jipitec

3 | 2020

Volume 11 (2020)
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 11 Issue 3 December 2020
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

Prof. Dr. Thomas Dreier, M. C. J. (NYU)
KIT - Karlsruher Institut für Technologie, Zentrum für Angewandte Rechtswissenschaft (ZAR), Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe Germany

Prof. Dr. Axel Metzger, LL. M. (Harvard)
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

by **Lucie Guibault**

Recommended citation: Lucie Guibault, Editorial, 11 (2020) JIPITEC 241 para 1.

1 This issue marks the tenth month into the COVID-19 pandemic. Since March 2020, we have learned to live with the more or less strict public health measures put in place to 'flatten the curve' of infection from the virus. Words like 'social distancing', 'mask wearing', and 'lockdowns' have taken an entirely new meaning. In spite of these measures, the human toll is huge, most clearly among frontline workers and vulnerable people. While the curve is far from flat in most countries, the pandemic has brought to light the long time unacknowledged persistence of systemic inequalities: figures show that poorer, often racialized, communities are affected in a disproportionate way by the virus.

2 The positive news is that, at the end of 2020, three vaccines received the approval of health authorities in most countries of Europe, Canada, the United States and elsewhere. Several challenges await, however. Among them are the need to ensure an equitable distribution of vaccine doses among the countries of the world, to organize the logistics behind the transportation and handling requirements of the vaccines, as well as to convince people to actually get vaccinated.

3 Amid a global rise in COVID-19 cases and deaths, the last few weeks of 2020 saw the simultaneous conclusion of the Brexit process and the meltdown of the Trump administration. While the deal reached between PM Boris Johnson and the European Commission is certainly going in the books as a major historic event, it pales in comparison to the events that took place in the United States following the Presidential elections on November 3rd. Nothing shocked the world more than the violent and lethal siege of the Capitol in Washington D.C. on January 6th 2021 by Trump supporters. This led to a second vote by Congress within a twelve month period towards the impeachment of the President, this time under the heading "willful incitement of insurrection." Democracy in America has never been so fragile.

4 It will take experts years to unravel what led to the catastrophic year of 2020. One clear contributor to the general upheaval is the role Big Tech played in the spread of online misinformation. Wild ideas and lies swirled on Twitter, Facebook, Parler, Instagram and others, ranging from COVID-19 denials, to Brexit manipulation, anti-vaxxer misconceptions, QAnon conspiracy theories and white supremacist propaganda. Once Trump and his supporters were banned from social media sites, researchers observed a seventy percent decline in online misinformation. The recurring call for the regulation of Big Tech companies deserves increased attention in the wake of the recent events. More research is critical to understand the complex workings of powerful, integrated disinformation ecosystems and develop ways to address competing rights and freedoms in a global economy.

5 While these events rage outside our windows, normal life continues as much as COVID-19 restrictions allow. This issue contains captivating articles on issues close to our daily lives, dealing more specifically with data protection, online copyright and patent protection. Two articles investigate the relationship between the General Data Protection Regulation and the Enforcement Directive, looking respectively at the notion of joint control (Radtke) and the right of access (Vogiatzoglou, Fantin and DeWitte). On a related topic is the article by Hoffman and Otero Gonzalez on the role of data interoperability in the access and sharing debate. Lasota wrote on the rarely considered issue of net neutrality as seen from the perspective of router and modem users. While Klobunick explores ways to facilitate the online licensing of musical works, Hanuz examines whether hosting platforms could be held directly liable for the illegal copyright content uploaded by their users. Last but not least is Rantasaari's article on the abuse of patent enforcement actions. Enjoy the read!

Lucie Guibault

The Concept Of Joint Control Under The Data Protection Law Enforcement Directive 2016/680 In Contrast To The GDPR

by **Tristan Radtke***

Abstract: While the EU General Data Protection Regulation 2016/679 (hereinafter the GDPR) is on everyone's lips, the EU Data Protection Law Enforcement Directive 2016/680 (hereinafter the LED) exhibits a rather shadowy existence. This also applies with regard to the concept of multiple controllers determining purposes and means of data processing activities (Joint Control). The LED requires the Member States to implement a Joint Control concept similar to the concept set out under the GDPR. Differences between the Joint Control concepts under the GDPR and LED lie in the details, but at the same time they are significant and representative of the specifics and particular aims of the LED compared to the GDPR. The following article discusses the objectives of the LED and the Joint Control concept and explains them on the basis of the differences between the provisions related to Joint Control (Art. 26 GDPR and Art. 21 LED). In addition, collisions of application of GDPR and LED and their impact on Joint Controllers are discussed.

Keywords: Joint Control; Data Protection; GDPR; LED

Recommended citation: Tristan Radtke, The concept of Joint Control under the Data Protection Law Enforcement Directive 2016/680 in contrast to the GDPR, 11 (2020) JIPITEC 242 para 1.

A. (General) Data Protection Law and the Concept of Joint Control

1 Data protection law intends to contribute to an effective protection of natural persons – the data subjects – in relation to the processing of "their" personal data (cf. Art. 1(2) GDPR and previously Art. 1(1) Data Protection Directive 95/46/EC[1] (hereinafter the DPD)). Thus, data protection law implements the corresponding right and objective enshrined in Art. 8(1) Charter and Art. 16(1) TFEU.[2]

2 Transparency (Art. 5(1)(a) GDPR) on data processing operations, the pursued purposes and the persons having control over the data processing operations is a key element to ensure data subjects are able to exercise their (other) data subject rights laid down in Art. 12 et seqq. GDPR.[3] For example, a data subject who is not aware that personal data are stored incorrectly is practically unable to obtain rectification of such data. In addition, transparency is particularly relevant when it comes to the addressee of any data subject right and claims. Such

* Tristan Radtke is working as Academic Assistant at the Institute for Media and Information Law (Professor Dr. Paal, M.Jur. (Oxford)) at the University of Freiburg and is working on his doctoral thesis with focus on data protection law.

1 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 [1995] OJ L281/31.

2 Recital (1) GDPR.

3 EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 362.

an addressee is generally the controller under the GDPR. It is the natural or legal person determining purposes and means of the processing of personal data (Art. 4(7) GDPR). As it can be assumed such a person is able to control the circumstances of data processing activities and would be able to implement changes, the controller is responsible for compliance with the GDPR (Art. 24(1) GDPR).

3 Already under the DPD the European legislator acknowledged that a natural or legal person may determine the purposes and means "jointly with others" – and gave birth to the concept of Joint Control.[4] For example, the CJEU considered the cooperation of a social network and a fan page provider[5] or social plugin embedder[6] as constellations of Joint Control. Such a broad interpretation[7] of the joint determination attracted the attention of the internet community. However, under the DPD the judgments led "only" to the sharing of the role of controllers by two or more persons in such constellations. Although the Article 29 Working Party has – prior to the judgements – taken the view that a clear allocation of responsibilities is necessary[8] and there might be a joint and several liability in some cases,[9] the provisions of the DPD laid down no such consequences or particular obligations of Joint Controllers explicitly.

4 The GDPR implemented changes in this regard.[10] The GDPR does not only provide for answers in case of liability when multiple controllers and/or processors might be involved (Art. 82(4) GDPR), but stipulates additional consequences of controllers being considered Joint Controllers explicitly in Art. 26 GDPR. It should not be overlooked that Joint Control also offers an opportunity to realize cooperation in a transparent manner and with agreement requirements that are not as strict as in the case of the engagement of a processor under Art. 28(3) GDPR.[11] According to Art. 26(1),(2) GDPR, Joint Controllers shall determine their responsibilities in a transparent manner in an arrangement (hereinafter Joint Control Agreement, abbrev. JCA) and the essence of such a JCA shall be made available to the data subject. Such an obligation is another implementation of the transparency principle (Art. 5(1)(a) GDPR)[12] and necessary for "the protection of the rights and freedoms of the data subjects".[13] However, pursuant to Art. 26(3) GDPR data subjects may exercise their rights in respect of and against each of the data controllers. Therefore, the effectiveness of the exercise of data subjects' rights does not (completely) depend on whether the JCA determines the responsibilities in a transparent manner. The transparency of the JCA still affects data subjects indirectly, e.g., when Joint Controllers are unable to ensure the lawfulness of the data processing activities due to non-transparent and unclear determinations, or when the lack of additional information impairs the success of data subjects' requests.

5 To sum up, Joint Control under the GDPR ensures the protection of data subject rights in several ways and particularly in complex, pluralistically controlled[14] data processing operations.

4 EDPS, 'Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' (2019) 22.

5 CJEU, Case C-210/16, Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388 para 42, 44; discussed by Charlotte Ducuing and Jessica Schroers and Els Kindt, 'The Wirtschaftsakademie Fan Page Decision: A Landmark on Joint Controllership - A Challenge for Supervisory Authorities Competences' (2018) 4 Eur Data Prot L Rev 547.

6 CJEU, Case C-40/17, Fashion ID, ECLI:EU:C:2019:629 para 84; discussed by Louisa Specht-Riemenschneider and Ruben Schneider, 'Stuck Half Way: The Limitation of Joint Control after Fashion ID (C-40/17)' (2020) 69 GRUR Int. 159.

7 René Mahieu and Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World' (2019) 10 JIPITEC 39 para 39.

8 Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) WP 169, 24. A revised (final) version of this Opinion by the EDPB is expected for the next months.

9 Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) WP 169, 22, 24.

10 Emphasized too by Paul de Hert and Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 CLSR 179, 185; Brendan Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibility and Liability* (intersentia 2019) para 206.

11 Similar Valentina Colcelli, 'Joint Controller Agreement under GDPR' (2019) 3 ECLIC 1032.

12 Implied by Valentina Colcelli, 'Joint Controller Agreement under GDPR' (2019) 3 ECLIC 1032, 1032 ff.

13 Recital (79) GDPR; previously SEC (2012)72 final, 'Impact Assessment - Annex 1', 18.

14 Joachim Schrey in Daniel Rücker and Tobias Kugler (eds), *New European General Data Protection Regulation* (2018) para 495.

B. Specifics of the LED

6 The LED is the *lex specialis*,[15] the GDPR for the area of law enforcement, i.e., for "purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" (Art. 1(1) LED). The EU decided that the processing of personal data under such circumstances does require a substantially different legal concept,[16] as demonstrated by the limited scope of the GDPR (Art. 2(2)(d) GDPR).

7 The LED contributes even more than the repealed Council Framework Decision 2008/977/JHA (hereinafter the Framework Decision)[17] to a harmonized and effective data protection law in the field of police and law enforcement.[18] As diverse legal acts for specific data processing cooperation such as Europol and Eurojust are still in place, the scope of the LED is limited (cf. Art. 60 LED).[19] Nevertheless, as its predecessor – the Framework Decision – with respect to the DPD,[20] the LED adopts quite a lot of provisions from the GDPR. This hardly comes as a surprise as both the GDPR and the LED aim to protect the rights and freedoms of data subjects (Art. 1(2)(a) LED), albeit under different circumstances. Some provisions such as important definitions in Art. 3 LED, (most) data protection principles in Art. 4(1) LED and most data subject rights in Art. 12 et seqq. LED, the concept of data protection by design and by default (Art. 20 LED) as well as provisions on data processors (Art. 22 LED), records of processing activities (Art. 24 LED), data protection impact assessments (Art. 27 LED), and data security measures (Art. 29 et seqq. LED) have been adopted in essence or even almost verbatim. However, as it will be shown with regard to the Joint Control concept below, the different circumstances of data processing activities under the LED required modifications.

8 Such different circumstances referred to are: (i) the legal status of the Directive addressing only the Member States instead of a general application such as with respect to the GDPR (cf. Art. 288 TFEU); (ii) the controllers being usually public authorities, each of the same Member State and its derivatives; and (iii) the different circumstances of data processing activities under the LED allowing transparency requirements which are not as strict as under the GDPR.

I. Directive instead of Regulation

9 Due to its legal act specifics, a Directive takes a different approach than a Regulation.[21] The Directive is addressed to the Member States (Art. 288(3) TFEU) and leaves it up to them – at least in theory – to choose the form and methods to achieve a result. This choice with respect to the LED has been criticized[22] as it may impair the degree of harmonization.[23] This may be not only the case when Member States adopt provisions on the basis of an opening clause in the

15 Teresa Quintel, 'Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive' (2018) 4 Eur Data Prot L Rev 104, 104. However, as the GDPR implements a scope exception in Art. 2(2)(d) GDPR for purposes covered by the LED, there is no true conflict of laws.

16 Paul De Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) 7 New J Eur Crim L 7, 8.

17 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60.

18 Thomas Marquenie, 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework' (2017) 33 CLSR 324, 328; cf. SEC (2012)72 final, 'Impact Assessment - Annex 1', 31 ff.

19 Cf. Diana Alonso Blas, 'Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom' (2010) 11 ERA Forum (2010) 233, 238. For the history of the different legal acts see Paul de Hert and Vagelis Papakonstantinou, 'The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for' (2009) 25 CLSR 403, 405 and 413.

20 Due to the limited scope of the Framework Decision it has a comparably low impact, Paul De Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) 7 New J Eur Crim L 7, 7; Thomas Marquenie, 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework' (2017) 33 CLSR 324, 325.

21 Stressing this too EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 385; Paul de Hert and Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 CLSR 179, 182.

22 Cf. EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 305.

23 Thomas Marquenie, 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework' (2017) 33 CLSR 324, 328 ff.

LED but also when they provide for an even stronger protection in general as allowed pursuant to Art. 1(3) LED.[24]

10 The flexibility of the Member States under the Directive affects the provisions on Joint Control as well as other provisions. For example, Art. 21(2) LED allows the Member States to choose whether the data subject should be able to exercise his or her rights in respect of and against each of the Joint Controllers. In contrast, a similar provision is mandatory under the GDPR. In addition, each Member State may take into account specifics of its LED relevant data processing activities and may provide for additional safeguards for Joint Control constellations, e.g., with respect to information obligations and to align Art. 21 LED with Art. 26 GDPR.

II. Public Authorities as Controllers

11 While under the GDPR any public or non-public body can be considered a controller (Art. 4(7) GDPR), under the LED only competent authorities[25] are controllers (Art. 3(8) LED). Insofar the circumstances are similar to those under the Regulation (EU) 2018/1725[26] stipulating data processing activities carried out by the Union institutions, bodies, offices and agencies. Accordingly, a comparison of the Joint Control concept under the LED and the Regulation might be useful for the interpretation of Art. 21 LED and will therefore be made in the following (see below C.IV., E.).

12 Pursuant to Art. 3(7)(b) LED "any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes" set out in Art. 1(1) LED may be considered a competent authority too.[27] Thus private bodies may be controllers under the LED. However, taking into account the police purposes as classical governmental tasks, the majority of controllers will still be public authorities.

13 In most cases, only the authorities within a Member State will cooperate in data processing activities under the LED as each Member State would like to uphold its national sovereignty in the fields of data processing for police purposes.[28] In such a case, only the authorities of one Member State and its bodies are Joint Controllers. Thus, the data subject is faced with data controllers as liability subjects of equal solvency. Therefore, it is of less importance to the data subject whether he or she can exercise his or her rights in respect of and against each of the Joint Controllers and whether they are each held liable for the entire damage. Nevertheless, (personal) data transfers between Member States or even to third countries could be admissible, as Art. 35 et seqq. as well as Art. 50 LED demonstrate.

14 In addition, each Member State will most likely regulate the processing activities of its authorities – as Art. 8(1) LED with Union or Member State law as only legal base demonstrates[29] and as already required for example by the German constitution.[30] Even possible constellations of Joint Control might be already governed by the respective law. There is less need for an additional transparent agreement if the legislator itself has already regulated the responsibilities in detail and by means of mostly public accessible law.

III. Restriction of Transparency due to specific purposes

15 With respect to (iii), transparency is a leading principle of the GDPR and not of such great importance under the LED.[31] Even when comparing the occurrence of

24 Refer as well to recital (15) LED.

25 Preferring a narrow understanding of this term Plixavra Vogiatzoglou and Stefano Fantin, 'National and public security within and beyond the Police Directive' in Anton Vedder and others (eds), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Intersentia 2019) 31 and 48 ff; EDPS, 'Opinion 6/2015 – A further step towards comprehensive EU data protection' (2015) 9.

26 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295/39.

27 Refer as well to recital (11) LED.

28 Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15' (1987) para 29.

29 In detail Juraj Sajfert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for police and criminal justice authorities' in Mark D Cole and Franziska Boehm (eds), *GDPR Commentary* (Edward Elgar Publishing, forthcoming) 6.

30 Cf. EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 399, 401.

31 Critical EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012)

the words "transparency" and "transparent" in both legal acts, the GDPR prevails with 14 against 2 occurrences. This might be justified because of the specific character of the data processing purposes within the scope of the LED.[32] Consequentially the LED does not explicitly require controllers to process personal data "in a transparent manner in relation to the data subject" (cf. Art. 5(1)(a) GDPR). The principle of "lawfulness, fairness and *transparency*" (Art. 5(1)(a) GDPR) has been narrowed down to a principle of lawfulness and fairness (Art. 4(1)(a) LED).[33] The information to the data subject has to be provided not in a "concise, *transparent*, intelligible and easily accessible form" (Art. 12(1) GDPR) but in a "concise, intelligible and easily accessible form" (Art. 12(1) LED). Therefore, the LED gives the impression that public data processing activities related to criminal offences require less transparency in general. As covert investigations, video surveillance or other forms of covert data processing activities are more likely under the circumstances covered by the LED, this might be an explanation for such an adaption[34] – whether this can be criticized or not.

16 In addition, there are several specific exemptions from the right of access in Art. 15 LED, e.g., to "avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties" (Art. 15(1)(b) LED). However, transparency still has to be taken into account by controllers under the LED.[35]

C. Joint Controllers – Consequences according to Art. 21 LED

17 As under Art. 26 GDPR, important aspects – in particular responsibilities regarding the exercise of data subject rights – related to Joint Control constellations falling within the scope of the LED shall be determined in a Joint Control Agreement (Art. 21 LED). This important legal consequence of Joint Control has been modified in several respects under the LED. Such modifications are representative for the necessary deviations from the GDPR provisions due to the described specifics of the LED such as its material scope.

18 After all, the GDPR concept of Joint Control in essence has been implemented under the LED as well. The Joint Control concept implemented in the LED aims to protect the data subjects too, particularly when it comes to transparency and effective data subject rights. And even under the LED, despite the minor importance of transparency thereafter, a clear "allocation"[36] – respectively "attribution"[37] – of the responsibilities of Joint Controllers is necessary.

