Content Owners in DMCA Safe Harbors', Fed. Comm. LJ 62,153, 2010.

105 See in further detail: D. Weinstein, 'Defining Expeditious: Uncharted Territory of the DMCA Safe Harbor Provision-A Survey of What We Know and Do Not Know about the Expeditiousness of Service Provider Responses to Takedown Notifications', Cardozo Arts & Ent. LJ 26, 589, 2008.

106 See for an application of the DMCA on new developments: B. Brown, 'Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World', Berkeley Tech. LJ 23, 437, 2008. J. J. Darrow and G. Ferrera, 'Social networking web sites and the DMCA: a safe-harbor from copyright infringement liability or the perfect storm?', Northwestern Journal of Technology & Intellectual Property 6.1, 2007. M. S. Sawyer, 'Filters, fair use & feedback: user-generated content principles and the DMCA', Berkeley Tech. LJ 24, 363, 2009. C. W. Walker, 'Application of the DMCA safe harbor provisions to search engines', Va. JL & Tech, 9, 1, 2004.

notification should be issued. The DMCA gives a clear time path for the Internet provider, when to remove the content, when to notify the user of the copyright infringement notification, when to notify the copyright owner of a counter notification, when the content should be restored, and when the matter must be resolved by a judge. Consequently, if the Internet provider follows the clear and detailed instructions and the time path, it runs no risk of being held liable for any damages - either at the side of the copyright owner or at the side of the user.

58 There is no reason why this model should not be applied to privacy infringements in Europe as well. It would help to shed a light on the dark jungle that is the Internet intermediary liability regime in Europe right now. One addition would be important, namely that the Internet provider is at liberty to overrule either the complainant's or the defendant's claim or counter-claim on its own initiative to protect its own direct or indirect interests. This of course would be at its own discretion. If a provider would overrule a notification or counter-notification on its own initiative for no apparent reason, then it would be liable for the damages following from that action. If it did so mistakenly, but in good faith, a judge might overrule him in a legal procedure. Consequently, both the claimant and the defendant would also have the right to go to a court in case an Internet provider overrules their notification or counter-notification.

59 So let's suppose the situation in which a news portal is partly based on User Generated Content and partly on content produced by employees. The portal publishes a news item, written by one of its employees on a politician that might have been paid by a company to vote against a certain Bill. The site allows users to change or elaborate on the story; one user does and reveals that the politician had an extra-marital affair with the daughter of the CEO of the same company, making him vulnerable for blackmail. He does not cite a public source, but confidentially reveals to the Internet provider that he has contact with the daughter of the CEO and heard the story from her first hand. The Internet provider is not in any position to check this claim. The politician decides to complain to the news portal and to request the removal of the unsupported claim that he has or had an extramarital affair and has been or could have been blackmailed. It is up to the Internet provider to make a decision.

60 Under the current regime, the Internet provider is under a twofold burden. On the one hand, it has the leading role in establishing the facts and the actions taken thereupon. First, it has to assess the reliability and the veracity of the complaint by the politician. Second, it has to assess the reliability of the story of the user. Third, even if it is true, it has to balance the infringement of the politician's privacy against the public interest in knowing the facts disclosed. Fourth, there is no or only limited room for the Internet provider to take into account its own interests (either in being a trustful website not making false or unsubstantiated claims or in being a leading website bringing breaking news and scoops) and those of its readers. On the other hand, it might even be sued by either the politician or the user if it makes a wrongful decision and a judge might, as evidenced by Delfi v. Estonia, be held to pay a fine or damages. A judge might impose even further obligations on the provider, without being clear on how the obligations should be implemented or weighed with the other interests at stake.