I. Legislator first

19 When it comes to responsibilities of Joint Controllers determined by the legislator there are virtually no differences between the GDPR and the LED. To the extent "the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject" there is no need for determining such in an arrangement between the Joint Controllers (Art. 21(1)(2) LED). As described above (see B.II.), the constellations of Joint Control within the scope of the LED will mostly be governed by Union or Member State law when assigning tasks to their authorities and bodies. Therefore, a provision such as Art. 21(1)(2) GDPR is of much higher importance under the LED and there will be fewer Joint Control Agreements compared to constellations to which the GDPR applies.

20 In Germany, for instance, there is a central anti-terrorism file, which is fed by the data transferred by several public authorities and might be considered a Joint Control constellation. However, the legislator probably takes a different view as the respective Act ("Antiterrordateigesetz")does not provide for an explicit allocation of responsibilities within the meaning of Art. 21(1)(2) LED.

para 327.

32 Spring Conference of European Data Protection Authorities, 'Position paper on Law Enforcement & Information Exchange in the EU' (2005) 10.

33 Taking a different view Thomas Marquenie, 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework' (2017) 33 CLSR 324, 330.

34 Recital (26)(2) LED. See also EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 364; Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15' (1987) para 44 ff; Paul De Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) 7 New J Eur Crim L 7, 9; Diana Alonso Blas, 'Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom' (2010) 11 ERA Forum (2010) 233, 243.

35 Recital (26)(1) LED and Article 29 Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' (2017) WP 258, 17.

36 Recital (79) GDPR.

37 Recital (54) LED.

II. Lower requirements for content of the arrangement

21 Both the GDPR and the LED stipulate that the Joint Controllers have to determine the responsibilities for compliance with central data protection obligations by means of a Joint Control Agreement. The determination of the responsibilities regarding the exercise of data subject rights, including the information obligation(s), is emphasized as essential for the protection of data subjects. In addition, according to Art. 26(2)(1) GDPR, Joint Controllers shall ensure that the roles and relationships between them are duly reflected. This requires inter alia the description of the parties involved and information on different stages of the processing activity.[38] By requiring Joint Controllers to get an overview of their cooperation, transparency *vis-à-vis* data subjects is not only facilitated by preparing the provision of information to data subjects, but it also encourages Joint Controllers to assess whether the envisaged data processing activities meet essential requirements of data protection law (cf. Art. 24(1) GDPR).

22 Such a requirement regarding the reflection of the roles is completely missing in Art. 21 LED. This can again be explained by the fact that most controllers under the LED are public authorities and the legislator at least reflected the roles in the respective legal act. There is no need to reflect the roles and relationships in a JCA if this is already done by law. In addition, public authorities are particularly sensitive to the assessment of the lawfulness and admissibility of their (data processing) activities, as they are already constitutionally obliged to do so. For example, the German constitution and the principle of the rule of law enshrined therein require the authorities to always act in accordance with the law ("Gesetzmäßigkeit der Verwaltung") and provides for even stricter requirements in the (LED) area of the prosecution of criminal offences. Nevertheless, such an obligation of Joint Controllers would also have been suitable under the LED. There are similar controller obligations in general under the LED, even though controllers might be mostly public controllers (cf. Art. 19(1) LED). Particularly with respect to fundamental rights, which are of crucial relevance for data processing activities within the scope of the LED,[39] such a provision can sensitize public authorities, encourage them to self-control, and may therefore reduce the risk of unclear and non-transparent data processing activities which violate principles of data protection law. Accordingly, the German legislator, for example, requires that the roles and responsibilities shall be reflected in the Joint Control Agreement (Section 63 of the German Federal Data Protection Act ("BDSG")).

III. Mandatory contact point

23 According to Art. 26(1)(3) GDPR, Joint Controllers are free to designate a contact point. Such a designation may avoid the administrative effort necessary to forward data subjects' requests to the other Joint Controllers. At the same time, it may also allow for a request from a data subject being processed more quickly, which is of direct benefit to the data subject.[40] Ultimately, the provision is thus a manifestation of Art. 12(2)(1) GDPR (cf. Art. 12(2) LED), which requires controllers to facilitate the exercise of data subject rights. However, its material impact under the GDPR is limited, since the data subject may exercise his or her rights in respect of and against each of the Joint Controllers (Art. 26(3) GDPR).

24 In contrast, the designation of a contact point under the LED is mandatory pursuant to Art. 21(1)(3) LED – similar to Art. 24(1)(3) of the GDPR Draft of the Council.[41] This allows the data subject to contact a single person with regard to all data subject rights, so that the effective enforcement of data subject rights can be ensured. Due to the specific issue that the data subject is usually confronted with solvent public authorities as Joint Controllers and as a contact point (see above B.II.), this can therefore contribute almost as effectively to the protection of the data subject as the joint and several liability, the implementation of which is at the discretion of the Member States according to Art. 21(2) LED. This background completely changes the role of the contact point: While under the GDPR it is the icing on the cake for the data subjects, under the LED, in the absence of mandatory joint and several liability of the Joint Controllers, it is crucial for the effective protection of the data subjects and their

38 Jürgen Hartung in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung/BDSG* (2nd edn, C.H. Beck 2018) Art. 26 DS-GVO para 22.

39 EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 305 and 366; CJEU, Case C-362/14, Schrems, ECLI:EU:C:2015:650 para 86, 87, 94 et passim; CJEU, joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), ECLI:EU:C:2014:238. In detail on the required balance of interests and rights Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice* (Springer 2012) 19 ff.

40 Similar Valentina Colcelli, 'Joint Controller Agreement under GDPR' (2019) 3 ECLIC 1032, 1039.

41 Council of the European Union, Doc. 9565/15.

rights.[42] Even though, the concept of Joint Control and the requirement for the determination of responsibilities are not redundant. The mandatory contact point cannot contribute to the same extent to the effectiveness of data protection compliance, in particular with respect to data subject rights. Whether there is a contact point or not, the internal allocation of responsibilities by the (Joint) Controllers or the legislator ensures that each (Joint) Controller is aware of its specific obligations. Additionally, the allocation of responsibilities encourages each Joint Controller to implement appropriate measures and procedures necessary for data protection compliance when processing the personal data "of" the data subject within the scope of his responsibility.

25 The importance of the contact point under the LED indicates the necessity of further requirements in connection with the obligation of the Joint Controllers to designate a contact point. It already follows from the concept and aim of a contact point that it must actually be (easily) accessible for the data subject. Therefore, in particular, the data subject must be able to obtain information on whether a contact point exists and how to reach out for such a contact point, otherwise the objective pursued by this contact point will be counteracted. The obligation to designate a contact point thus implies an obligation to provide information on the contact point in accordance with Art. 12, 13 LED. In addition, the contact point must be a body which is also able to enforce the rights of the data subjects as effectively as possible. The designation of a person other than the public authorities involved as (Joint) Controllers is therefore not admissible, cf. Art. 21(1)(4) LED.

26 At this point, the Member States can fill in their regulatory leeway and thus not only ensure clarity, but also provide more details on the function of the contact person. Since a Directive requires the transposition by the Member States anyway, the prohibition of repetition[43] under European law such as for Regulations does not apply. Furthermore, pursuant to Art. 1(3) LED even stricter provisions of the Member States are permissible. Therefore, clarifications in the transposed provisions are all the more permissible. The national legislator should make use of such leeway and should explicitly stipulate the information obligations regarding the contact point. In addition, for example, national law could provide for the admissibility of the designation of an external (public) body as a contact point, provided that it (i) can process requests for data subjects at least as effectively as one of the Joint Controllers, and (ii) is an independent subject of liability, so that the Member State provides higher safeguards in accordance with Art. 1(3) LED with the implementation of an additional liability subject. However, as an example for reducing clarity as national legislator, the German transposition in Section 63 BDSG does not provide explicitly *even* for the requirement of the designation of a contact point in general.

IV. Absence of information obligation

27 In contrast to the GDPR (Art. 26(2)(2) GDPR), there is no obligation to provide data subjects with the essence of the Joint Control Agreement. One explanation might be that the obligation to reflect the respective roles and relationships (Art. 26(2)(1) GDPR) has not been adapted as well (see above C.II.). Therefore, the legislator might have been of the opinion there has been no necessity to implement Art. 26(2) GDPR as a whole. However, even under the GDPR, such essence of the Joint Control Agreement may also include information on the determination regarding the rights of the data subjects under Art. 26(1)(2) GDPR, in turn, adopted under the LED.[44] Therefore, the absence of a provision such as Art. 26(2)(1) GDPR alone cannot explain this.

28 Instead, a possible reason might be the greater relevance of the determination by the legislator as already elaborated (see above C.I.). In such a case, the legal regulation contains the information relevant to the data subject. Incidentally, this is also a manifestation of the lower transparency requirements (see above B.III.). Here, however, what is said about the mandatory designation of a contact point (see above C.III.) becomes particularly relevant. Since under the LED a contact point for data subjects must be designated in any case (Art. 21(1)(3) LED), additional information is of less importance for the exercise of the other data subject rights. Finally, the data subject is faced with a solvent contact point mostly (see above B.II.) against whom he or she can exercise all his or her data subject rights.

29 Insofar as the Member States implement the joint and several liability regarding data subject rights according to Art. 21(2) LED, such as the German legislator, such a national provision becomes more similar to Art. 26 GDPR. Nevertheless, there is no obligation under Art. 21 LED to provide data subjects

42 One might also discuss with respect to Art. 12(2) LED whether there is an obligation of Joint Controllers to forward a data subject request to the competent Joint Controller.

43 CJEU, Case 34/73, Variola, ECLI:EU:C:1973:101 para 9 ff. Cf. recital (8) GDPR.

44 Probably Valentina Colcelli, 'Joint Controller Agreement under GDPR' (2019) 3 ECLIC 1032, 1037; Mario Martini in: Boris P Paal and Daniel A Pauly (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz* (3rd edn, C.H. Beck 2021) Art. 26 DS-GVO para 32.

with the essence of the agreement. Such information is still necessary to enable the data subject to choose the best addressee instead of the contact point in order to exercise the data subject rights as effectively as possible. Thus, it might be possible for the addressed Joint Controller to act on the request more quickly, due to the distribution of tasks. The sense of such a duty to provide information on the responsibilities is therefore not completely eliminated under the LED. This is also confirmed by the Regulation (EU) 2018/1725: Although controllers in the meaning of this Regulation are (Union) public authorities (Art. 3(8) Regulation (EU) 2018/1725), Art. 28(2)(2) Regulation (EU) 2018/1725 obliges Joint Controllers to make the essence of the JCA available to the data subject and Art. 28(3) Regulation (EU) 2018/1725 stipulates a joint and several liability. Therefore, the fact that controllers under the LED are mostly public authorities may not justify such an omission of Art. 26(2)(2) GDPR.

30 Member States can fill in their regulatory leeway in this respect. Insofar as the Directive (EU) 2018/1725 provides as well as the GDPR for a Joint Control information obligation, this does not mean that the reverse conclusion can be drawn that a corresponding provision in the context of the LED would be inadmissible due to Art. 21 LED being conclusive in this regard. Such an information obligation would be an example par excellence for a higher safeguard in the meaning of Art. 1(3) LED. It is therefore once again up to the Member States to provide for an information obligation when transposing the LED and thus ensure more transparency vis-à-vis data subjects. Such a provision could at the same time include the obligation to inform the contact point (see C.III. above) implementing a coherent overall Joint Control concept.

D. Right to compensation

31 Infringements of the GDPR resulting in a person suffering damage give the data subject[45] the right to compensation according to Art. 82 GDPR. While this right to damages is regulated in detail in Art. 82 GDPR, Art. 56 LED leaves the details to the Member States. Thus, the provision on joint and several liability of multiple controllers, such as Joint Controllers, in Art. 82(4) GDPR is not mandatory under the LED. In view of the lower solvency risks with regard to public authorities as potential debtors (see above B.II.), the negative impact on the data subjects under the LED is limited. However, a particular disadvantage could be that, due to non-transparent or even uncommunicated cooperation between the Joint Controllers, the data subject does not know for certain in respect of and against which Joint Controller he or she can exercise his or her right to compensation. Even though, it should be noted that the right to compensation constitutes a right within the meaning of Art. 21(1)(4) LED. Thus, the data subject can also exercise his or her right to compensation in respect of and against the contact point. The wording ("right") does not contradict this, but even supports such an interpretation. Systematically, especially the position of Art. 21 LED outside Chapter III shows that reference is not only made to rights mentioned there but also includes rights such as the right to compensation from Chapter VIII (Art. 56 LED).

E. Collision of the GDPR and LED

32 Considering the differences between the implementation of the Joint Control concept under the GDPR and the LED, it could become particularly challenging if both the GDPR and the – Member State transpositions of the – LED would be applicable to such cooperation.

33 The material scope of the GDPR and the LED are mutually exclusive based on the processing purposes (Art. 2(2)(d) GDPR, Art. 2(1),1(1) LED). As the GDPR covers all data processing purposes except for the purposes covered by the LED, the LED is considered the *lex specialis*.[46] Nevertheless, in some constellations it may not be entirely clear whether the purpose falls within the scope of the LED, as for example in the case of migration and border control and potential criminal offences.[47] However, there is no combined applicability of the Joint Control concepts of the GDPR and LED – i.e. controllers under the GDPR and LED being considered together as Joint Controllers – for two reasons.

34 First, in practical terms, whenever personal data are processed by the competent authorities for the purposes covered by the LED with particular relevance to fundamental rights, the legislator will not want to provide for the right of other (GDPR) bodies to determine purposes and means of such processing activities, especially when personal data

45 Art. 82(1) GDPR just states "any person".

46 Cf. Teresa Quintel, 'Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive' (2018) 4 Eur Data Prot L Rev 104, 104.

47 In detail Juraj Sajfert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for police and criminal justice authorities' in Mark D Cole and Franziska Boehm (eds), *GDPR Commentary* (Edward Elgar Publishing, forthcoming) 3; EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 317.

are or should be transferred to private bodies.[48] This would be in line with the Council of Europe's recommendation that data transfers from the police sector to recipients for non-police purposes should be limited to the absolute minimum necessary.[49] If one thinks for example of a private body providing retained personal data to a competent public authority for the purpose of investigation detection or prosecution of criminal offences,[50] the private body and the public authority do not determine such purpose jointly and are therefore not Joint Controllers.[51]

35 Second, Art. 26(1)(1) GDPR as well as Art. 21(1)(1) LED require "two or more *controllers*" in the meaning of the GDPR and the LED, respectively, as a condition for Joint Control. In contrast, Art. 28(1)(1) Regulation (EU) 2018/1725 stipulates explicitly "controllers other than Union institutions and bodies" and includes therefore controllers, which are not controllers in the sense of the Regulation (EU) 2018/1725. Thus, as long as there is only one GDPR and one LED controller only the relevant act will apply in each case. Provided that there are at the same time two or more (Joint) Controllers under the GDPR or LED for connected data processing activities, the respective Joint Control provisions will apply for the data processing activities covered by the scope of either the GDPR or the LED. It might be theoretically conceivable that the identical processing activity serves a purpose in terms of both the GDPR and the LED. In practice, however, it will be possible to split up such processing activity and separate the processing activities clearly, for example if the personal data already collected under the LED are processed further for statistical purposes in accordance with the GDPR *at a later time*. The (Joint) Control under the LED/GDPR thus ends with the corresponding processing activity such as a transmission – and the (Joint) Control under the GDPR/LED begins with the corresponding subsequent processing activity such as a collection. As such a constellation may happen only when the LED *and GDPR* purposes are pursued for connected data processing activities, the function of the LED as a *lex specialis* with regard to the *LED purposes* does not prevent such a consecutive Joint Control according to two legal acts. Such a constellation may take place when a LED controller works together with a GDPR controller for GDPR purposes and is therefore a GDPR controller when processing the same data. For example, personal data might be processed for purposes within the meaning of Art. 1(1) LED and later as part of different processing activities for internal administrative purposes, such as in cases of theft and lost property,[52] or scientific research purposes and statistical purposes (cf. Art. 9(2) LED).[53] However, this will also take place regularly within one authority and the processing activities will be strictly separated.

36 Therefore, a real collision of both provisions is unlikely. When the same public authority is considered a controller under both the GDPR and LED for related data processing activities and there are two controllers under the GDPR and/or LED, then each provision will apply separately and only to the data processing activities covered by the respective legal act. As there are different processing activities, separated inter alia by the different purposes, such a consecutive application and e.g., two Joint Control Agreements can be handled in practice.

F. Summary

37 The concept of Joint Control has been implemented in both the GDPR and the LED. Due to its legal nature as a Directive, public authorities being data controllers in most cases, and different transparency requirements, the implementation of the Joint Control concept required deviations from the GDPR, e.g., in case of Joint Control and Art. 21 LED. Under the LED, not only will the legislator stipulate Joint Control situations more frequently, but there are also less strict requirements for the JCA and – even

48 For instance, information concerning stolen credit cards, Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15' (1987) para 63. Regarding the necessity of transfers for the LED purposes Diana Alonso Blas, 'Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom' (2010) 11 ERA Forum (2010) 233, 242; Spring Conference of European Data Protection Authorities, 'Position paper on Law Enforcement & Information Exchange in the EU' (2005) 4 and 7. For any data processing activities falling in the scope of the GDPR, in addition compliance with Art. 10 GDPR has to be ensured.

49 Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15' (1987) para 56 ff.

50 Recital (11) LED.

51 Cf. Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) WP 169, 20.

52 Cf. Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15' (1987) para 53.

53 Denis Kelleher and Karen Murray, *EU Data Protection Law* (Bloomsbury 2019) para 21.13. For another example EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 317; and in general recital (19)(4) GDPR. In Germany, for example, one might think of the police crime statistics ("Polizeiliche Kriminalstatistik (PKS)").

though not always comprehensible[54] – information obligations. However, the contact point is gaining in importance under the LED and in this respect an obligation to inform who the contact point is. The Member States should fill in their regulatory leeway to align the Joint Control concept under the LED with the GDPR with respect to transparency. A Joint Control constellation with applicability of both the GDPR and LED to connected data processing activities is conceivable, but the respective provisions need to be assessed separately and the different purposes and separable data processing activities allow for the handling of such a constellation.

54 Cf. EDPS, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) para 441.

Demystifying The Role Of Data Interoperability In The Access And Sharing Debate

by **Jörg Hoffmann and Begoña Gonzalez Otero***

Abstract: In the current data access and sharing debate, data interoperability is widely proclaimed as being key for efficiently reaping the economic welfare enhancing effects of further data reuse. Although we agree, the role data interoperability plays for data access cannot be straightforwardly answered. First, data interoperability, as a technical mechanism, is an inherent part of some regulated data access rights. In these particular cases, data interoperability is the key enabler for efficient (re-)use of data. This example shows the relevance of addressing data interoperability within the corresponding obligation of the access right. It also reveals that interoperability becomes key from a market failure perspective if the failure stems from a lack of efficient data use or potential lock-ins. Another example where data interoperability goes hand in hand with data access regimes is digital platforms. However, digital markets have a tendency to "tipping". Such a tendency is not natural but induced by individual practices, e.g., the obstruction to interoperability. To this end, subjecting dominant online platform companies to additional interoperability obligations and stricter monitoring could be an effective approach to control the abuse of market power. Likewise, the current EC's ambition to pave the way towards European digital sovereignty highly depends on the design of a data interoperability policy within the context of access to and re-use of data. With this background in mind, our contribution answers the question of when and how data interoperability, as a precondition to data quality, should be addressed by the legislature. The paper brings together the technical, legal and economic aspects of data interoperability, conceptualizing it within the data sharing debate. It first elaborates on the notion of interoperability in the current data access and data governance frameworks. An analysis of the different technical interoperability facilitators and the existent legal framework that may hinder data interoperability in this context follows. The debate of APIs is still ongoing and brings on fundamental questions to the proper functioning of exclusive rights. To what extent could IPRs and trade secret protection encumber data interoperability? What would be the implications of granting IPR or trade secret protection for APIs, both in terms of raising incentives for their provision and with regard to effects on competition? The paper continues by considering the pros and cons of a more normative approach toward data interoperability. Data interoperability should be treated only as a means to an end and not as an end in itself. It should be taken as a part of the broader data sharing and access discussion, reflecting on the positive and adverse effects alike. To this end, a public law approach within the realm of a data governance solution seems more favorable. Such a governance solution could also entail a more consistent solution to conflicting IP, sui generis database and trade secrets protection in data, which is currently not thoroughly and clearly assessed either. These conflicts need a more holistic assessment of overlapping exclusive rights and their re-usability options.

Keywords: data driven innovation; data market failures; data governance; APIs; competition and regulation; interoperability

Recommended citation: Jörg Hoffmann and Begoña Gonzalez Otero, Demystifying the role of data interoperability in the access and sharing debate, 11 (2020) JIPITEC 252 para 1.

A. Introduction

1 In the ongoing debate about how to achieve the full realisation of the data economy, a lack of data interoperability has been rightly identified as a key impediment. A couple of years ago, the International Data Corporation's report distinguished three main paths followed to solve the lack of data interoperability[1]: First, firms and public bodies increasingly opening up their data via Application Programming Interfaces (APIs) granting access to third parties. Second, specific industry data standards and more high-level architecture standards have been developed to make data easily accessible and transferable. Third, a new category of firms has emerged, which focus on data transformation and provide services directly to end users.

2 Additionally, future data marketplaces could also act as data normalizers and define standard data models and formats for all the traded data.

3 From a regulatory perspective, there are different strategies and options to enhance data access, sharing and re-use across society.[2] In the case of regulated data access regimes, what we have noticed is that only thinking about the access right itself is not enough. Data interoperability, as a technical mechanism, is an inherent part of some data access rights.

4 In such cases, data interoperability is the key enabler for efficient (re-)use of data. Thus, it is important to address data interoperability within the corresponding obligation of the access right. Interoperability becomes key from a market failure perspective if the failure stems from a lack of efficient data use or potential lock-ins.

5 A clear example where data interoperability goes hand in hand with data access regimes are digital platforms. The use of data is now the world's biggest business. Some $1.4trn of the combined $1.9trn market value of Alphabet and Facebook comes from users' data and the firms' mining of it, after stripping out the value of their cash, physical and intangible assets, and accumulated research and development.[3] Digital platforms provide a basis for delivering or aggregating services and content from service and content providers to end users. These basic operating principles are found in platforms in a variety of sectors and they are reflected in other definitions of digital (or online) platforms, such as those proposed earlier by the European Commission.[4] Digital platforms are key enablers of digital trade.[5] They facilitate access to information; they also reduce the traditional friction of matching supply and demand. As such, digital platforms may serve as a driver for innovation. However, several governmental and academic studies[6] have found violations of antitrust[7], consumer protection and privacy law.

* Max Planck Institute for Innovation and Competition, Munich. E-mail: joerg.hoffmann@ip.mpg.de; begonia.otero@ip.mpg.de.

1 IDC, "Technical Barriers to Data Sharing in Europe" (January 2017) <https://view.publitas.com/open-evidence/d3-12-technicalbarriers_06-01-2017-1/page/1> (accessed 13.09.20).

2 OECD "*Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*" OECD Publishing, (Paris, 2019) < https://doi.org/10.1787/276aaca8-en> (accessed 13.09.2020).

3 Cf. Viktor Mayer-Schönberger has noted that access to capital is no longer the biggest problem for startups. It is access to data. See The Economist, "Who owns the web's data?" (October 22, 2020) <https://www.economist.com/business/2020/10/22/who-owns-the-webs-data> (accessed 13.09.2020).

4 European Commission, "Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries, Data and Cloud Computing and the Collaborative Economy" (2015) < https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environmentplatforms-online-intermediaries-data-and-cloud> (accessed 13.09.2020).

5 Digital trade is a broad concept, capturing not just the sale of consumer products on the Internet and the supply of online services, but also data flows that enable global value chains, services that enable smart manufacturing, and myriad other platforms and applications. USTR, Key Barriers to Digital Trade (2017) <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade#:~:text=Digital%20trade%20is%20a%20broad,myriad%20other%20platforms%20and%20applications> (accessed 13.09.2020).

6 Among other Jacques Crémer, Yves-Alexandre de Montjoye, Heike Schweitzer, "Competition Policy for the Digital Era" (2019) <http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf >; (accessed 13.09.2020); Stigler Committee on Digital Platforms. Final report (2019); Australian Competition and Consumer Commission, "Digital platforms inquiry - final report (parts 1–3)" (July 2019); Philip Marsden, Rupprecht Podzsum, "Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement" Konrad Adenauer Stiftung e. V. (2020), Jason Furman, Diane Coyle, Amelia. Fletcher, Philip Marsden and Derek McAule, "Unlocking Digital Competition" (London: HM Treasury, 2019).

7 On October 20, 2020, the DOJ filed a civil antitrust lawsuit in U.S. District Court for the District of Columbia to stop Google from unlawfully maintaining monopolies through anticompetitive and exclusionary practices in the search

These are motivated by certain characteristics of digital platforms, namely, network externalities, economies of scope and their inherent advantages such as access to data. Some giant platforms have occupied a gatekeeper position allowing them to decide on economically dependent ecosystem partners, to determine the conditions for access and to control the consumer interface. Information asymmetries take place, not only between big tech platforms and small businesses and consumers, but also between big tech platforms and governments. A high concentration of market power throughout many different markets, together with certain acquisitions of startups and the potential to leverage data specific competitive advantages, is likely to lead to market foreclosure effects ultimately causing both static and dynamic inefficiencies. In order to reduce the potential leveraging of data power, the idea of imposing data sharing obligations for platforms is currently being discussed. To this end, a good example of how to address the interoperability provision would be the imposition of *ex ante* rules of conduct for dominant platforms with more stringent interoperability obligations as a potential remedy against the data induced power asymmetries. Subjecting dominant online platform companies to additional interoperability obligations and stricter monitoring could be an effective approach to control the abuse of market power.

6 Similarly, the current EC's ambition to pave the way towards European digital sovereignty highly depends on the design of a data interoperability policy within the context of access to and re-use of data. Such a design needs to reconcile the interests of all parties implied and must reflect on the positive and adverse effects of data sharing. The accomplishment of high levels of trust among the participating parties is a key aspect of further incentivizing data sharing. Data trusts and hybrid federated infrastructural models such as Gaia-X[8], intended to build European Data Spaces will very much depend on a proportionate and clear legal framework for data interoperability.

7 Technically, data interoperability depends on certain facilitators, namely data standardization and APIs. This paper explores data standardization as a technological enabler of data interoperability considering both positive and negative effects.[9] Yet, the debate about APIs is still ongoing and raises fundamental questions regarding the proper functioning of exclusive rights. To what extent could IPRs and trade secret protection encumber data interoperability? What would be the implications of granting IPR or trade secret protection for APIs, both in terms of raising incentives for their provision and with regard to effects on competition? To this end, there are three key aspects that need to be considered: first, whether APIs, as part of a computer program, can enjoy the same copyright protection; second, what happens if a third party uses the underlying right when establishing data interoperability; and, third, to what extent the user of an API can rely on current exceptions and limitations.

8 Furthermore, standardization of APIs, working as plug-and-play gateways, could provide better levels of data interoperability, but might as well bring new challenges for competition law as it may expose the party seeking access to potentially share 'their' data in return. Opening up APIs by providing plug-and-play solutions may thus contain the risk of inappropriately reinvigorating data-induced market dominance, potentially causing further market foreclosure scenarios.[10] Analyzing how firms use APIs for data transfers and what happens when sensitive data is exposed or the API is hacked are important within the data sharing debate, but would involve further considerations on data protection law, cybersecurity, liability and cross border enforcement that are beyond the scope of this paper.

9 Our original intention was to assess data interoperability in all regulatory interventions of the EU legislature, which have generated either data governance obligations or data access rights for private actors.[11] However, while we engaged in this endeavour, we realized we needed to take a prior step. That is, to conceptualize data interoperability within the data sharing framework. As a result, this first paper answers the question of when and how data interoperability[12], as a precondition to data

and search advertising markets and to remedy the competitive harms. < https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws> (accessed 13.09.2020).

8 Gaia-X: A Federated Data Infrastructure for Europe, <https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html> (accessed 13.09.20).

9 For a detail study on data standardization, Michal Gal, Daniel Rubinfeld "Data Standardization" NYU Law Review (2019) 738-769.

10 On adverse effects of extensive data sharing see e.g. Jörg Hoffmann, Safeguarding Innovation through Data Governance Regulation: The case of Digital Payment Services (2020) 21-25 with further references.

11 This assessment is developed in a second paper to be published soon.

12 Data interoperability is also considered as a precondition for open data. Cf. Laura DeNardis (ed.) "Opening Standards. The Global Politics of Interoperability" (MIT Press 2011).

quality, should be addressed by the legislature and whether amendments in the respective IP and trade secret regimes are necessary.

10 Our conceptualization consists of the following: (1) understanding the notion of interoperability in the current data access and data governance frameworks; (2) comprehending the different technical interoperability solutions; and (3) assessing the existing legal framework pertaining IP rights and trade secrets that may hinder data interoperability in this context.

11 The paper continues with an analysis of whether a more normative approach toward data interoperability could truly help fostering data re-use and thus the full realization of the data economy. We build on the assumption that interoperability should not become another policy on its own. Data interoperability should be considered as a part of a broader data sharing and access discussion and it should always reflect on the positive and adverse effects alike in order to reconcile the different interests implied.

B. Clarifying terms: Interoperability and its enablers, data standardization and APIs

I. Looking for a definition of interoperability

12 Interoperability, like openness, is something that we generally think of as a "good thing". Yet, an extensive review of definitions in technology, business, policy and legal literature, even of case studies, reveals that there is not one acceptable uniform definition of interoperability. This may bear certain risks with regard to already or future legislative action in this field. As data interoperability and data access are inherently tangled, the use of one or another definition of interoperability might affect the concrete data access regime.

13 Generally speaking, interoperability is a technical mechanism for computing systems to work together – even if they are from competing firms.[13] Yet, one can find several definitions for interoperability in the fields of engineering and computer science literature. Among them, the joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) defines interoperability as '*the capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units.*'[14] It means that interoperability aims to achieve the harmonious working of heterogeneous software products and services that make up the ICT infrastructure, but the needs for interoperability extend beyond this sector.

14 In an even broader view, interoperability is defined by the Institute of Electrical and Electronics Engineers (IEEE) as '*the ability of two or more systems or components to exchange information and to use the information that has been exchanged.*'[15] Most recently, in the IoT context, interoperability has been defined as the ability of two systems to communicate and share services with each other.[16]

15 From a more general perspective, the Oxford Dictionary gives a definition for interoperability as '*ab[ility] to operate in conjunction*'. This implies that two interoperable systems can understand one another and use the functionality of each other. From a policy perspective, the Data Commons Framework developed by the Berkman Klein Center does not precisely define interoperability but rightly divides it in different layers: technology, data and format, human and institutional, and organizational, which all imply a certain degree of data standardization.[17]

16 The EU legislature defined the concept of interoperability for the first time in Recital 12 of the Computer Programs Directive as '*the ability to exchange information and mutually to use the information which has been exchange*'. Some scholars have rightly emphasized that this concept of interoperability as isolated policy on compatible computer programs might no longer be applicable[18]; for instance if we

13 Ian Brown, "The technical components of interoperability as a tool for competition regulation" (Preprint 12 October 2020), 3.

14 ISO/IEC 2382-1:1993 Information Technology – Vocabulary – Part 1: Fundamental terms. International Organization for Standardization (ISO)" < http://www.iso.org/iso/catalogue_detail.htm?csnumber=7229> (accessed 13.09.2020).

15 IEEE, "Standard Glossary of Software Engineering Terminology" (1990) Doc IEEE Std 610121990, 3.

16 Jussi Kiljander et al, "Semantic interoperability architecture for pervasive computing and internet of things" (2014) IEEE Access 2, 856–873.

17 Elena Goldstein, Urs Gasser, and Ryan Budish, "Data Commons Version 1.0: A Framework to Build Toward Al for Good" (2018) <https://medium.com/berkman-klein-center/data-commons-version-1-0-aframework-to-build-toward-ai-for-good-73414d7e72be> (accessed 13.09.2020).

18 Michael Anthony C. Dizon, "Decompiling the Software Directive, the Microsoft CFI Case and the i2010 Strategy: How to Reverse Engineer an International Interop-

are talking about sharing services over a software system as in the IoT context.

17 The European Commission Expert Report 'Competition policy for the digital era' [19] defines three different types of interoperability. 'Data interoperability' is according to the report *equivalent to data portability but with a continuous potentially real time, access to personal or machine user data.*[20] 'Protocol interoperability' refers to *the ability of two services or products to interconnect, technically, with one another.*[21] 'Full protocol interoperability' refers to '*standards that allow substitute services to interoperate, e.g. messaging systems'.*[22]

18 Furthermore, the interim report on digital advertising by the United Kingdom's Competition and Markets Authority (CMA) coined the term 'content interoperability' as '[the] *ability to post content across several platforms simultaneously; the ability to view posts from friends on other social platforms; and how the standards surrounding these features should be developed and monitored.'* [23]

19 This vast number of definitions shows that there is no one-size fits-all definition of interoperability[24], rather it is a very context-specific concept that crosscuts a wide spectrum of laws, policies and technologies, where standards play a prominent role.

20 One common point of all the previous definitions is that interoperability always denotes the ability of either a system, a product, or a service to communicate and function with other technically different systems, products, or services. Consequently, one of its primary benefits is that interoperability can preserve key elements of alternative technical solutions and thus innovation and competition while ensuring that systems work together. However, one of the tricks to the creation of interoperable systems, products and services is to determine what the optimal level of interoperability will be: in what ways should the systems, products and services work together, work across, and in what ways should they not?[25]

21 The norm in the software industry has been to build distributed systems[26], which normally began as fully compatible or interoperable. Yet the bigger the firms grow, the less interoperability they allow to better reap network effects and to better foreclose others.[27] Designing decentralized or distributed systems are more burdensome, as they require high levels of coordination and investment and involve the setting of standards in collaboration.[28] However,

erability Regime" (2008). Computer and Telecommunications Law Review, Vol. 14, p. 213 Available at SSRN: <https://ssrn.com/abstract=1407131>; Wolfgang Kerber, Heike Schweitzer, 'Data Interoperability in the Digital Economy' (2017), JIPITEC 8 (1); Begoña González Otero, *Interoperabilidad, Internet de las Cosas y Derecho de Autor*, (2019) Reus, Madrid.

19 Jacques Crémer, (n. 6).

20 Ibid, 58. This definition can be misleading, as data portability is a right and should not be mixed with the concept of data interoperability, which in principle is technical.

21 Ibid.

22 Ibid.

23 Competition and Markets Authority (CMA) "Online Platforms And Digital Advertising, Market Study Interim Report" (2019), 26 < https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pdf>; (accessed 13.09.2020).

24 John Palfrey and Urs Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems*, Basic Books (2012) Introduction.

25 John Palfrey, Urs Gasser, *Interop* (2012), p 11.

26 See among others: Timothy F. Bresnahan, Shane Greenstein "Technological Competition and the Structure of the Computer Industry" The Journal of Industrial Economics (1999) 47(1), 1; Lawrence A Sharrott, "Centralized and Distributed Information Systems: Two Architecture Approaches for the 90s." in M.J. Ball et al (eds) *Healthcare Information Management Systems. Computers in Health Care*. Springer (New York, 1991).

27 This was pointed out already in the explanatory memorandum of the Computer Programs Directive Proposal when referring to the production of inter-operative systems. See European Commission, Proposal for a Council Directive on the legal protection of computer programs (1989) COM(88) 816 final, 3.11. See also Michael Katz, Carl Shapiro, "Systems Competition and Network Effects" Journal of Economic Perspectives, Vol 8 – 2 (1994), 93–115. Joseph Farrell and Timothy Simcoe, 'Four Paths to Compatibility', *The Oxford Handbook of the Digital Economy* (Oxford University Press 2012). Cory Doctorow, "Adversarial Interoperability: Reviving an Elegant Weapon from a More Civilized Age to Slay Today's Monopolies" EFF Deeplinks (2019) <https://www.eff.org/es/deeplinks/2019/06/adversarial-interoperability-reviving-elegant-weapon-more-civilized-age-slay> (accessed 13.09.2020).

28 Hadil Abukwaik, Davide Taibi, and Dieter Rombach, "Interoperability-Related Architectural Problems and Solutions in Information Systems: A Scoping Study" in P. Avgeriou and U. Zdun (eds.) ECSA Proceeding, LNCS 8627, 308–323 (2014). Chris Gebhardt, "Decentralized Information and the Future of Software – Draft" (2019) <https://infocentral.org/

the building of decentralized and distributed systems keeps gaining traction as it is essential for the deployment of working IoT technologies. The firm needs to balance relevant considerations because allowing for ample interoperability might entail losing the firm's competitive advantage, while overly restrictive access will struggle to engage with users of the system.

22 Similar considerations apply to products and services. On the product level, the idea of "device neutrality" arose a few years ago as an essential freedom of users to access digital content and use the applications and operating systems they wish.[29] This means a dissociation of operating systems from devices, which requires device (data) interoperability. The provision of digital services implies the electronic delivery of information, including data and content across multiple platforms and devices like web or mobile. Interestingly, in the field of services, an industry consortium, the Web Services Interoperability Organization, was founded in 2002 and chartered to promote interoperability among the digital services provided across the web.[30]

II. Conceptual frameworks

23 Conceptual frameworks help us to consider interoperability in different contexts and from different perspectives.[31] It is particularly relevant to understand what syntactic and semantic interoperability are. Overall, because they are like magnetic poles. It is hard to encounter one without the other.