61 The alternative approach would ameliorate this situation in two ways. On the one hand, it gives a clear indication regarding what information the notification by the politician should contain, that the provider should take down the alleged infringing information and that it should notify the user of the takedown. If the user subsequently argues that the story was indeed true and legitimate, the provider has to inform the politician thereof and restore the content. If the parties still disagree, the matter shall be resolved by a court of law. If the Internet provider follows this procedure, it cannot be held liable for damages either by the politician or by the user. In addition, this system has the benefit as it allows the Internet intermediary to take into account its own direct or indirect interests. For example, even though the user might claim that he is sure that the story is true and legitimate, the provider still runs the risk that a judge will rule otherwise. This would presumably not be a problem for a gossip magazine, but for a quality news portal this might be problematic because it undermines the name of the newspaper. Similarly, a quality news portal could, for example, have the policy of only publishing stories on the public lives of public figures, not about their private lives and so decide to reject the story by the user to protect the integrity and corporate identity. This decision could be challenged by the user, for example arguing that the private life of the politician had an effect on his profession.

62 On the other hand, the judge would have a clearer decision tree to arrive at his or her conclusion. Of course, the judge has to determine the truthfulness of the story. Presuming the court would hold the story to be true, it would then not only balance the freedom of speech of the user against the right to privacy/reputation of the politician, but also the interests of the Internet intermediary and of its users. Moreover, it would take into account the steps taken by the Internet provider to prevent or minimize damage to the politician, for example, by letting an employee verify the story written by the user. The court would then consider all these values and interests and weigh and balance them against

each other. This would not only make it easier for the court to arrive at its decision, it would also become clearer for the parties involved how the court arrived at its decision, which interests were taken into account and how they were balanced and weighed against each other.

* Bart van der Sloot is a researcher at the Institute for Information Law, University of Amsterdam, the Netherlands. This article contains revised and updated parts of an article that has appeared in Dutch. B. van der Sloot, 'Welcome to the jungle: de aansprakelijkheid van internet-intermediairs voor privacyschendingen in Europa', SEW - Tijdschrift voor Europees en economisch recht, 2014-10.

Getting Privacy to a new Safe Harbour

Comment on the CJEU Judgment of 6 October 2015, Schrems v Data Protection Commissioner

by **Philipp E. Fischer***

Keywords: privacy; Safe Harbor; CJEU; Max Schrems; Data Protection Directive; surveillance; data transfer

Recommended citation: Philipp Fischer, Getting Privacy to a new Safe Harbour. Comment on the CJEU judgment of 6 October 2015, Schrems v Data Protection Commissioner, 6 (2015) JIPITEC 229 para 1.

A. Background

1 For a number of years, Facebook user and privacy law expert Maximilian Schrems[1] has insisted on a better data protection on Facebook. Since 2011, Schrems filed 22 complaints[2] against Facebook´s European headquarters in Dublin based on alleged infringement of the Irish Data Protection Act and the underlying European Union (EU) Data Protection Directive of 1995[3]. Following nearly three years, Schrems´ initiative "Europe vs. Facebook"[4] withdraw these complaints against Facebook; however, the "PRISM complaints"[5] were still pursued. The latter consisted of complaints against Apple[6], Facebook[7], Skype[8], Microsoft[9] and Yahoo[10]. In his lodged complaint with the Irish supervisory authority (the Data Protection Commissioner) regarding Facebook, Mr. Schrems upheld the view that, in light of the revelations made in 2013 by Edward Snowden concerning the activities of United States´ (US) intelligence services (in particular the National Security Agency - NSA), the law and practices of the US do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country. On 24 March 2015, the Court of Justice of the European Union (CJEU) heard[11] this procedure against Facebook, which had been referred[12] by the Irish High Court.

2 Facebook is bound to a legal basis called the "Safe Harbour" decision[13]. According to the EU Data Protection Directive of 1995, personal data may only be transferred to "third countries" (countries outside the EU and the EEA), if information is sufficiently protected in the country of destination. It is under the authority of the European Commission to decide whether other countries can guarantee this level of protection. In 2000, the EU Commission defined the level of protection set out by the Safe Harbour program - adopted by the US Department of Commerce - as adequate. US companies can therefore self-certify that they comply with European data protection rules. In order to do so they must prove their commitments regarding data

1 https://en.wikipedia.org/wiki/Max_Schrems.

2 http://www.europe-v-facebook.org/EN/Complaints/complaints.html.

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

4 http://www.europe-v-facebook.org/EN/en.html.

5 http://www.europe-v-facebook.org/EN/Complaints/PRISM/prism.html.