24 Syntactic interoperability refers to interoperation of the format, as well as the data structure used in any exchanged information or service between heterogeneous entities.[32] An interface needs to be defined for each resource, exposing some structure according to some schema. Web Service Definition Language (WSDL) and RESTful designed APIs are examples. The content of the messages needs to be serialized to be sent over the channel and the format to do so (such as XML or JSON). The message sender encodes data in a message using syntactic rules, specified in some grammar. The message receiver decodes the received message using syntactic rules defined in the same or some other grammar. Syntactic interoperability problems arise when the sender's encoding rules are incompatible with the receiver's decoding rules.[33]

25 Semantic interoperability as defined by the World Wide Web Consortium (W3C) refers to the "*enabling of different agents, services, and applications to exchange information, data and knowledge in a meaningful way, on and off the web*"[34] The Web of Thing (WOT) addresses the current fragmentation within the Internet of Things by exposing things and systems data and metadata through APIs. But such efforts have been hampered because the corresponding parties need to exchange information about certain aspects –i.e. the disclosure of specifications or the explanation of an implementation - of an API[35] and

drafts/DecentralizedInformation.html#monetization-and-incentives> (accessed 13.09.2020).

29 The idea was first proposed in 2014 by a member of the Italian Parliament, who proposed a law that should include the users' freedom to access content and use the applications they wish, provided they are legal, they do not impair safety and security, and they are not in violation of other laws or court orders. A limitation of this freedom by device manufacturers should be examinable on the grounds of anti-consumeristic behavior. See: Mastrolonardo, Raffaele. "Net neutrality could become law in Italy - unless internet users would rather opt out", ZDNet <https://www.zdnet.com/article/net-neutrality-could-become-law-in-italy-unless-internet-users-would-rather-opt-out/> (accessed 13.09.2020). Later, the Body of European Regulators for Electronic Communications (BEREC) published the report "On the impact of premium content on ECS markets and the effect of devices on the open use of the Internet"(2018) < https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8013-berec-report-on-the-impact-of-premium-content-on-ecs-markets-and-the-effect-of-devices-on-the-open-use-of-the-internet> (accessed 13.09.2020). Similarly, the French peer, l'Autorité de régulation des communications électroniques et des Postes (ARCEP) published a report "Smartphones, tablets, voice assistants-Devices:weak link in achieving open internet access" (2018) <https://archives.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf> (accessed 13.09.2020).

30 <https://en.wikipedia.org/wiki/Web_Services_Interoperability> (accessed 13.09.2020).

31 Among the latest: European Interoperability Framework, SWD (2017) 112 final, Annex to EC European Interoperability Framework – Implementation Strategy, COM (2017) 134 final, 18 to 28; New European Interoperability Framework (EIF), 2017, 21 to 32. Available at: https://ec.europa.eu/isa2/eif_en (accessed 13.09.2020).

32 Magdha Noura, Mohammed Atiquzzaman and Martin Gaedke, "Interoperability in Internet of Things: Taxonomies and Open Challenges" Mobile Netw Appl 24 (2019) 799.

33 Ibid.

34 W3C, "W3C Semantic Integration & Interoperability Using RDF and OWL" (2001) https://www.w3.org/2001/sw/BestPractices/OEP/SemInt/, (accessed 13.09.2020).

35 Martin Bauer et al, "Semantic Interoperability for the Web

non-technically spoken, many devices do not speak the same language and cannot exchange across different gateways and smart hubs.[36] If the data generated by systems and products have a defined data format, but the data models and schemas used by different sources are dissimilar, not always compatible, and data representation is not consistent, data communication will not work.

26 In the context of data sharing, semantic interoperability plays a key role. It is essential for the efficient use of data and for enabling data driven innovation. Data driven innovation builds on the information in the data. Not any data server or constitute data driven innovation, but only information that is implemented on a knowledge level. This already requires syntactic interoperability, which depends on a certain degree of semantics to allow for access and a certain degree of communication. Moreover, the more interoperability of products and services throughout different sectors is demanded, the higher the need for semantics is. With semantic interoperability in place, various corporate data governance systems may work seamlessly together – decreasing cost that may arise due to a lack of interoperability and thus further incentivizes data sharing.[37] Potential reuse of an already existing technical solution together with less data interoperability conflicts. However, semantic interoperability, seems to not be sufficiently addressed in the current regulatory framework of data governance regimes.

III. Enablers of data interoperability

27 The main technical enablers to achieve syntactic and semantic interoperability are the following: data standardization and application programming interfaces (APIs). There is a key difference between them. Namely, when a firm chooses one or the other enabler this has important consequences from a competition and innovation perspective. APIs represent an endpoint interface and are usually designed unilaterally by the owner of the system, product or service; they are not a give-and-take agreement and do not require full disclosure.[38] On the other hand, data standardization such as data models, data formats or protocols, require the agreement of the parties involved, therefore, collaboration and disclosing of information is required.

28 From a data standardization perspective, data formats relate to the organization of information according to pre-set instructions,[39] while data models are conceptual representations that help in the visual representation of the information contained in data.[40] In principle, data formats better serve to achieve syntactic interoperability, while data models work for both syntactic and semantic interoperability. More metaphorically put, a data model is as the architect's building plan while the format is the type of bricks used. A data communications protocol deals with the rules for the transmission of data between two or more points (or nodes, as they may also be called).[41] Central to

of Things" (2016), doi: 10.13140/RG.2.2.25758.13122

36 Maria Shiao, "Internet of Things. Standardisation and Architectures. Workshop Report" (2015) European Commission, 4, < https://ec.europa.eu/digital-single-market/en/news/standards-and-architecture-iot-path-convergence-main-outputs-workshop-iot-standardisation-and > (accessed 13.09.2020).

37 See for instance the 2020 guidelines "Interoperabilität durch standardisierte Merkmale" (Interoperability by standardized properties) of the German Mechanical Engineering Industry Association (Verband Deutscher Maschinen-und Anlagenbau – VDMA), which are based on the creation of common semantic attributes and data models. More information at: https://www.vdma.org/v2viewer/-/v2article/render/39746287 (accessed 13.09.20).

38 Therefore, they should not be conceptualized as data standards. Cf. Michal Gal, Daniel Rubinfield "Data Standardization" NYU Law Review (2019) 750 referring to Oscar Borgogno, Giuseppe Colangelo "Data Sharing and Interoperability: Fostering Innovation and Competition Through APIs" Computer L. & Security Rev. (2019) 8, stating that the most commonly used data standards are Application Programming Interfaces (APIs).

39 A significant challenge for data formats relates to how the structure and description of data and metadata (data about data, such as the author or producer of the dataset and the date the data was produced) can be organized consistently. See Luis González Morales, Tom Orrell "Data Interoperability: A Practitioner's Guide to Joining Up Data in the Development Sector" (2018) 22. <http://data4sdgs.org/resources/interoperability-practitioners-guide-joining-data-development-sector> (accessed 13.09.2020). See also: Daan Broader, Dieter van Uytvanck, "Metadata Formats" in *The Oxford Handbook of Corpus Phonology* (Oxford University Press, 2014).

40 See Amarnath Gupta, Data Model vs Data Format, Big Data Modelling and Management Systems, University of California in San Diego, available at: https://www.coursera.org/lecture/big-data-management/data-model-vs-data-format-xZmuD (accessed 13.09.2020).

41 An example is SOAP, a lightweight protocol intended for exchanging structured informationin a decentralised, distributed environment over a network. See W3C, "SOAP Version 1.2 Part 1: Messaging Framework" (Second Edition, 2007),< www.w3.org/TR/soap12/> (accessed 13.09.2020).

these rules is the concept of layers. Protocol layers were conceived in order to divide the duties of a protocol into manageable chunks.[42]

29 APIs are a type of computer program interface consisting of sets of functions, procedures, definitions and protocols for machine-to-machine communication and the seamless exchange of data. Conceptually APIs can be divided into "specifications" and "implementations". Specifications are made of declaring code, but they do not instruct a computer to do anything. Implementations are a set of step-by-step instructions to be used directly or indirectly in a computer in order to bring about certain result.[43]

30 The expansion of cloud computing brought about the rapid development and adoption of a technology referred to as web services. Web services stands as a key technology in terms of allowing computers to communicate machine to machine, server to server and to exchange data. The W3C has defined web services as a software system designed to support interoperable machine-to-machine interaction over a network.[44] Web services technology has transformed digital services. Amazon Web Services (AWS)[45] is the first reference that might come to mind, but all existing digital platforms use web services.[46] A key feature of web services is the degree of interoperability they offer, so that applications can be written in various languages and are still able to communicate by exchanging data with one another, server to server.[47]

31 Looking at the definition of web service (a software system designed to support interoperable machine-to-machine interaction and exchange of data over a network), one might correctly assume that they resemble the definition of APIs (software interface designed for machine-to-machine communication and the seamless exchange of data). Most specialists say that web services are a type of API, which can only be accessed through a network connection.[48] Yet, not all APIs are web services. APIs can be on- or offline. Another central difference is that APIs can utilize any kind of communication convention (communication agnosticism) while web services are restricted. A web service developer has more restrictions in terms of design. However, an API developer can utilize different tools to make its program simpler and less complex or the other way around. Thus, APIs can utilize any kind of communication convention and are not as restricted as a web service is.

32 Maybe that is the reason why a majority of firms providing web services have decided to unilaterally design their own APIs for their web services. These are the so-called "Web-APIs" [49] which allow for data exchange machine-to-machine (or as the Open Data Directive refers to "dynamic data" made available via APIs).[50] The primary intent of web APIs is to exchange (or even modify)[51] data between software systems. Web APIs, same as APIs, can be open or restricted.

33 From a data interoperability perspective, it is relevant to see how much web APIs design rely on semantics. The two mostly spread designs are the SOAP specification (Simple Object Access Protocol) and the

42 Edward Insam, *TCP/IP Embedded Internet Applications* (Elsevier, 2003) 55.

43 Brief Amici Curiae of 83 Computer Scientists in Support of Petitioner, No. 18-956 (2020) 7. Available at <https://www.supremecourt.gov> (accessed 13.09.2020).

44 See <https://www.w3.org/TR/ws-gloss/> (accessed 13.09.2020).

45 Amazon evolved from selling books, to selling a much more diverse set of goods, to needing an (internal) platform supporting the provisioning general purpose network and compute resources necessary to support the development of an (external) platform that facilitated third party sellers' access to Amazon's global market presence. For further details see Jon Swartz, "How Amazon created AWS and changed technology forever" Market Watch (2019) < https://www.marketwatch.com/story/how-amazon-created-aws-and-changed-technology-forever-2019-12-03> (accessed 13.09.2020).

46 GoogleSearch API is another example of Web services.

47 Marshall Breeding, "Introduction to Web Services" Library Technology Reports (2006) < https://journals.ala.org/index.php/ltr/issue/view/152> (accessed 13.09.2020).

48 See <https://blog.thedigitalgroup.com/api-vs-web-service-understanding-the-difference>; < https://nordicapis.com/what-is-the-difference-between-web-services-and-apis/#:~:text=There%20you%20have%20it%3A%20an,all%20APIs%20are%20web%20services.> (accessed 13.09.2020).

49 See <https://en.wikipedia.org/wiki/Web_API> (accessed 13.09.2020).

50 See Art. 2 (8) and Recitals 31 and 32 of the Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, ELI: http://data.europa.eu/eli/dir/2019/1024/oj.

51 "Operations to modify data are a core part of the Web API. In addition to a simple update and delete, you can perform operations on single attributes and compose upsert requests that will either update or insert an entity depending on whether it exists". See < https://docs.microsoft.com/en-us/powerapps/developer/common-data-service/webapi/update-delete-entities-using-web-api#:~:text=Operations%20to%20modify%20data%20are,depending%20on%20whether%20it%20exists.> (accessed 13.09.2020).

REST principles (Representational State Transfer). Web-APIs adhering to the SOAP specification[52] facilitate exchanging structured information in a decentralized, distributed environment. Even if the World Wide Web infrastructure is distributed, as indicated earlier, decentralized and distributed system infrastructures require higher investments than centralized ones due to their complexity.[53] The REST principles appeared as a more flexible approach to build lightweight and fast web and mobile applications and gained popularity over SOAP.[54] REST architecture relies on the idea that any API or web API must comply with certain principles to be certified as "RESTful".[55] Such design principles or constrains are highly based on data semantics to ensure that the API is predictable and easy to understand and use by a third party invoking it.[56] These design principles also implied the idea of disclosing information, as the API documentation (the specifications) to be RESTful needs to be easily accessible and comprehensible by other firms. The "Unified API" by the City of London Railway[57], the use of "REST" APIs[58] by several municipal public transport providers[59], the "RESTful" API of UBER[60] are examples. In the last two years, another design approach is increasingly being adopted by firms and developers. Instead of using a data protocol or a set of design principles, GraphQL is an open-source data query and manipulation language (a syntax) that describes in steps how to ask for data from the API, preventing excessively large amounts of data from being returned.[61]

34 All these approaches toward effective design of web APIs, by which their main function is data communication machine-to-machine, clearly shows how important and complex the achievement of high levels of semantic data interoperability is. This also becomes necessary for effective data access and reliable data sharing. However, this does not mean that web APIs or APIs based on the principle of any of these designs are open by default. APIs, as it happens with software, offer the dual virtues of practical modular design and precise metering of access.[62] They have become the foundation of almost any digital infrastructure and a critical facilitator for data interoperability –besides data standardization.

52 The SOAP specification was initially designed as SOAP was designed as an object-access protocol by Microsoft and IBM. However, later on it became the underlying layer of a more complex set of web services. For further details see https://en.wikipedia.org/wiki/SOAP (last accessed 12.08.20).

53 For a comparison between centralized, decentralized and distributed systems see: < https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/> (accessed 13.09.2020). On the relationship between federation, distribution and decentralization, see: Gaia-X: Technical Architecture (2020) 23 < https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical-architecture.html> (accessed 13.09.2020).

54 For differences between SOAP and REST see: < https://testautomationresources.com/api-testing/differences-web-services-api/> (accessed 13.09.2020).

55 Representational State Transfer (REST) are a set of design principles presented by Roy Fielding in his PhD "Architectural Styles and the Design of Network-based Software Architectures" in 2000. <https://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm> and <https://restfulapi.net/> (accessed 13.09.2020).

56 Ruben Verborgh, Andreas Harth, Maria Maleshkova et al. "Semantic Description of Rest APIs", available at: https://tomayac.com/papers/semantic_description_of_rest_apis.pdf (last accessed 12.08.20). See also: https://dzone.com/articles/rest-its-all-about-semantics (last accessed 12.08.20.) and https://scotch.io/bar-talk/designing-a-restful-web-api#:~:text=REST%20is%20basically%20a%20list,easy%20to%20understand%20and%20use.&text=Semantics%2C%20semantics%2C%20semantics%3A%20The,Status%20Codes%20and%20HTTP%20Authentication) (last accessed 12.08.20).

57 See: https://tfl.gov.uk/info-for/open-data-users/unified-api#on-this-page-3

58 REST stands for representational state transfer.

59 Ably Hub, "The maturity of public transport APIs 2019" (2019). Available at: https://files.ably.io/research/white-papers/the-maturity-of-public-transport-apis-2019-ably-realtime.pdf. (accessed 13.09.2020).

60 See: https://developer.uber.com/ (accessed 13.09.2020).

61 It was built by Facebook and recently moved to the GraphQL Foundation, hosted by the Linux Foundation. For more details see: < https://graphql.org/learn/> (accessed 13.09.2020).

62 Seth G. Benzell, et al. „The Paradox of Openness: Exposure vs. Efficiency of APIs" <http://ide.mit.edu/sites/default/files/publications/The%20Paradox%20of%20Openness%208-3-19.pdf> (accessed 13.09.2020).

C. The role of data interoperability in data related market failures

35 Data interoperability is the key prerequisite for efficient data sharing and data driven innovation. Indeed, the expected economic and social benefits of data access and sharing are enormous. Data driven innovations have already transformed multiple sectors in the economy and are a new disruptive source of productivity growth.[63] In particular, the advanced use of data analytics and artificial intelligence enables undertakings to scale up their business at much lower costs than in analogue times.[64] Data are the essential inputs for AI applications. Even beyond productivity growth, a greater availability of data can create beneficial spill-overs.[65] Data also has a central role in online markets. Value creation is reinforced through a recursive data capture and data deployment feedback loop, which is enabled by machine learning (ML) technologies.

36 Amidst fierce global competition, AI has become – according to the European Commission - one of "the most strategic technologies of the 21st century".[66] The EC has already outlined the strategic role the right EU legal framework for AI should play in defining the future we would live in. It is thus of utmost importance that the EC pursues a strategic maneuver with regard to IP and data access innovation policies and AI. This already led to direct market interventions through data access, portability and data governance regulation - some still adhering to competition specific traditional refusal to deal considerations - together with data sharing remedies in both merger control and abuse of dominance cases. Moreover, there are private data sharing initiatives.

37 Yet, there is also a cost to data sharing and re-use. Private firms may incur costs when they share data with parties that can harm their interests. They take data sharing decisions in function of the expected benefits and costs.[67] Furthermore, other negative externalities may arise due to increased data sharing. This implies data protection and data security concerns but potential negative effects of data-induced distortions of competition.[68] Although increased data sharing may create both static and dynamic efficiencies, if it does not go hand in hand with data interoperability considerations, this may also create the ability for undertakings to enter into strategic market foreclosing behavior that bars others from market entry or may eventually lead to anti-competitive market concentrations, such as the so-called digital "gatekeepers" or data-opolies.[69]

38 Regulating data sharing and thus any attempts of the EU and its Member States to directly shape data driven innovation should still reflect on traditional market failure considerations stemming from economic normative regulatory theory. Markets are constituted by the consent of economic citizens to individual transactions and typically do not require centralized coordination in the sense of a centrally planned economy. The legal foundation of markets consists in the freedom-of-contract principle, which is safeguarded by competition law.[70] Decentralized decision making between the parties of the contract is to be favored because individual economic preferences of numerous economic agents would be outvoted in a centralized decision-making process, and this would contradict the principles of individual freedom and self-determination, which are also enshrined in Articles 6, 16 and 17 CFR.[71]

39 In order to assess market failure in data access cases,

63 According to one of the most recent studies conducted by the OECD, data access and sharing can help generate social and economic benefits worth between 0.1% and 1.5% of gross domestic product (GDP) in the case of public-sector data, and between 1% and 2.5% of GDP (in few other studies up to 4% of GDP) when also including private-sector data. See OECD, Enhancing Access to and Sharing of Data (2019), 60.

64 And this goes much beyond 'scaling without mass'. Cf. Erik Brynjolfsson and others, 'Scale Without Mass: Business Process Replication and Industry Dynamics' (2008) Harvard Business School Technology & Operations Management Unit Research Paper No 7/16.

65 OECD (n. 64), 64

66 European Commission, Communication on Artificial Intelligence for Europe (2018) COM(2018) 237 final, SWD(2018) 137 final, 1.

67 Bertin Martens, et al, "Business-to-Business Data Sharing: An Economic and Legal Analysis" (July 22, 2020) 5, <https://ssrn.com/abstract=3658100> (accessed 13.09.2020).

68 For an overview on potential adverse effects see Hoffmann (n. 10) 1-26.

69 See: Ariel Ezrachi, Maurice E. Stucke, "eDistortions: How Data-Opolies are dissipating the Internet's potential", in Guy Rolnik (ed.) *Digital Platforms and Concentration*, Stigler Center, University of Chicago Booth School of Business (2018), 5, <https://promarket.org/digital-platforms-concentration/> (accessed 13.09.2020).

70 Franz Böhm, *Wirtschaftsverfassung und Staatsverfassung* (1950), 50 et seq.; Böhm, 'Privatrechtsgesellschaft und Marktwirtschaft' (1966) ORDO 75, 92.

71 Josef Drexl, 'Competition Law as Part of the European Constitution' in Armin von Bogdandy and Jürgen Bast (eds) Principles of European Constitutional Law (2010) 633, 660.

one has to distinguish between personal and non-personal data. Whereas data protection laws may already create high hurdles for switching and create lock-ins, non-personal data cases – particularly in after-market constellations – need a different assessment. On the off chance that it goes to the question whether enough data is really utilized and re-used, the role data pools, data trusts and data marketplaces play as data sharers and data normalizers need to be taken into account.[72] Only if all of these options fail to provide for efficient data use, one may actually identify a market failure. Even though it seems that particularly large platform undertakings are systemically blocking access to data, this does neither mean that this conduct tantamount to an exploitative abuse case nor does it mean that any market operator is anti-competitively excluded from markets.[73] The current discussion on the planned European Digital Markets Act and the 10th Amendment of the German Antitrust Code are looking at both asymmetric access and interoperability obligations exclusively for the undertakings with paramount importance across markets, i.e. gatekeepers.[74]

40 Applying this principle of an open market and competition system to the question of how to regulate access to data and data interoperability, one should note that states should refrain from directly innovation-enabling *ex ante* regulation going beyond merely safeguarding the well-functioning of open competitive markets.[75] Market considerations build their assumptions on the fact that under conditions of effective competition, rule-based economic freedoms of action lead to results that correspond to positive general welfare effects.[76] One of the prerequisites of a competition system is the primacy of exclusivity and imperfect knowledge that is usually constituted by a property system or factual exclusivity combined with contractual freedoms. These are primary enablers of markets, framed by regulation, which safeguards freedom of competition.[77] Under these circumstances markets evolve spontaneously and usually regulate themselves.[78] Indeed, even though the current platform regulation debate is foreseeing stronger *ex ante* regulation against platforms with paramount importance across markets, competition –as institution – should still be the guiding principle for pro-innovation regulation. Competition serves as an incentive for innovation and a means to new discoveries.[79] Translated in the data context, some form of factual exclusivity of data is still a prerequisite for data specific markets and market force led data driven innovation. This also holds true under utilitarian incentive considerations. To this end, it should be kept in mind that data may have high economic and competitive value. Data may thus not only be valuable trade secrets, the aggregation of high value information and the inferred information in ML applications may provide huge competitive advantages. Factual exclusivity over valuable information may be one of the key competition parameters, could also serve as investment incentive, and may attenuate the relevance of IP protection from an AI perspective. Factual data exclusivity and expertise are the key competitive factors with regard to the development of AI.[80]

72 Cf. Heike Schweitzer, Martin Peitz, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf? (2017) Discussion Paper No. 17-043, ZEW, 4ff.

73 ibid. 5. Cf.

74 European Commission, "The Digital Service Act Package" (2020) < https://ec.europa.eu/digital-single-market/en/digital-services-act-package> (accessed 13.09.2020); European Commission, "Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the European Union's internal market, Inception Impact Assessment" Ref. Ares(2020)2877647 - 04/06/2020 (2020). The text of the German draft bill of 9 September 2020 (GWB10) can be found at <https://www.bmwi.de/Redaktion/DE/Downloads/G/gwb-digitalisierungsgesetz-referentenentwurf.pdf>, and English version can be consulted at < https://www.d-kart.de/en/blog/2020/02/21/draft-bill-the-translation/> (accessed 13.09.2020).

75 This applies to interoperability too. See Wolfgang Kerber, Heike Schweitzer, 'Interoperability in the Digital Economy' (2017) 8 JIPITEC 39, 1, 71-75.

76 Ernst-Joachim Mestmäcker, 'Europäische Wirtschaftsverfassung' (2009) EUP, 2.

77 Walter Eucken, Die Grundlagen der Nationalökonomie (1947, 9th ed. 1989), 256; Franz Böhm, Wirtschaftsverfassung und Staatsverfassung (1950), 50.

78 Friedrich August von Hayek, 'Der Wettbewerb als Entdeckungsverfahren, in: Freiburger Studien, Mohr-Siebeck, Tübingen (1969), 249 -265.

79 Even though there are different opinions on the question of how much competition is actually necessary to foster innovation, competition is still the allocation model in market economies. Cf. Kenneth J. Arrow, 'Economic Welfare and the Allocation of Resources for Invention' (1962) National Bureau of Economic Research, 'The Rate and Direction of Inventive Activity: Economic and Social Factors' 609, 620. Different opinions on this: Joseph Schumpeter, Theorie der wirtschaftlichen Entwicklung (1912), 157 and Aghion and Howitt, 'A model of growth through creative destruction' (1992), 60 (2), Econometrica, 323. Cf. DOJ (n. 7).

80 Reto M. Hilty, Jörg Hoffmann, Stefan Scheuerer, "Intellectual Property Justification for AI" (2020) available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539406>

41 Despite potential lack of data sharing, data commons or open data by default – comparable to Ostrom's 'commons'[81] considerations – should not be the guiding principle.[82] Indeed, similar to traditional 'service public' considerations in the utilities sectors, data has already widely been recognized as an infrastructure.[83] Such reasoning may provide for a justification for broader B2B data access regimes in the EU. Contrary to some (former) existent natural monopolies in the telecommunication or electricity sector however, there is typically no natural monopoly in B2B data specific markets that would justify a universal open data access regime. There are strong data network effects and data specific economies of scope. Yet, data need to have certain correlations in order to really provide for something new on the knowledge level and thus for constituting data driven innovation. Using completely randomized data to train a certain ML model, for example, will not improve its quality.[84]

42 Notwithstanding the potential positive effects of a lack of data interoperability, a simple access right that does not further reflect on modalities of the sharing of data within a broader data governance framework may fall short of remedying the identified market failure. Data lock-in scenarios may not be entirely solved by simply outlining the privately enforceable obligation of sharing of information in a processable and electronically readable, interoperable, format. In order to fully reap the advantages of data sharing without causing other negative externalities – particularly privacy and data security related – a broader regulatory approach is necessary. Thereby the transaction costs should also be explicitly considered and thus a public law approach dealing with non-waivable data interoperability obligations may be the favorable way forward.[85]

43 For instance, what the majority of governmental and academic studies about digital platforms have in common is that economies of scale and traditional and data-driven network effects not only have characterized the evolution of the online system, but also have led to the rise of key online gatekeepers with the potential to foreclose other market participants.[86] While such a dynamic is welcomed when it delivers greater efficiencies, innovation and quality, disruption is problematic when it challenges the boundaries of law, causing market distortions. In order to ensure a level playing field, there is a public interest in competition rules being applied equally to the market players. In this regard, data interoperability has the potential of becoming a distortion-preventing tool. Among others, the 2018 Study on Abuse for the German Ministry for Economic Affairs and Energy pointed out that digital markets have a tendency towards "tipping". Such a tendency is not natural but induced by individual practices, e.g. the obstruction to interoperability.[87]

44 All in all, outlining specific data access rights may not suffice for efficiently reaping the welfare enhancing effects of increased data sharing. To this end, data interoperability has its specific role to play. As efficient re-use of data depends to a high extent on data interoperability, a lack of interoperability or stand-alone interoperability regulation may already provide or hinder efficient data sharing and thus may either efficiently provide for a remedy for the data specific market failure or may prevent the adverse effects of excessive data sharing. Indeed, the negative externalities that come with increased sharing and use of data are typically addressed in specific legal regimes, respectively.[88] Yet, data

(accessed 13.09.2020).

81 Elinor Ostrom, *Die Verfassung der Allmende* (1999). Even there, one has to assess that efficient cooperation within commons systems only worked for smaller, very restricted cooperation mechanisms.

82 Hoffmann (n. 10), 16-18.

83 K.S. Rahman, 'Regulating informational infrastructure: Internet platforms as the new public utilities. Georgetown Law Technology Review 2, 234-252; Gintare Surblyte, 'Data as digital resource' (2016) Max Planck Institute for Innovation and Competition Research Paper No. 16-12, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849303> (accessed 13.09.2020), M. Janssen, S.A. Chun, J.R. Gil-Garcia Building the next generation of digital government infrastructures (2009) Government Information Quarterly, 26, 233-237.

84 Looking for structures and regularities in data is not enough to understand or acquire knowledge. Knowledge cannot be derived through induction alone; it requires a theory or a prior framework that can be tested. Humans necessarily predetermine this framework and thus data have to be related – at least to some extent. See R. Vigo, 'Complexity over uncertainty in generalized representational information theory (GRIT): A structure-sensitive general theory of information' (2013) 4 Information 1- 30, 4.

85 Cf. on high transaction costs in data trading, Schweitzer, Haucap (n. 72), 6.

86 Cf. (n. 6).

87 Heike Schweitzer, Justus Haucap, Wolfgang Kerber, Robert Welker "Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen" Projekt Nr. 66/17 (2018), 12.

88 For instance, the current discussion with regard to the European competition policy is focusing on further adapting competition laws for tackling (- or regulating) so-called undertakings with tantamount importance for competition across markets. This is currently discussed in Germany un-

interoperability, the scope and modalities of the data access right and other options of remedying the negative externalities should always be looked at together.

D. APIs: IP and Competition Law considerations

45 As we have seen, APIs are one of the technical means to facilitate data interoperability. This type of software interface has attracted a lot of attention in the last decades because free implementation of API specifications has been not only essential to realizing fundamental innovations in computing, it is also essential for efficient data sharing and thus data driven innovation. Any firm will be faced with competing options and will need to make trade-off decisions. To maximize the likelihood of an API project succeeding and minimize design delays, the firm should establish a set of guiding principles to address architectural preferences and delivery approaches, this means how to balance the dual virtues of a practical modular design and a precise metering of access. Consequently, APIs are instruments that allow for controlling follow on innovations not only in the software market but in any data-driven market that requires a network (web services or IoT) and the innovation capacities of whole data ecosystems and thus their monetization. In this context, there are three relevant questions that need to be addressed: first, the "appropriation" of APIs through IPRs, where the jurisprudence and academic debate on the copyright protection of APIs remains; second, what happens if a third party uses the underlying right when establishing data interoperability; and, third, to what extent the user of the API can rely on exceptions and limitations.

46 As to the "appropriation" of APIs, the first question that comes to mind is whether APIs can be the object of an intellectual property right. Copyright protection of APIs has drawn criticism for decades. The Computer Programs Directive makes clear that ideas and principles underlying any element of a computer program, including those which underlie its interfaces, are not protected by copyright.[89] Contrary to that, the expression of API specifications and API implementations, could qualify for protection as independent works subject to the originality threshold.[90] Even if the CJEU gave a purposive interpretation of the Directive so that the functionality of software interfaces (as it is the case with APIs) should not restrict interoperability[91], the question of protection of APIs as independent works of copyright remains unsettled. As some have rightly pointed out, while data and user interfaces are substantially different from APIs, the interpretation made by the CJEU would appear to offer ground in terms of reaching the conclusion that choices for interfaces concerning the implementation of abstract ideas contained in the source code can be sufficiently original, as were deemed to be those concerning languages or formats.[92]

47 Furthermore, web services can be considered a computer program that happens to also be an API. A web service, as said earlier, is a technology that accomplishes the task of communicating and exchanging data over a network between two machines. It is expressed in code. The "underlying" function of achieving the communication can be enabled via a web API or via other data standardization means – this is a design decision. Thus, in principle there is no merger between idea and expression. Web services as long as they are original, could be eligible for protection under the Computer Program Directive. In any case, since the Supreme Court of the US admitted the petition from Google in the (now) Google v. Oracle case, the discussion of potential copyright protection of APIs is back on the table.[93]

48 Regardless, having access to API information is of importance to competitors in software dependent markets. As a representative of the US government stated during the Microsoft case: "*[t]o control the*

der the draft of the 10th amendment of the German Antitrust Code for example.

89 Article 1(2) Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version), ELI: http://data.europa.eu/eli/dir/2009/24/oj. This was made clear by the CJEU both in 2010, case C-393/09, Bezpečnostní softwarová asociace - Svaz softwarové ochrany v Ministerstvo kultury [2010] ECLI:EU:C:2010:816, and 2012, case C-406/10, SAS Institute Inc. v World Programming Ltd [2012] ECLI:EU:C:2012:25.

90 Case C-393/09, *Bezpečnostní softwarová asociace - Svaz softwarové ochrany v Ministerstvo kultury* [2010] ECLI:EU:C:2010:816 para 41 – 43; Case C-406/10, *SAS Institute Inc. v World Programming Ltd* [2012] ECLI:EU:C:2012:259 para 35 and 39.

91 Case C-406/10, SAS Institute Inc (...) 39 and 46.

92 Nicolo Zingales, "Of Coffee Pods, Videogames, and Missed Interoperability: Reflections for EU Governance of the Internet of Things", TILEC Discussion Paper No. 2015-026 (2015) 10, https://ssrn.com/abstract=2707570, (accessed 13.09.2020).

93 *Google LLC v. Oracle America, Inc.*, U.S. docket number No. 18-956 (Nos. 2017-1118, 2017-1202 (Fed. Cir. Mar. 27, 2018).

interface specifications is to control the industry."[94] It is for this reason that the Computer Programs Directive provides for a limited exception to copyright infringement in the case of decompilation[95] performed to achieve interoperability. However, the Directive falls short of imposing a positive obligation to disclose interoperability information. At best, the Directive does not enable copyright holders to rely on their copyright and prohibit others from uncovering such information through decompilation when such information is not made available by the copyright holders themselves. Decompilation is a technically complex, costly and time-consuming reverse engineering technique that is best avoided where possible. Article 6 of the Directive codifies the legal position under EU law. It does not require the authorisation of the copyright holder where such action is '*indispensable to obtain the information* necessary *to achieve interoperability of an independently created computer program with other programs*'[96] The indispensability requirement restricts the scope of the copyright exception for the only purpose of achieving interoperability with an independently created program. Three additional conditions must be fulfilled for decompilation to be lawful. First, the performer must be a licensee or a lawful user of the software. Second, the information sought must not be available to the party carrying out the act through any other means (for instance, a refusal to license). Finally, decompilation must be restricted to the parts of the program necessary to achieve interoperability (which in principle might be very difficult to delineate for a third party).[97] An additional problem is that for interoperability to take place, the third party needs to exactly adhere to the relevant specifications and decompilation does not guarantee this. Furthermore, decompilation becomes futile if a computer program is provided as a service. Additionally, decompilation is totally useless if the owner of the API modifies the specifications relatively often, as tends to be the case.

49 Another IPR to consider as to the appropriation of APIs are patents. Under the European Patent Convention, computer programs 'as such' are excluded from patent protection.[98] However, the case law of the European Patent Office (EPO) and the examination guidelines that derive from this case law make it clear that this exclusion does not apply when the computer program has a technical character.[99] This limitation to the exclusion[100] is the narrow window through which software developers try to push their products to obtain a patent. Traditional APIs, which are part of a computer program, or when the computer program is embedded in a device, could easily be protected under a computer implemented implementation.[101] However, APIs could also be considered aspects of the computer program where the invention as a whole does not claim an abstract or non-technical subject matter. If only a portion of code from a computer program that relates to the computer-implemented invention has been used by an unauthorized party, it may not necessarily lead to patent infringement.

50 This might be more problematic in the case of web services as they are a type of technology which happens to also be an API. As in the case of computer programs, while each case depends on its own merits, there is a rather clear line to decide whether an invention has the required technical character: computer programs, or in this case a web service, are methods to accomplish tasks or solve problems (the communication and exchange of data over a network between two machines). As long as the method remains abstract, it cannot be patented under the rules of the EPC even if it runs on a computer. As soon as the method is put to specific, technical use, it will be treated just like any other solution for a problem and subjected to the further patent requirements of novelty and inventive step. This type of protection could be relevant for the webservice/API implementation, where the technical effect might take place. The specifications part, which is no more than declaring code, but it is the part that contains essential information for a third party if wants to invoke data interoperability, would not be covered by the scope patent. Conversely, API specifications would not be part of the patent application, nor will they be disclosed.

94 *United States v. Microsoft Corp.*, 87 F. Supp. 2d 30 (D.D.C 2000).

95 Decompilation is a reverse engineering technique that mainly consists of translating object code into source code.

96 Article 6 Directive 2009/24/EC on the legal protection of computer programs.

97 For a detailed assessment of Article 6 of the Computer Programs Directive see: Begoña González Otero *Interoperabilidad, Internet de las Cosas y Derecho de autor* (Reus, 2019) 232.

98 Articles 52(2) and (3) European Patent Convention.

99 Guidelines for Examination Part G II 3.6; EPO T 1173/97 and EPO G 3/08. The EPO assesses the technical effect without taking into consideration the prior art. Therefore, simply replacing a process or the acts of a human being, which are not considered to be technical, does not suffice to give the invention a technical character. See: EPO T 1227/05; EPO T 1784/06; EPO T 1370/11; EPO T 1358/09.

100 Limitation that one cannot explicitly find in the wording of the EPC.

101 Some examples of patents relating to computer program interfaces can be found in EPO Dec. T 2217/08 (Executable code/Microsoft) and T 1415/07 (Converting graphical programs/National Instruments).

In these cases, a reverse engineering exception for the purpose of achieving interoperability could help. Such an exception only exists in the text of the Agreement of a Unified Patent Court (UPC)[102], which entry into force is still unknown. Article 27 regulates the *'[L]imitations of the effects of a patent"* and its letter (k) states that *"the rights conferred by a patent shall not extend to any of the following: (k) the acts and the use of the obtained information as allowed under Articles 5 and 6 of Directive 2009/24/EC, in particular, by its provisions on decompilation and interoperability.'*

51 The main problem here is that, as explained above the decompilation exception is quite complex and, in the end, does not really guarantee that interoperability would be achieved. Additionally, a restrictive interpretation of this limitation in the field of patent brings two additional obstacles. First, only the acts and the use of the information obtained through reverse engineering techniques such a black box analysis[103] and decompilation[104] are regulated. The reason is obvious. Copyright protects the expression of the computer program, the code. Reproduction of the code is essential for the program to function. However, the underlying principles of the program, the ideas, fall out of the scope of copyright protection. For this reason, observation, studying and testing of the functioning of a program is allowed to a lawful user.