6 http://www.europe-v-facebook.org/prism/apple.pdf.

7 http://www.europe-v-facebook.org/prism/facebook.pdf.

8 http://www.europe-v-facebook.org/prism/skype.pdf.

9 http://www.europe-v-facebook.org/prism/microsoft.pdf.

10 http://www.europe-v-facebook.org/prism/yahoo.pdf.

11 Reference for a preliminary ruling from High Court of Ireland (Ireland) made on 25 July 2014 – Maximillian Schrems v Data Protection Commissioner, Case C-362/14, http://curia.europa.eu/juris/document/document.jsf?text=&docid=157862&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=161179.

12 http://www.europe-v-facebook.org/ref_ecj.pdf.

13 C(2000) 2441, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF.

protection before the US Federal Trade Commission (FTC). This includes the duty to inform users which personal information they transfer for what purpose, to disclose information on its transfer to third parties, to give users the right to access stored data, and to rectify data or to delete data. Among data privacy experts however, there were doubts[14] whether and to what extent US-based corporations would actually comply with this self-certification process, as companies are not obliged to provide evidence of these commitments and the EU itself does not oversee this process. The EU Commission also expressed its concerns: "Due to deficiencies in transparency and enforcement of the arrangement, specific problems still persist and should be addressed: a) transparency of privacy policies of Safe Harbour members, b) effective application of Privacy Principles by companies in the US, and c) effectiveness of the enforcement."[15] As Facebook grants the US intelligence services access to their databases, the US is not a "safe harbour" for European citizens' personal data; thus on 23 September 2015, the EU Advocate General, Mr. Yves Bot, brought into question the continuation of Safe Harbour on which data transfers to the US are based on.[16]

B. Decision of the CJEU of 6 October 2015

3 In its judgement of 6 October 2015[17], the CJEU declared the Safe Harbour decision of 2000 void. Although the CJEU ruled that the validity of the decision of 2000 is not a subject of the referred question itself, it indicated in margin numbers 93 and 94, that mass surveillance practices are incompatible with European fundamental rights. The CJEU claimed - in a remarkable way - decision-making power on questions of fundamental rights of EU citizens, which the EU Commission had formerly dealt with: "It is thus ultimately the Court of Justice which has the task of deciding whether or not a Commission decision is valid".[18] The CJEU held that "even if the Commission has adopted a decision, the national supervisory authorities, when dealing with a claim, must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the directive." [19] Thus, the CJEU found that the nature of Art. 3 of the Safe Harbour decision is illegitimate in this respect as it reduces the competence of national data protection authorities to fully assess the adequate level of data protection of self-certified companies in the US.

4 In light of this decision, the Irish High Court decided on 21 October 2015 that the Irish Data Protection Commissioner should investigate "Facebook Ireland Ltd" over alleged cooperation of "Facebook Inc" with US spy agencies, such as under the NSA's "PRISM" program. The initiative "Europe vs. Facebook" legally requested Data Protection Authorities in Ireland[20], Belgium[21] and Germany[22] to enforce the CJEU´s judgement on Facebook by reviewing and suspending Facebook's data transfers over US spy programs.

C. Valuation

5 The CJEU nullified one of the potential legal bases of EU-US data flow. A broad discussion has begun among EU data privacy experts whether - after the decision of the CJEU - alternatives to Safe Harbour are still permissible. Companies that have so far transferred European users' personal data to the US on the basis of Safe Harbour must now turn to another legal basis, such as binding corporate rules (BCR)[23], standard contractual clauses (SCC)[24] or consent given by the person affected.

6 After Safe Harbour was invalidated, companies such as Facebook have started to use contractual agreements[25] as an alternative in order to lawfully transfer data; this alternative is permissible insofar as these companies are not complicit in illegal "mass surveillance". Gerard Rudden representing the complainant in Ireland stated that: "All relevant

14 Press release of the Conference of German Data Protection Commissioners from 24 July 2013, https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9283.de.

15 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf, p. 18.

16 http://curia.europa.eu/juris/celex.jsf?celex=62014CC0362&lang1=de&type=TXT&ancre=.