52 Nevertheless, if patent law needs to provide a limitation over the same acts, would this not mean that functions contained in the code of the program are given patent protection? Would this not be a tacit admission that computer programs "as such" could be within the scope of the patent? There is no need to provide a limitation over something that is already excluded of patent protection. Second, what happens with the acts and the use of information obtained through decompilation? In the copyright case, interoperability information discovered after decompilation can only be used for the creation of an independent program, which interoperates with the one decompiled. How Article 6 Computer Program Directive could be applied in the field of patent law is uncertain. What seems clear is that decompilation as such constitutes an infringement of the exclusive rights of reproduction and adaptation of the computer program (thus the copyright limitation); but in any case, decompilation of a computer program as such could constitute patent infringement. Therefore, how Article 27(k) UPC Agreement would apply to patent cases is extremely difficult to say. If it were merely meant to preserve and shelter the existing copyright limitations, it would seem redundant. If not, it gives more reasons for concern as it would constitute a limitation of which scope is decidedly unclear. On top of that, both possibilities bring a field of more potential national law fragmentation, decreasing the level of legal certainty.

53 Notwithstanding the fact that terms and conditions to access APIs are more often found in separate contractual annexes to software licenses, seems to suggest that protection of APIs under copyright or patent law is less and less reliable.

54 Without legal intervention, APIs specifications and API implementations need no disclosure and access to them needs to be requested on a contractual basis. APIs can be 'open' or 'restricted'. In the case of truly "open" API, any third party at any point, under any circumstances, is able to invoke it and the owner will strive to fulfil the request. APIs are often authenticated and typically limited both technically (amount of data transmitted) and through usage policies. Thus, no personal data or security breaches would be made available through an open API. Public-facing APIs are often documented exhaustively, as their primary added value for the system´s owner is in empowering third parties to deliver benefit to the platform by extension as it might encourage adoption.[105] This is not the case with restricted APIs, where the figure of trade secrets applies for the best candidate of the APIs' appropriation. Even if the European Trade Secrets Directive (TSD) is a new legal instrument, with very recent implementations by most Member States.[106] The definition of a trade secret provided by the TSD repeats the wording of Art. 39(2) TRIPS Agreement.[107] The protection of APIs specifications and implementations as trade secrets is a matter of fact.

102 Agreement on a Unified Patent Court, OJ C 175, 20.6.2013, p. 1–40.

103 Article 5 (3) Computer Program Directive.

104 Article 6 Computer Program Directive.

105 Chris Riley, Unpacking interoperability in competition, Journal of Cyber Policy, 5:1 (2020), 99.

106 At the EU level, the trade secrets civil legal protection was harmonised for the first time by the Directive 2016/943/EU on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition of the 8th June.2016.

107 Article 2(1) TSD: "'trade secret' means information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret".

55 From the perspective of a third party, there is normally no limitation on the use of the trade secret once lawfully attained and it is not feasible to differentiate between acquisition and use.[108] However, the TSD is even more restrictive than the decompilation exception of the Computer Programs Directive. It allows reverse engineering[109] where the acquirer is free from any legally valid duty to limit the acquisition of the trade secret.[110] The question is whether the restrictions on the use of information achieved via decompilation, imposed by Article 6 of the Computer Programs Directive could amount to a "legally valid duty" and this would take reverse engineering of a computer program to find its APIs out of the scope of Article 3 TSD. The novelty of the Directive and the actual absence of case law triggers uncertainty on this point.

56 Appropriation of APIs, due to network effects and switching costs, that acting together can cause market monopolization and thus consumer welfare loss, including spurring excessive marketing costs, increasing prices for consumers and increasing barriers to further innovation. On the other hand, one could consider that foreclosing API documentation may unlock downstream innovation and can seed the growth of competitors, but the platform owns the only master key. However, this argument is difficult to stand alone when potentially facing disruptive innovation options.[111] Restricted APIs clearly provide one more opportunity for lock in. This brings us to the refusal to deal cases where the question of using the information for the facilitation of vertical or horizontal interoperability becomes relevant for enabling intra-brand or inter-brand competition.[112] As already outlined above, interoperability has always played a peculiar role in this kind of case. However, access to API information might not always be indispensable when interoperability could be attained by other means, as the CJEU has also ruled.[113] Recently a refusal to deal case in Switzerland about data interoperability information provides a new court practice for these tensions between copyright and competition law.[114]

108 Roland Knaak et al, "Comment on the Max Planck Institute for Innovation and Competition on the Proposal for a Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure" IIC 45(8) (2014) 953, 961.

109 Article 3 (1) (b) of the TSD defines reverse engineering as observation, study, disassembly or testing of a product or object.

110 Article 3 (1) (b): "1. The acquisition of a trade secret shall be considered lawful when the trade secret is obtained by any of the following means: (b) observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret".

111 On the role of market concentration and innovation see Kenneth J. Arrow, 'Economic Welfare and the Allocation of Resources for Invention' (1962) National Bureau of Economic Research, 'The Rate and Direction of Inventive Activity: Economic and Social Factors' 609, 620. Different opinions on this: Joseph Schumpeter, Theorie der wirtschaftlichen Entwicklung (1912), 157 and Aghion and Howitt, 'A model of growth through creative destruction' (1992), 60 (2), Econometrica, 323. Joseph L. Bower and Clayton M. Christensen, "Disruptive Technologies: Catching the Wave." Harvard Business Review (1995) <https://hbr.org/1995/01/disruptive-technologies-catching-the-wave> (accessed 13.09.2020).

112 To ensure that their APIs are accessible, firms publish documentation outlining how their API is designed, what kind of information third parties can access, the manner in which they have to make the call to receive a reply, and the terms of use for the API *See, e.g.*, *Microsoft API and Reference Catalog*, Microsoft Developer Network, <https://docs.microsoft.com/en-us/previous-versions/iis/microsoft.web/microsoft-api-and-reference-catalog> (accessed 13.09.2020); *Google APIs Explorer*, Google, <https://developers.google.com/apis-explorer> (accessed 13.09.2020). Sadly, this documentation "is notoriously neglected and often out of date or incomplete, meaning the specifications that set forth purportedly permissible interactions may be incorrect, while other technically possible interactions could be undocumented. See Suzanne Van Arsdale and Cody Venzke, "Predatory Innovation in Software Markets", Harv. J.L. & Tech. 29 (2015) 243, 263 citing Ian Sommerville, *Software Engineering* (Addison-Wesley, 9th ed. 2011) 64. Documentation is often low priority, so emergency fixes may be made and forgotten, leaving documentation and code unaligned Sommerville at 239.

113 Case T- T751/15 *Contact Software* [2017] ECLI:EU:T:2017:602. The General Court also upheld that Article 102 was not applicable because Contact Software's claimed need for direct access to interoperability information failed to satisfy the indispensability requirement, as Contact Software's customers could obtain the interface information through a licensing process. However, what is interesting is the assessment of the Court on the relevance of achieving interoperability as to fulfil the indispensability requirement. The Court found that other PDM software vendors (competing with Contact Software) had stated that even without the interface information for CAD software products, they nonetheless reached an interoperability degree of 8/10. The GC agreed with the Commission that this demonstrated that the interface information was not indispensable for Contact Software to compete on the PDM software market.

114 Bundesverwaltungsgericht, B-831/2011, decision of 18 December 2018, < https://www.bvger.ch/bvger/de/home/medien/medienmitteilungen-archiv-2002---2016/medien-

The decision analyses the relationship of these two legal regimes with respect to decompilation of data interfaces in the credit/debit card payment transactions systems.[115] The Swiss Court, in balancing the interests in conflict, prefers a narrow interpretation of the scope of copyright while prominence is given to fair competition. The Federal Court upholds that the principles of the Swiss Cartel Act and the specific provisions of the Copyright Act codifying the decompilation exception to computer programs[116] aim at the same objective, therefore the copyright holder should support decompilation when it has pro-interoperability effects. This seems to go even far beyond the Microsoft case.

57 In any case it should be borne in mind that the usefulness of APIs as enablers of interoperability for the firm depends on how to balance the dichotomy of modularity design and access control. This assessment should duly reflect on the fundamental freedom of any firm to freely conduct their business.[117]

58 On a more radical approach, some have proposed the mandatory opening of APIs in order to reap the entire potential of data driven innovation, completely negating potential utilitarian incentive considerations with regard to the exclusivity and/or excludability of the information in order to safeguard investment protection of firms.[118] Therefore, parallel to considerations mentioned above, proposals for mandating the openness of APIs should be taken with due caution. Furthermore, API adoption is endogenous and according to recent policy reports, is still relatively new for most organizations, with more than half of the organizations only starting to create APIs in the last five years.[119] As shown previously, the web API design styles used by the industry indicate that they are taking steps toward more data standardization, and this is supported by the increased adoption of the OpenAPI specification[120], a broadly adopted industry standard for describing APIs created by a consortium of industry experts.[121] Yet, this will bring interoperability through standardization considerations to the table, with its benefits and costs.[122] Furthermore, there are also aspects of API standardization, such as data format standardization and semantic similarity of data that become relevant in this context and which are not sufficiently addressed.

59 Additionally, APIs normally come with a license contract that enshrines the terms and conditions under which access to the API, to the interface specifications and further additions can be used by developers. From a legal perspective, the legal framework pertaining the licensing contract is thereby relevant and also requires reflection.

60 Lastly, from a competition economics perspective, another issue needs further reflection. The current context of competition law practice builds on the assessment of legal contracts governing prices and terms of deals between undertakings. Highly trained lawyers and judges understand the relevant nuances and can compare them to existing precedents. Yet, determining whether a change to the permissions and usage policies of an API constitutes a thoughtful response to a legitimate security concern, or an anti-competitive act designed to foreclose a competitor, is a different challenge. For instance, assessing whether standardized APIs, working as plug-and-play could inadvertently allow the API provider to get access to additional information from the party

mitteilungen-2019/sanktion-gegen-six-group-bestaetigt.html > (accessed 13.09.2020).

115 For a detailed analysis of the decision see Rolf Weber, "Data Interfaces: Tensions between Copyright and Competition Law – A New Swiss Court Practice for an Old Problem" GRUR Int. 69(2) (2020) 119-127.

116 Article 21 of the Swiss Copyright Act codifies a broader decompilation exception than the one of the Computer Programs Directive: *"Art. 21 Entschlüsselung von Computerprogrammen (1) Wer das Recht hat, ein Computerprogramm zu gebrauchen, darf sich die erforderlichen Informationen über Schnittstellen zu unabhängig entwickelten Programmen durch Entschlüsselung des Programmcodes beschaffen oder durch Drittpersonen beschaffen lassen. (2)Die durch Entschlüsselung des Programmcodes gewonnenen Schnittstelleninformationen dürfen nur zur Entwicklung, Wartung sowie zum Gebrauch von interoperablen Computerprogrammen verwendet werden, soweit dadurch weder die normale Auswertung des Programms noch die rechtmäßigen Interessen der Rechtsinhaber und -inhaberinnen unzumutbar beeinträchtigt werden".*

117 Article 16, 6 CFR. .

118 Oscar Borgogno, Giuseppe Colangelo, "Data sharing and interoperability: Fostering innovation and competition through APIs", Computer Law & Security Review 35(5) (2019) https://doi.org/10.1016/j.clsr.2019.03.008.

119 Smartbear, "The State of API Report "(2020) < https://static0.smartbear.co/smartbearbrand/media/pdf/smartbear_state_of_api_2020.pdf > (accessed 13.09.2020).

120 In 2020 OpenAPI continues as a dominant API standard, with a dramatic growth for GraphQL as preferred design approach. See (Smartbear, "The State of API Report "(2020) < https://static0.smartbear.co/smartbearbrand/media/pdf/smartbear_state_of_api_2020.pdf > (accessed 13.09.2020).

121 It has an open governance structure under the Linux Foundation.

122 Cf. Wolfgang Kerber, Heike Schweitzer, "Data Interoperability in the Digital Economy" (2017), JIPITEC 8 (1), 6.

invoking the API. This could have adverse effects on competition. As this however ultimately depends on the technology itself, more research is needed.

E. Fostering re-usability of data with a normative interoperability approach

61 Interoperability has been a subject of vivid scholarly debate since the end of the 1980s.[123] It again gained traction in the current policy debate concerning the right legal framework for a data driven economy.[124] The digital package published by the European Commission last February, includes three strategic documents and in all of them, interoperability is mentioned as one of the key aspects.[125]

62 A year earlier, the European Commission released an Expert Report entitled "Competition policy for the digital era."[126] The report used the word 'interoperability' 105 times and defined three separate types of interoperability for purposes of understanding competition in the digital economy: "protocol interoperability", "data interoperability", and "full protocol interoperability". The interim report on digital advertising by the United Kingdom's Competition and Markets Authority (CMA) added another term: "content interoperability."[127]

63 Interoperability has often been used as buzzword and proclaimed as a 'Holy Grail' for benefiting from the expected welfare enhancing effects of increased data use. Yet, it is also commonly acknowledged that a lack of interoperability and certain bundling strategies of firms may also have certain welfare enhancing effects.[128] It also has to be noted that too much interoperability may have hidden costs and challenges for society that need to be thoroughly assessed and addressed.

64 As already outlined above, one of the broadest and fastest evolving discussions brought by the emerging data economy is the need for more data interoperability.[129] It can be found throughout the current policy discussions and legislative proposals regarding facilitating access to data either directly via competition law[130] and sector-specific data access regimes[131] or indirectly through improving data portability.[132] Moreover, the introduction of

123 See Frank Eliassen, and Jari Veijalainen, "A Functional Approach to Information System Interoperability", in Rolf Speth (ed.) *Proceedings EUTECO 88* Vienna (1988) 1121-1135.

124 It should be borne in mind that interoperability also applies to hardware, networking protocols and many other pieces of the information and communications technology stack. However, the greatest focus in current policy debates is on the software side, on the one hand looking at the services internet-connected layer, apps and social networks and the World Wide Web. On the other hand, as a data sharing enabler.

125 European Commission, Shaping Europe's digital future, Communication (2020) COM(2020) 67 final, A European Data Strategy, Communication (2020) COM (2020) 66 final, and White Paper on Artificial Intelligence Communication (2020) COM(2020) 65 final.

126 Crémer (n. 6).

127 Competition and Markets Authority (CMA) "Online Platforms And Digital Advertising, Market Study Interim Report" (2019) < https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pdf>; (accessed 13.09.2020).

128 Wolfgang Kerber, Heike Schweitzer, 'Data Interoperability in the Digital Economy' (2017), JIPITEC 8 (1).

129 Ibid.

130 See for competition policy Heike Schweitzer, (n. 87); Jacques Crémer, (n. 6); Philip Marsden (n. 6); Monopolkommission, "Control of abusive practices in the digital platform economy" in Biennial Report XXIII (2020).

131 The sectors with already existent data access regulations in place are the automotive, intelligent transport systems, gas metering and electricity sector. Commission Regulation (EC) 715/2007 [2007] OJ L171/1 as amended Regulation (EU) 595/2009 [2009] of 18 June 2009 on type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles (Euro VI) and on access to vehicle repair and maintenance information and amending Regulation (EC) No 715/2007 and Directive 2007/46/EC and repealing Directives 80/1269/EEC, 2005/55/EC and 2005/78/EC OJ L 188/1, smart metering information – Directive (EU) 2009/73 of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC [2009] OJ L211/94, electricity network data – Directive (EU) 2019/944 on common rules for the internal market for electricity and amending Directive 2012(27/27/EU [2019] OJ L158/125 or electricity transmission – Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation[2017] OJ L220/1, intelligent transport systems – Commission Regulation (EU)2015/703 of 30 April 2015 establishing a network code on interoperability and data exchange rules [2015] OJ L 113/13.

132 On the regulatory shortcomings of the data portability right of the GDPR see Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability as last revised and adopted on 5 April 2017' (16 EN, WP 242 rev.01); Com-

new consumer data rights, introducing portability rights for consumers - potentially also relating to industrial non-personal data - addresses the issue.[133] Even in solutions related to unfair commercial practices laws[134] – especially in cases of unequal bargaining power between the data claimant and the data holder, i.e. the refusal to grant access to certain data sets may be tantamount to unfair commercial practices – data interoperability needs to be considered.

65 Despite the ongoing and ever-growing discussion on creating (more) mandatory access and portability rights however, it is crucial to broaden the perspective from merely outlining the obligation to grant access to data. Even though the rights of others to access data or get their data ported correlate with the obligations of data-holders, merely outlining rights without clearly defining the scope of the right and performance needed, simply renders any data access regime insufficient. Therefore, mandatory access alone might not be sufficient for solving the current issues that arise with regard to the actual impediments of innovation and competition enabling function of increased data sharing. This can be seen in already existent data portability and access regimes and in the current debate pertaining digital services of platforms.

66 Taking the portability right under Article 20 (2), (1) GDPR as an example. There is a broad consensus that so far, the portability right does not lead to efficient solutions. The outlining of the right's scope is already unclear and too short-sighted, and it also insufficiently addresses large technical and other feasibility problems. Admittedly, it may be argued that Article 20 GDPR should not establish high regulatory entry barriers and may thus be a good first step towards breaking up consumer lock-ins. Yet, it also has to be kept in mind that the data portability right due to a lack of clearly outlining the modalities of the portability right simply creates too high transaction costs for consumers. Although it seems to be a common understanding that the data portability right encompasses neither the right for the portability of data in real-time nor does it entail interoperability requirements[135] for enabling the technical feasibility of data portability, the wording is simply not clear. Although Recital 68 refers to 'structured, commonly used, machine-readable and interoperable format(s)' one should bear in mind that recitals are not binding. It is therefore not surprising that the discussion is shifting to the question of how this data portability right in the GDPR can be improved in terms of efficiency.[136]

67 Another way interoperability finds the way in the legal sphere is via the scope of the access right itself. Such a right could entail certain technical interoperability obligations that data holders need to comply with in order to perform their access obligation. In the case of vehicle repair and maintenance information (RMI) for instance, the CJEU already ruled that the obligation to provide standardized access to RMI in a standardized format does not entail the obligation for car manufacturers to provide the information in amenable form to onward electronic processing.[137] The provided read-only access meets the requirement of 'unrestricted access in the form of a standardised format' outlined in Article 6 (1) Regulation (EC) No. 715/2007. The Court's interpretation of the access obligation enshrined in Article 6 (1) Regulation (EC) No. 715/2007 has an impact on the aftersales services markets. Access

mission, COM(2020) 66 final (n. 1) 10, 21; Inge Graef, Martin Husovec and Nicola Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German Law Journal 1356; Jacques Krämer, P Senellart and Alexandre de Streel, 'Making Data Portability more effective for the Digital Economy' (2020) CERRE report June 2020.