17 European Court of Justice, Case C362/14, JUDGMENT OF THE COURT (Grand Chamber) of 6 October 2015, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5248977b390cb4b77beacd6135154f1a0.e34KaxiLc3eQc40LaxqMbN4Oc38Oe0?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=156974.

18 Court of Justice of the European Union, PRESS RELEASE No 117/15, p. 2.

19 Court of Justice of the European Union, PRESS RELEASE No 117/15, p. 2.

20 http://www.europe-v-facebook.org/comp_fb_ie.pdf.

21 http://www.europe-v-facebook.org/comp_fb_be.pdf.

22 http://www.europe-v-facebook.org/comp_fb_de.pdf.

23 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf.

24 http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

25 http://www.europe-v-facebook.org/comp_fb_scc.pdf.

EU decisions include an exception for cases of mass surveillance. There is no 'quick fix' through alternative transfer methods for companies that are involved in the violation of European fundamental rights."[26]

7 The German data protection authorities are of the opinion that the standard contractual clauses are also "disputable"[27], because the reasons on which the CJEU based its decision on Safe Harbour apply also – at least partially - to standard contractual clauses. The CJEU found that the de facto poorly restricted access of intelligence agencies on electronic communication is inconsistent with European fundamental rights and that neither Safe Harbour, nor standard contractual clauses, would restrict this power of public authorities. Based on the argument of the Advocate General, Flemming Moos und Jens Schefzig[28] argue that even when concluding a contract based on the standard contractual clauses an adequate level of data protection cannot be guaranteed. The Council and the European Parliament had given the Commission the power to decide, on the basis of Art. 26 (4) of the EU Data Protection Directive of 1995[29], that certain standard contractual clauses offer sufficient safeguards as required by Art. 26 (2). The CJEU held however that only the CJEU can declare a decision by the EU Commission void. This would therefore also concern the Commission´s decisions on standard contractual clauses. Until such a ruling by the CJEU, the standard contractual clauses would remain valid. Practitioners are therefore of the opinion that, until a new "safer safe harbour" is created, the transatlantic data flows could go on unhindered based on this available legal mechanism.[30]

8 The distinction between the validity of the standard contractual clauses as such – which has to be affirmed according to the findings above – and the competence of national supervisory authorities to suspend trans-border data flows should be emphasised. SSCs and BCRs cannot override the arguments made by the CJEU on mass surveillance under the Charter of Fundamental Rights (CFR)[31]. The CJEU held that the existence of a Commission decision cannot eliminate or even reduce the powers available to the national supervisory authorities. Thus, the same issues that lead to the invalidation of the Safe Harbour decision, could be brought before any of the national supervisory authorities in the 28 member states, in the case that a data subject claims that these contractual solutions do not properly protect the fundamental rights of the data subject. The relevant Decisions 2001/497/EC[32], 2004/915/EC[33] and 2010/87/EU[34] all have a clause that cares for exactly this situation, and allow DPAs to suspend data flows if "it is established that the law to which the data importer is subject imposes upon him requirements to derogate from the relevant data protection rules which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the standard contractual clauses"[35]. Whilst a supervisory authority assesses an adequate level of data protection, it may de facto block trans-border data flows.

9 After a review of the ongoing discussions on the CJEU´s decision, the author of this comment notes a lack of precise distinction in especially these three matters:

I. The two-stage process of an assessment of lawfulness of trans-border data transfers from an EU/EEA country to a third country

10 The European Data Protection Directive and the corresponding implementation in the Federal Data Protection Act of Germany (BDSG) contain two requirements for a lawful data transfer to third countries: The first ("first stage") is the need for a legal basis for the transmission as such (Art. 7 Data Protection Directive, § 4 (1) BDSG, § 4 (2) BDSG, §§ 27 ff BDSG). The second ("second stage") assesses the question if the data recipient in a third country can prove an adequate level of data protection (Art. 25

26 http://www.europe-v-facebook.org/prism2_en.pdf.

27 https://www.datenschutz.hessen.de/ft-europa.htm#entry4521.