133 The concept of consumer data is strongly influenced by current regulatory endeavours in Australia, under which sector-specific access rights are defined parallel to horizontal regulatory approaches. See on the current discussion OECD, 'Consumer Data Rights and Competition - Background Note' (2020) DAF/COMP(2020) 1.

134 Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) JIPITEC 8 (4), 62,63.

135 The differences between data portability and data interoperability become clear when thinking about how competition emerges in practice. In particular, data portability does not port networks, only the personal data of the subject. Even if the user of a social network can port their "social graph" of connections to a competing service, one user only can't force all of his or her connections to also switch services. Data interoperability, with its real-time functionality, would overcome that gap by allowing users to send messages through the first and second platforms.

136 See for the discussion about the data portability right of the GDPR Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability as last revised and adopted on 5 April 2017' (16 EN, WP 242 rev.01); Commission, COM(2020) 66 final (n. 1) 10, 21. For a more recent discussions see Inge Graef, Martin Husovec and Nicola Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German Law Journal 1356; Jacques Krämer, Pierre Senellart and Alexandre de Streel, 'Making Data Portability more effective for the Digital Economy' (2020) CERRE report June 2020; Kommission Wettbewerbsrecht 4.0, 'Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft' (2019), 39-44.

137 Case- 527/18 Gesamtverband Autoteile eV v. Kia Motors [2018] ECLI:EU:C:2019:762.

to processable information is indispensable for independent suppliers of aftersales services. Without access to processable information on all components used by a manufacturer – containing for each spare part of the manufacturer the part number of their own compatible spare part – independent parts manufacturers can hardly provide repairers with alternative spare parts. On the case at hand, the provided access on the interface of the website displayed authorized original spare parts dealers only. This may eventually not only avoid market entry by independent spare part manufacturers, but independent repairers alike. This may also increase maintenance costs for consumers.[138] The narrow interpretation enables vehicle manufacturers to capture the spare parts hardware markets.[139]

68 Furthermore, data interoperability could become a legal tool for enabling data access in the realm of current the digital platforms debate. There seems to be a broad consensus among governmental[140] and academic studies[141] that the inclusion of asymmetrical interoperability obligations for dominant platforms (gatekeepers) could help to correct market foreclosures and information asymmetries. This is the approach followed by the European Commission in the Digital Services Act package, as to ensure that gatekeepers' platforms behave fairly and can be challenged by new entrants and existing competitors, so that consumers have the widest choice, fostering innovation and competition.[142]

69 However, the existence of already outlined private data access rights is not enough. A public law approach within the realm of a data governance solution seems more favorable. This is because of a lack of feasibility of enforcing the rights due to high transaction costs, legal uncertainty, technical impediments and opposing exclusive rights of others. Such a governance solution could also entail a more consistent solution to conflicting IP, database sui generis, and trade secrets protection in data, which is currently not thoroughly and clearly assessed either. Such conflicts need a more holistic assessment of overlapping exclusive rights and their re-usability options. As stated in the previous section however, solutions should still mirror traditional market failure considerations and need to align the different interests implied. Therefore, data interoperability should be treated only as a means to an end and not as an end in itself.

70 This holds particularly true as data standards and standardized ways of communication have still not reached high market penetration. The term data governance is already used as micro economic (corporate) data management concept concerning the capability that enables an organization to ensure that high data quality exists throughout the complete lifecycle of the data, and data controls are implemented that support business objectives.[143] The key focus areas of data governance include availability, usability, consistency, data integrity and data security, as well as establishing processes to ensure effective data management throughout the organization such as accountability for the adverse effects of poor data quality; lastly, ensuring that the data, which an organization has, can be used by the entire organization. Data governance strategies are ideally already incorporated at the organizational practices level. They contain a quality control discipline for assessing, managing, using, improving, monitoring, maintaining and protecting organizational information as a proper management system of data. This will not only lead to an increasing consistency and confidence in decision-making, it also maximizes the income generation potential of data (including the avoidance of data silos in different departments and business units, the reduction of errors in data sets and misuse of

138 Bertin Martens, Frank Müller-Langer, *Access to digital car data and competition in aftersales services* (2018) JRC Technical Reports, JRC Digital Economy Working Paper 2018-06, 7.

139 See Wolfang Kerber and Daniel Gill, "Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation" 10 (2019) JIPITEC 244 para 1.

140 Crémer (n. 6); Monopolkommission (n. 145); Secrétariat d'État Chargé de la Transition Numérique et des Communications Électroniques, Ministy of Economic Affairs and Climate Policy, "Consideration of France and the Netherlands regarding intervention on platforms with a gatekeeper position" (2020) < https://www.privacy-web.nl/cms/files/2020-10/non-paper-fra-nl-ex-ante-regulation-platforms-final-1410.pdf> (accessed 13.09.2020).

141 Ian Brown "Interoperability as a tool for competition regulation" (preprint 30 July, 2020) doi: 10.31228/osf.io/fbvxd; Furman (n. 6); Mardsen (n. 6); Stigler Report (n. 6).

142 European Commission, "The Digital Service Act Package" (2020) < https://ec.europa.eu/digital-single-market/en/digital-services-act-package> (accessed 13.09.2020); European Commission, "Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the European Union's internal market, Inception Impact Assessment" Ref. Ares(2020)2877647 - 04/06/2020 (2020).

143 Vijay Khatri and Carol V. Brown, 'Designing Data Governance' (2010) Communications of the ACM 53 (1), 148; Leo L. Pipino, Yang W. Lee and Richard Y. Wang, 'Data Quality Assessment' (2002) Communications of the ACM 45 (4), 211-218; Craig Stedman and Jack Vaughan, 'What is data governance and why does it matter?', online available at: <https://searchdatamanagement.techtarget.com/definition/data-governance> (accessed 13.09.2020).

data, the establishment of a common understanding of data and the compliance with regulations).[144] Yet, even though data governance strategies might already be incorporated on a micro-level in firms, a lack of data interoperability on a horizontal level between firms due to fragmented data standards and various proprietary APIs, leads to data silos and the balkanization of data. Despite international standardization endeavors and other private and hybrid initiatives, at firms' organizational levels, data interoperability is insufficiently addressed. As previously mentioned, semantic and syntactic interoperability work like magnetic poles. However, there is still a significant fragmentation at such levels and the communication via technical means, i.e. web-services, OBD ports or APIs, has not achieved the envisioned ambition of making data re-usable. This increases up-front investment in the efficient re-use of the data and raises transactions costs to outweigh a lack of quality data. This in the end may further minimize the incentives to share data. It is to this end where the role of the legislature becomes essential.

71 As sneak peek, our analysis of horizontally applicable data access regimes and of the sector-specific data access solutions shows the need for an even more comprehensive regulatory approach towards data governance solutions that also reflect the importance of potentially regulating data interoperability and standardization and addressing data safety and security issues, for ensuring the effectiveness of data governance solutions.[145] Despite the existence of already outlined private data access rights, a public law approach within the realm of a data governance solution is exactly what seems favourable. This is because of a lack of feasibility of enforcing the rights due to high transaction costs, legal uncertainty, technical impediments and opposing exclusive rights of others.

F. Conclusions

72 Demystifying the role of data interoperability in the access and sharing regimes is a Sisyphus work. Data interoperability is a complex technical issue, and thus another example of how important a good understanding of the technology is. As data interoperability counts with different levels and, as the market failures ought to build upon the ones from data access regimes, it should reflect on the same considerations. This however is currently hard to predict, as the discussion and the policy with regard to data access seems to move towards data commons and away from market force driven solutions that enable data driven innovation. Establishing data interoperability is thereby one of the key ambitions of the EU policy strategy. As data interoperability is also inherently tangled to the data access right, courts may interpret data interoperability in the realm of defining the scope of the access right. Ultimately, data interoperability may also be subject to direct data governance market regulation and thus subject to different regulatory goals, e.g., cyber security, data protection, data sovereignty, competition or data driven innovation.

73 The existence of multiple notions of interoperability may affect its own interpretation in the context of data access rights as well as in further delineating a data governance regulation. Therefore, from a legal policy perspective, a common understanding of data interoperability in the specific legal context is highly desirable. This will help to clearly outline the scope of data interoperability and therefore, would provide for a more coherent delineation of data access regimes when interpreted by courts. This is particularly relevant with regard to a harmonized Digital Single Market and the need of cross-border data flows. It would eventually increase legal certainty and predictability to private actors, thus fostering trust and probably increasing data sharing practices. Additionally, one should always bear in mind that interoperability, even if enshrined in the obligations correlating to data access rights, is still not a legal right or obligation (although it might become one soon). Using it as equivalent to data portability might come at the risk of confusing both. In addition, as explained earlier, it is still under debate what, if any, interoperability requirements the right to data portability of the GDPR entails.

74 In fact, technology may already govern data access and data sharing without legal intervention. If legal intervention takes place however, it may not only affect the efficacy of the access right itself, but also affect the effective enforcement of such right. Thus, interoperability is about to become another example of Lessig's "code is law". From this perspective, there is the threat of using interoperability as a goal and not as a means to an end. Pre-designed data interoperability by default is indeed a key enabler for data driven innovation. This however comes with the caveat of adverse effects of a high level of data interoperability. This not only relates to negative effects of data sharing itself – among others privacy or data induced competition concerns. It also relates to a potential hampering of innovation with regard to data and APIs.

75 Additionally, policy makers should bear in mind that APIs are one of the enablers of data interoperability. APIs represent an endpoint interface and are usually designed unilaterally. They are not a give-and-take

144 Ibid.

145 The analysis will be published soon, in a follow-up piece.

agreement and do not require full disclosure. Data standardization is another data interoperability enabler, where the design of data models, data formats and protocols require the agreement of the parties involved, therefore, collaboration and disclosing of information is required.

76 The EU Commission policy rightly foresees the role of the legislature being one that refrains from fiat and focusses on more flexible regulatory approaches. To this end, fostering the building of hybrid decentralized and distributed infrastructural systems, based on the development of data standards or fostering the standardization of APIs might be a better option than just mandating the full disclosure of APIs. Opening up of APIs as a default rule, without taking market failure considerations into account, negates potential utilitarian incentive considerations with regard to the exclusivity and/or excludability of the information in order to safeguard investment protection of firms.

77 Therefore, Member States' initiatives such as Gaia-X or data trusts seem to be a good example of how to achieve high levels of semantic data interoperability (also increasing data quality) and increase data sharing with the use of data standards. Hybrid forms of setting *de facto* data standards may also have spill-overs. Yet one should keep in mind that not addressing the issue of data interoperability on a multilateral level may have potential negative effects for international firms – despite current claims for a digital sovereignty of the EU.

78 From a competition economics perspective, traditional considerations with regard to vertical and horizontal interoperability cases may still be applicable in data cases and thus, essential facility considerations. There might be cases however, where the factual data exclusivity (based on a lack of interoperability information disclosure) makes the assessment of potential consumer welfare enhancing effects extremely complicated. Yet, data may be used for multiple other occasions that lack traditional market specific foreclosure scenarios. Data interoperability is always a matter of degree and does not necessarily lead to a market foreclosure of competitors.

79 As to the appropriation of APIs via IP rights and trade secrets, technological advancements in machine-to-machine communication, i.e., web services, have brought back to the table the need of re-assessing the balance between IP rights and the enabling of the free flow of data in a data driven economy. Even if under utilitarian efficiency considerations IP protection of APIs might be justified, the existing exceptions and limitations are not good enough as they do not ensure a balance between the protection of interests of right holders and third parties. For instance, the decompilation exception is dysfunctional and impracticable. It requires high up-front investments by the legitimate user without any guarantee that it will work; that is, it does not really guarantee that interoperability would be achieved. Additionally, it does not allow for free re-usability of the results.

80 From a global perspective, the Google v. Oracle case needs thorough attention. Copyrightability of APIs may indirectly affect the competition policy in software dependent markets.

81 Based on all the above, it seems that there is need for a more comprehensive regulatory approach towards data governance solutions that also reflect the importance of potentially regulating data interoperability and standardization and addressing data safety and security issues, for ensuring the effectiveness of data governance solutions.

82 These (sector-specific) data governance solutions are favorable as they also have the potential to holistically address the different IP and trade secret protection regimes, e.g., Open Data Directive and database protection. It will also need to reflect on IPRs over means of communications, i.e., APIs, OBD ports, web-services.

83 Therefore, despite the existence of some private data access rights, a public law approach within the realm of a data governance solution seems favorable. This is because of a lack of feasibility of enforcing the rights due to high transaction costs, legal uncertainty, technical impediments and opposing exclusive rights of others. Within such a data governance solution, conflicts of law and overlapping exclusive rights could be better addressed and aligned. This may provide for more practical, balanced solutions than adapting dysfunctional existing exceptions and limitations in IP and trade secrets regimes. Further elaboration on these solutions and policy recommendations are part of the follow-on study we have conducted, which will soon be published.

Acknowledgements: *This paper builds upon work carried out at the 'IoT Data Interoperability' Workshop, organized by the Max Planck Institute for Innovation and Competition in October 2018. The authors are grateful to Beatriz Conde Gallego (MPI Munich), Simonetta Vezzoso (University of Trento), Ian Brown (visiting CyberBRICS professor at FGV Law School), Marcus Irmscher (Rahi Systems Engineer) and Bertin Martens (JRC of EC) for valuable comments on an earlier version of this article.*

From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives

by **Plixavra Vogiatzoglou, Katherine Quezada Tavárez, Stefano Fantin and Pierre Dewitte***

Abstract: The right of access is often considered as the most important prerogative in the data subject's toolkit because it grants individuals the possibility to complement the information made available through privacy notices, but also because it paves the way for the exercise of other rights enshrined in data protection law, such as the rights to erasure or rectification. While the efficiency of the right of access under the General Data Protection Regulation has already been abundantly documented, there is a lack of empirical evidence as to its counterparts in the area of law enforcement and security. This contribution aims to fill that gap and provide insight into the practical exercise of the right of access in the Law Enforcement and Passenger Name Record Directives. Through both traditional desktop research and a legal-empirical study, the present paper delves into the national transpositions of those texts in a selection of Member States, and highlights the issues encountered when practically exercising the right of access against competent authorities and Passenger Information Units. It also draws upon the lessons learned from that exercise and suggests solutions and ways forward in order to overcome the obstacles faced along the way.

Keywords: Law Enforcement Directive; PNR Directive; data subject's rights; data access requests; legal-empirical study

Recommended citation: Plixavra Vogiatzoglou, Katherine Quezada Tavárez, Stefano Fantin et al., From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives, 11 (2020) JIPITEC 274 para 1

A. Introduction

1 The "EU data protection reform package", as introduced in 2016, comprises the widely known General Data Protection Regulation (GDPR)[1] as well as the Law Enforcement Directive (LED)[2]. The latter, on which this paper is partly focused, governs the collection and use of data in a security-related environment, as it applies to the processing of personal data by controllers for law enforcement

* Plixavra Vogiatzoglou is a doctoral researcher, Katherine Quezada Tavárez is a legal researcher, Stefano Fantin is a doctoral researcher and Pierre Dewitte is a doctoral researcher at the KU Leuven Centre for IT & IP Law (CiTiP) – imec. All authors have contributed equally to this paper.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR).

2 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (LED).

purposes.[3] The second focal point of this paper is the Passenger Name Record (PNR) Directive[4], which was enacted at the same time and regulates the transfers of passenger information to authorities that process the data for the purposes of prevention, detection, investigation and prosecution of serious crime, including terrorism.

2 Given the scarce empirical evidence documenting the exercise of the data subject's rights in the contexts of law enforcement and security, we decided to gather empirical evidence by testing the right of access under the LED and the PNR Directive against national competent authorities and Passenger Information Units (PIUs), respectively. Given the nature of those instruments, we also investigated how the LED and the PNR Directive have been transposed into national laws, paying close attention to the provisions dealing with the exercise of the right of access. The empirical data used for this study originate from Subject Access Requests (SARs) submitted to competent authorities and PIUs in eleven European countries, namely: Belgium, Cyprus, France, Greece, Ireland, Italy, Luxembourg, Malta, the Netherlands, Portugal, and the United Kingdom (UK).

3 This paper proceeds as follows. Section B sets the scene by detailing the rationale and scope of the research. Section C delves into the methodology adopted for the gathering of the empirical evidence. Section D outlines the legal frameworks under scrutiny and highlights the relevant provisions for the analysis performed in the subsequent sections. Section E, divided into two core parts, is devoted to the results of the empirical research. First, it sets out the theoretical framework by examining the scope of the right of access in the LED and the PNR Directive and investigating its relevance in security-related situations. Second, it examines the practical implementation of the right of access under the LED and the PNR Directive across the investigated Member States by summarising the results of our study. Section F then provides an assessment of the overall research findings and identifies common trends and areas for improvement in the national practices regarding the exercise of informational rights in security. Finally, Section G concludes this study and outlines some recommendations that may facilitate the exercise of the data subject's rights in a security context.

B. Rationale and scope

I. Rationale: Legality, accessibility and safeguards

4 When implementing norms into law, states must abide by national and international requirements aiming at safeguarding democratic values such as the rule of law. In addition, when adopting legal instruments that regulate the processing of personal data, fundamental rights, namely to privacy and to data protection, must not be impermissibly interfered with. More specifically, as enshrined in the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the EU (the Charter), interferences with fundamental rights can be justified upon the condition that they meet the requirement of legality, pursue a legitimate aim of general interest, and are necessary and proportionate to achieve the said aim.[5]

5 In accordance with the jurisprudence of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), legality derives from the rule of law principle and incorporates the protection of citizens against arbitrary interferences with their fundamental rights.[6] For an interference to be considered lawful, two conditions must be satisfied: the existence of a national law – a requirement easily met – and the quality of law.[7] The latter requires the said legislation to be accessible, foreseeable and to provide judicial safeguards, especially in cases where the law

3 Considering that the scope of the LED is restricted to the processing of data carried out by competent authorities (as defined in art 3(7) of the LED) for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

4 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132 (PNR Directive).

5 See Council of Europe, European Convention on Human Rights (last amendment 2010) (ECHR), art 8(2). Charter of Fundamental Rights of the EU [2016] OJ C202/391 (Charter), art 52(1). Moreover, according to the Charter, art 52(3), legality and proportionality under both the Charter and ECHR may be interpreted in a similar fashion, at least in the sense that the fundamental rights safeguards established under the ECHR are the baseline of protection for the Charter rights.