28 http://www.cr-online.de/blog/2015/10/05/eugh-count-down-fuer-safe-harbor-teil-33-auswirkungen-eines-potenziellen-urteils.

29 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

30 http://www.eu2015lu.eu/en/actualites/communiques/2015/10/06-cjue-schrems/index.html; https://www.datenschutzbeauftragter-info.de/safe-harbor-gekippt-wie-geht-es-weiter/; http://rechtsanwalt-schwenke.de/was-bedeutet-das-safe-harbor-urteil-des-eugh-fuer-sie/.

31 Charter of Fundamental Rights of the European Union, 2000/C 364/01, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

32 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001D0497&from=en.

33 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004D0915&from=EN.

34 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF.

35 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001D0497&from=en, p. 4.

Data Protection Directive, § 4b BDSG). Unfortunately, it is still a common misconception that a data transfer to third countries can be lawful based only on ensuring (second stage) an adequate level of data protection.

11 Several online blogs[36] outline that the basis for a legitimate transfer could be consent given by the person affected. Such consent to be obtained by the person affected must be 1. freely given, 2. specific, 3. informed and 4. unambiguous (Art. 26 Data Protection Directive, § 4c Nr. 1 BDSG). The requirements for lawfully given consent should be clearly distinguished between the above mentioned two stages: for complying with stage two a user would have to be informed about the specific situation. The duty to inform according to § 4a (1) sentence 2 BDSG must be broadened and specified; there must be a notice which does not only designate the recipient country but also the lower level of protection so that the person can include this fact in its decision. Many US companies would then have to seek consent of persons affected in the EU for each transmission of data in advance, to inform these persons on the exact purpose and scope of the data processing and to indicate in its terms and conditions that US intelligence agencies have access to stored data. But this is problematic, as US law prohibits revelations of their cooperation with these agencies. Notifying the user that "data is transferred outside of the EU/EEA", as for example Facebook currently does in its terms and conditions[37], cannot be deemed appropriate. Mr. Schrems states: "To get a valid consent Facebook in our example would have to be very upfront and explain that all data that is used on facebook.com is subject to mass and indiscriminate surveillance by the US government."[38] According to the above-mentioned position paper of the German data protection authorities, the consent may "be given solely under strict conditions"; basically, the data transfer on the basis of consent "cannot be carried out repeatedly, en masse or routinely". According to Peter Schaar, former *Federal Commissioner* for *Data Protection* and Freedom of Information of Germany, a "blanket consent to extensive state surveillance by a third country, together with the absence of legal protection under EU law" would therefore be ineffective.[39]

II. The differences between the derogations set out in Art. 26 Data Protection Directive

12 In many cases, mass surveillance will not be of importance for trans-border data transfers. When data transfers previously relied on Safe Harbour, and a US controller or processor is not subject to US mass surveillance laws, a consent given by the person affected may be a reasonable option. Or for example, in the case that personal information is sent to the US for the purpose to "perform a contract" or for the "vital interests of the data subject". Most of the daily business transactions will therefore be able to use one of the derogations in Art 26 of the Data Protection Directive.

III. The legal basis for data transfers, the political debate about mass intelligence surveillance and the corresponding issue of infringement of the European Charter of Fundamental Rights

13 From a political view: for nearly two years, the EU and the US are negotiating a revision of the Safe Harbour Agreement. According to Reuters news agency, the discussions should be close to completion.[40] The CJEU´s decision will certainly have an impact on the ongoing negotiations. From a legal point of view: the CJEU´s decision makes it clear to national governments and EU institutions that European law is not allowed to crumble into dust only because of enhancing transatlantic trade. Through this judgment, the protection of fundamental rights in the EU has become a community project[41] and the CJEU´s decision is currently the third step on its long way to this. The first judgment dates back to April 2014 on data retention regulation. The second was that of May 2014 on the right to be forgotten and against Google. The third judgment is now attempting to end the discussion of the Internet as a legal vacuum. The court made it clear that future agreements relating to the traffic of data are a judicial subject.

36 e.g. http://www.heise.de/newsticker/meldung/Nach-dem-EuGH-Urteil-Alternativen-zu-Safe-Harbor-2837700.html and http://www.heise.de/newsticker/meldung/Safe-Harbor-Urteil-Gibt-es-ueberhaupt-noch-Alternativen-fuer-den-Datentransfer-in-die-USA-2840322.html.

37 https://www.facebook.com/policy.php.

38 http://www.europe-v-facebook.org/EN/Complaints/PRISM/Response/response.html.

39 http://www.eaid-berlin.de/?p=789.

40 http://www.reuters.com/article/2015/08/05/us-usa-eu-data-idUSKCN0QA1XB20150805.

41 Süddeutsche Zeitung, 07.10.2015, Ressort: Meinungsseite.

D. Perspective

14 The question regarding which "future regulation" could solve the above-mentioned recurring problems of legal and political bandwidth when it comes to trans-border data flows should be raised. Peter Schaar states that "in the longer term, the only way is to enforce on a global level privacy rights guaranteed in Art. 12 of the UN Declaration of Human Rights[42], the EU Charter of Fundamental Rights and in other constitutions of democratic states"[43].

15 To reach that goal, one objective should be a consolidated definition of what a trans-border data flow is, to define its features by explaining various combinations (controller, processor, sub-processor, data subject), the reason for it, its legal basis and the function of the level of protection of the country of destination, and to consider the radically increased quantity of such flows.

16 Another objective should be to examine existing bilateral and multilateral treaties and the rules therein that tend to regulate the flow of data across national borders. The first data protection laws, mainly in Europe, did not contain provisions restricting trans-border data flows. It was only when data outsourcing became an option to avoid strict domestic privacy laws, that some countries, partly based on the Convention 108 of the Council of Europe[44], started to introduce rules on trans-border data flow. The history of regulation in different regions, through leading regional and international instruments of the EU, OECD, Council of Europe, APEC, and other bodies should be considered in this respect.

17 It is important to analyse whether there is a common type of approach within these rules. For example, European regulations are advanced and set out a high level of data protection. In the US, the emphasis is more on self-regulatory approaches, as seen currently in the Safe Harbour case, however, the increase in global data transfers also influences understandings in these areas and could be of importance in order to find a common denominator. It should then be possible to outline certain typologies of different regulatory approaches. The nature of these approaches also depend on different aspects of privacy, such as the history of privacy, theories of privacy and the varying understanding of privacy mainly between the US and Europe.

18 Constantly developing technological solutions will also be of importance as well as regulations developed by the private sector. It will additionally be relevant to examine to which extent trans-border data flows provide compelling challenges to cloud adoption and as a result offer a solution for any business seeking to transfer data that must exercise significant care and due-diligence to avoid infringing privacy regulations and protections by sending data to or through places that do not guarantee the same level of protection.

19 The next objective for stakeholders for the protection of people´s privacy should then be to find out whether the actual status quo is of a sufficiently harmonized nature. Particularly, the contents of three current major frameworks, the US, the EU and the APEC, have to be analysed and outlined to what extent these could form a basis for harmonised international rules.

20 Finally, it has to be answered whether an international harmonisation of trans-border data flows could be reached through an international compromise. Harmonisation has made some progress on a regional level, for example within the members of the European Union. It ought to be defined how the General Data Protection Regulation[45] could be of influence on international transfers by regulating the territorial scope of the Regulation, highlighting the question of the application of EU rules to controllers not established in the EU when processing personal data of EU citizens.

21 Christopher Kuner states that "there is a nature desire to find a single, high-level solution to the legal issues raised by transborder data flow regulation, and the inability to do so is frustrating"46. Data privacy experts and policy makers should thus concentrate their efforts more than ever to confront this task.

* Philipp E. Fischer, LL.M. (IP, London/Dresden) is a Ph.D. cand. (UOC, Barcelona) and works as a Data Protection Officer & Auditor (TÜV) in Munich.

42 http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.

43 http://www.eaid-berlin.de/?p=789.

44 http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CAHDATA-RAP03Abr_En.pdf.

45 http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

46 Kuner, C. (2013): Transborder Data Flows and Data Privacy Law, Oxford University Press, p. 186.

jipitec

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

www.jipitec.eu