6 *Malone v the UK* App no 8691/79 (ECtHR, 2 August 1984); *Sisojeva and others v Latvia* App no 60654/00 (ECtHR, 15 January 2007).

7 For an in-depth analysis of the requirement of legality under the ECtHR jurisprudence, see Geranne Lautenbach, *The Concept of the Rule of Law and the European Court of Human Rights* (Oxford University Press, 2013).

grants wide discretionary powers to governmental authorities.[8] Accessibility, more specifically, is achieved insofar as citizens are able to know the rules applicable to a given situation.[9] Besides, the requirement of foreseeability is met when the law is clear enough to enable individuals to grasp the consequences of an infringement and the conditions under which the government may take actions.[10]

6 For an interference to be justified, the principle of proportionality *lato sensu* must also be respected. In other words, the interfering measure must be suitable and appropriate to meet the objective of general interest (here, security), strictly necessary and least onerous in relation to that objective. It must also be proportionate *stricto sensu*, i.e. achieve a fair balance.[11] In cases of legislation relating to security authorities and the rights to privacy and to data protection, proportionality and strict necessity are assessed by virtue of minimum safeguards providing individuals with sufficient guarantees to effectively protect their rights against the risk of abuse.[12] Such safeguards include the clear delineation of the conditions and circumstances under which authorities may undertake the interfering measures; for instance in relation to access to and use of personal data, as well as the existence of prior authorisation, supervision, notification and effective remedies for the affected individuals.[13]

7 The existence of judicial safeguards, linked to both legality and proportionality[14], is mainly discussed in cases where a Member State enjoys wide discretionary powers, such as in the field of security, and requires the existence of effective control, preferably by the judiciary, over the interfering measure.[15] According to both the ECtHR and the CJEU, any legislation imposing surveillance measures must also provide for the possibility of an individual to seek effective remedy in order to obtain information and/or access to the data relating to her or him. In the security field, discretionary powers conferred upon public authorities must be balanced through safeguards ensuring that individuals are adequately protected against arbitrary or abusive exercise of said powers.[16]

8 States have the responsibility to comply with and guarantee citizens' rights at a level that is considered acceptable as per national, international and European human rights legal instruments. When implementing a national law that may affect the rights of individuals, states have the obligation to meet the threshold of protection guaranteed by these instruments, which may be considered higher for states than for private entities given the constitutional and primary nature of human rights. Against this backdrop, it may be expected from states, when implementing laws on personal data processing by governmental security authorities, to comply with the legality requirement and set the example for the effective exercise of citizens' rights. The national transposition of the conditions for the exercise of the right of access before security authorities is instrumental in fulfilling these requirements.

1. Scope: The LED and the PNR Directive

9 One of the driving forces behind the EU data protection reform package was to increase the effectiveness of data protection rules by enhancing the control of individuals over their personal data.[17] The resulting instruments therefore include strong data protection safeguards aiming at ensuring the

8 *Malone* (n 6).

9 ibid.

10 ibid, *Leander v Sweden* App no 9248/81 (ECtHR, 26 March 1987); *Roman Zakharov v Russia* App no.47143/06 (ECtHR, 04 December 2015).

11 Jonas Christoffersen, *Fair balance: proportionality, subsidiarity and the primarity in the European Convention on Human Rights,* (Martinus Nijhoff Publishers, 2009).

12 For an extensive overview of the jurisprudence and minimum requirements in question see *Big Brother Watch and others v the UK* Apps nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2019); *Zakharov* (n 10); Joined cases C-203/15 and C-698/15 *Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, [2016] ECLI:EU:C:2016:970; Opinion 1/15 [2017] ECLI:EU:C:2016:656.

13 ibid.

14 The existence of judicial safeguards as part of the legality assessment may be assessed through the lens of proportionality and may overlap with the guarantees provided for by the right to an effective remedy enshrined in ECHR, art 13 and Charter, art 47. See Lautenbach (n 7).

15 *Klass and others v Germany* App no 5029/71 (ECtHR, 6 September 1978).

16 ibid.

17 European Commission, 'COM(2010) 609 final - Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A Comprehensive Approach on Personal Data Protection in the European Union' (European Commission 2010) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> accessed 20 June 2020.

highest standards of data protection across the EU. In that spirit, the LED was adopted in 2016 as an evolution of the Council Framework Decision 2008/977/JHA (CFD)[18]. The LED had the effect of broadening the scope of the CFD and the realm of legal safeguards and protections of individual rights when data processing takes place in the context of criminal investigations and proceedings.

10 Concomitantly, the terrorist attacks of the 21st century and the growing pressure towards enhanced cooperation on security and crime-related information led to the establishment of a passenger data exchange system in the EU.[19] A passenger name record (PNR), in particular, consists of a record of a passenger's information, which is necessary to enable reservations for each journey the passenger embarks on by plane.[20] While discussions on an internal EU PNR data exchange system date back to 2007, concerns on its nature and necessity raised by the European Parliament stalled its adoption until 2015, when the terrorist attacks in Europe raised that matter into swift motion.[21] The PNR Directive finally entered into force on 4 May 2016. The controversy, however, follows the PNR Directive which was challenged before German and Austrian administrative courts and the Belgian Constitutional Court. The German and Belgian courts decided to submit references for preliminary rulings before the CJEU, with questions regarding the compatibility of the directive with the fundamental rights to privacy and to data protection, due to its broad scope and the generalised processing of data it imposes.[22]

11 Similar to the GDPR, both the LED and the PNR Directive provide data subjects with "informational power"[23] by incorporating the right of access as part of the data subject's prerogatives. In particular, the right of access can function as a mechanism to address power asymmetries resulting from information imbalances in a security environment.[24] Yet, this informational empowerment is subject to a more limited scope in a security-related context, as explained in more detail under section E.

12 Data subjects' rights would, however, be worthless if they did not work in practice, be it because access to information is limited under domestic law or because of procedural obstacles to their exercise. While the right of access used to be disregarded and rarely exercised by data subjects,[25] it is currently growing

18 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60 No longer in force (CFD).

19 In particular, following 9/11, the first EU-US Passenger Name Records (PNR) Agreement was adopted in order to provide US authorities access to passenger data collected by air carriers. The Agreement, later substituted by a newer version with a different legal basis, essentially provides US authorities with access to the traveling information of every passenger flying from the EU to the US, but not vice-versa. See Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Modern Studies in European Law (Oxford: Hart Publishing, 2017), https://doi.org/10.5040/9781509901708.; Cristina Blasi Casagran, 'The Future EU PNR System: Will Passenger Data Be Protected?' (2015) 23 European Journal of Crime, Criminal Law and Criminal Justice 241.

20 PNR Directive, art 3(5) states that "PNR means a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers on to flights, or equivalent systems providing the same functionalities". PNR data are further explained through a list of 19 data categories in Annex I PNR Directive, including inter alia name, payment information and advance passenger information (API) data collected (e.g. nationality, family name, gender, date of birth).

21 See Tzanou (n 19); David Lowe, 'The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit for Purpose?' (2016) 16 International Criminal Law Review 856.

22 From Germany: request for a preliminary ruling in joined Cases C-148/20, C-149/20 and C-150/20 *Deutsche Lufthansa* [2020] OJ C279/21 (pending) and Case C-222/20 *Bundesrepublik Deutschland* [2020] OJ C279/30 (pending); from Belgium: Case C-817/19 *Ligue des droits humains* [2020] OJ C36/16 (pending).

23 Jef Ausloos, Michael Veale and René Mahieu, 'Getting Data Subject Rights Right: A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2019) 10 JIPITEC 283, 296.

24 René LP Mahieu and Jef Ausloos, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access. A Call to Support the Governance Structure of Checks and Balances for Informational Power Asymmetries' [2020] LawArXiv <https://osf.io/preprints/lawarxiv/b5dwm> accessed 14 July 2020.

25 As widely shown by empirical evidence. See Antonella Galetta, Chiara Fonio and Alessia Ceresa, 'Nothing Is as It Seems. The Exercise of Access Rights in Italy and Belgium: Dispelling Fallacies in the Legal Reasoning from the "Law in Theory" to the "Law in Practice"' (2016) 6 International Data Privacy Law 16, 21; Clive Norris and others (eds), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe* (Springer International Publishing 2017) 106; Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors. Data Subject Access Rights in Practice' (2018) 8 International

in popularity as a tool to foster transparency of data controllers, perhaps as a consequence of the increasing awareness resulting from recent privacy backlashes. This is certainly the case in the private sector, as illustrated by the extensive empirical evidence gathered and documented in the current literature.[26] Nevertheless, we suspect that the right of access remains a largely unknown and underused prerogative, at least in the area of law enforcement and security – an idea that seems supported by the research findings upon which this paper is based.[27] In other words, while scholars have already thoroughly explored the practical exercise of the right of access under the GDPR, the functioning of its counterparts in both the LED and the PNR Directive is still largely undocumented. This is particularly timely for the PNR Directive, since the European Commission issued its review[28] on 24 July 2020, the conclusions of which were "overall positive".[29] It was found that, although some Member States "have failed to fully mirror all [data protection requirements] in their national laws", overall compliance is achieved. No mention is made of the practical exercise of data subjects' rights, however.[30] Besides, it is not clear to what extent the data protection reform has contributed to the enhancement of the right of access.[31] Thus, it is still necessary to determine how the "architecture of empowerment"[32] brought by the EU reformed data protection legal framework works in practice in security-related data processing.

C. Methodology

13 The findings discussed in the present contribution build on two distinct initiatives. First, traditional desk research exploring the right of access as well as the transposition of both the LED and PNR Directive into national law. Second, a legal-empirical study during which we analysed the transparency measures adopted by competent authorities and PIUs, and exercised our right of access against the relevant controller(s). This section briefly introduces the reader to the methodology deployed in order to gather and analyse the results detailed in the remainder of the paper.

Data Privacy Law 4, 7.

26 For a detailed account of the experiences of an individual's attempts to access CCTV data through SARs, see Keith Spiller, 'Experiences of Accessing CCTV Data: The Urban Topologies of Subject Access Requests' (2016) 53 Urban Studies 2885; for a thorough overview of the practical exercise of the right of access under the now repealed 1995 Directive and an empirical analysis involving organisations in the public and private sectors across different EU countries, see Norris and others (n 25); for a study on the exercise of the right of access under the national implementation of the 1995 Directive in the Netherlands, as well as an assessment of to what extent the right of access involves a mechanism for citizens to obtain meaningful actual transparency in the public and private sector, see René LP Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 Internet Policy Review <https://policyreview.info/articles/analysis/collectively-exercising-right-access-individual-effort-societal-effect> accessed 29 April 2020; for an empirical examination of the right of access under the 1995 Directive against online platforms, as well as a detailed account on the difficulties encountered by data subjects when attempting to exercise access rights, see Ausloos and Dewitte (n 25); for a study uncovering the flaws in policies and practices on how the right of access under the GDPR is handled, as well as the dangers in that relation, see Mariano Di Martino and others, 'Personal Information Leakage by Abusing the GDPR "Right of Access"', *Proceedings of the Fifteenth Symposium on Usable Privacy and Security* (2019); other right of access initiatives and experiences by individuals, journalists, and civil society are inventoried in Mahieu and Ausloos (n 24).

27 Some of the referenced literature somewhat relate to security (as they included SARs to obtain CCTV footage, police records and data collected by Europol (see Spiller (n 26); Galetta, Fonio and Ceresa (n 25); and Norris and others (n 25)). However, none of the SARs in those earlier studies was filed under legal instruments specifically covering the processing of data in law enforcement and security (such as the LED and the PNR Directive).

28 Due by 25 May 2020, PNR Directive, art 19(1). Similarly, a review for the LED is due to take place by 6 May 2022, in accordance with LED, art 62(1).

29 European Commission, 'Report from the Commission to the European Parliament and the Council, On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', (Communication) COM (2020) 305 final.

30 ibid. According to the report, under footnote 17, '[a] comprehensive assessment of the completeness and conformity of the national transposing measures and their practical implementation has been carried out in the framework of the compliance assessment, conducted by an external contractor, under the supervision of the Commission.' This compliance assessment has nonetheless not been made public nor was made available upon the submission by one of the authors of an application for access to documents, due to protection of court proceedings, of the purpose of investigations and of the decision-making process.

31 As claimed in Norris and others (n 25), chapter 3.

32 Mahieu and Ausloos (n 24) 2.

I. General set-up

14 Both the desk research and the legal-empirical study were conducted by three researchers in Law at the KU Leuven Centre for IP & IT Law assisted by three students of the KU Leuven Advanced Master of Intellectual Property & ICT Law acting in the context of their Master's Theses. The desk research was conducted in January 2020, while the legal-empirical study spanned over a period of four months between February and June 2020. Initially, the intention was to investigate twelve countries, selected on the basis of the languages we speak as well as the countries we had flown to, from or through during the six months preceding the sending of the SARs[33]. Amongst the initially selected countries was Spain, which had not, at the time, transposed neither the LED nor the PNR Directive.[34] The workload on the remaining eleven countries[35] was then evenly shared based on the above-mentioned criteria. At each step of the process, we shared our findings through dedicated online surveys designed to orient the empirical research and provide an appropriate means to obtain meaningful, structured results at the end of the allocated time frame. Those surveys raised both quantitative (e.g. how many days did it take for the PIU to provide a first substantive answer?) as well as qualitative (e.g. how satisfied are you with the process of sending the access request?) issues. Regular meetings between the researchers and the students were held in order to ensure a shared understanding of the questions included in the surveys as well as the consistency of the results.

II. The desk research: The transpositions of the LED and PNR Directive into national law

15 Unlike the GDPR, which materialised the long-awaited shift from a directive to a regulation, the law enforcement reform was achieved through the means of directives. As a result, it was agreed to delve into the national transposition of the LED and PNR Directive for each of the investigated countries with the aim of uncovering the extent to which Member States had – or had not – diverged from the European texts. More specifically, the emphasis was put on the way each Member State had transposed the provisions related to data protection safeguards and the right of access as well as the modalities surrounding its exercise. We compiled our findings into two surveys: one for the LED and one for the PNR Directive. The results were then shared in order to have a common understanding of the transposing acts and relevant provisions in national law.

III. The legal-empirical study: Transparency measures and exercise of the right of access

16 The desk research served as a basis for the legal-empirical study, which itself consisted of two distinct efforts. First, we performed an analysis of the transparency measures put in place by each Member State according to the relevant provisions of both the LED and the PNR Directive as well as the national transposing acts. To that end, we went through the relevant texts in order to find the identity of the controller as well as (potential) instructions as to how to file an access request. We also browsed the websites of the said entities in order to assess their compliance with the transparency obligations stemming from European and national law. The second effort substantiated in the sending of an actual access request under both the LED and the PNR Directive. Here, the goal was to gather practical evidence as to how – and, in some cases, if – competent authorities and PIUs would handle the exercise of the data subject's rights. In order to ensure the comparability of the results, we relied on pre-defined templates when exercising our right of access.[36] Regular meetings also helped smooth out the obstacles faced along the way by systematically agreeing on a common pathway in the individual interactions we had with the competent authorities. At the end of the allocated time frame, we

33 This follows from the obligation for PIUs to depersonalise the Passenger Name Record (PNR) data after a period of six months by masking a series of data points that could serve to identify directly the passenger to whom the PNR data relate. See PNR Directive, art 12(2).

34 Because of that, the European Commission brought action before the CJEU against Spain to declare the failure to fulfil its obligations under Article 63(1) LED and to impose financial penalties for such failure and for as long as the infringement continues to take place. Case C-658/19 *European Commission v Kingdom of Spain,* [2019] OJ C357/27 (pending). At the time of submission of the paper (29 October 2020) Spain had still not transposed the LED. However, Spain published the national law transposing the PNR Directive on 17 September 2020. The latter was not taken into account for this paper, since the empirical study was concluded in June 2020. See Spain: Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.

35 Namely Belgium, Cyprus, France, Greece, Ireland, Italy, Luxembourg, Malta, the Netherlands, Portugal and the UK.

36 Attilia Ruzzene, 'Drawing Lessons from Case Studies by Enhancing Comparability' (2012) 42 Philosophy of the Social Sciences 99.

compiled our findings into two surveys dealing with transparency obligations and the sending and following-up of the access requests, respectively.

IV. Limitations

17 Before proceeding with the analysis of the results, it is worth highlighting some of the limitations of this research. First, several questions raised in the online surveys are subjective in nature (e.g. how easy/difficult would you describe the process of finding whom to send the access request to?). While the answers might therefore differ depending on the perception of each participant, this was mitigated by the introduction of more quantifiable indicators (e.g. Likert scales, amount of interactions during the follow-up process), the regular meetings and the experience of the researchers and students in the fields of European privacy and data protection law. Second, the selection of countries investigated is limited. The languages spoken by the participants as well as their travel history did not allow us to cover all EU countries. It should also be noted that the UK, which is currently in the process of leaving the EU, is among the selected countries. Moreover, it was decided to submit the SARs in an official language of each investigated country, so as to facilitate the process. We therefore cannot know whether language has been an impediment to or requirement for the requests, while the findings could potentially be different if they were submitted in English. Third, the legal-empirical study was conducted at a time when the COVID-19 pandemic started to escalate in Europe. While this had a limited impact on the desk research, it has potentially affected the accuracy of the findings related to the handling of the requests by (allegedly or genuinely) overwhelmed competent authorities and PIUs.

V. Objective

18 Beyond gathering and presenting concrete evidence as to the compliance of competent authorities and PIUs with data subjects' rights, the goal of this initiative is also to highlight the added-value of supplementing classic desk research with empirical findings in order to explore the many facets of an issue that might – at first sight – seem rather theoretical. Building on a similar initiative conducted throughout the academic year 2016-2017[37], the involvement of Masters students is also seen as a way to both offer a more interactive research path compared to traditional Master's Thesis topics and expand the coverage of the empirical part of the initiative. While the findings presented below certainly are the core contribution of this paper, we also aim to raise awareness on and promote the benefits of the potential of this type of research.

37 Ausloos and Dewitte (n 25).

D. The Directives and their transposition into national law

I. The Law Enforcement Directive

1. Scope of application

19 According to Articles 1 and 2, the scope of application of the LED extends to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection and prosecution of crimes, the execution of criminal penalties, and the safeguarding of public security. While the rather broad definitions of the term "public security"[38] and "competent authorities"[39] have sparked academic interest[40], what seems to converge in both scholars' and policymakers' views[41] is that law enforcement agencies *stricto sensu* (i.e. national police bodies and their local ramifications) fall under the scope of the LED. Moreover, as "public authorities competent for the prevention [..] of criminal offences" and "other bodies or entities entrusted by Member State law to exercise public authority and public powers" for the same law enforcement purposes also fall under the LED[42], its scope is much broader than criminal justice authorities.

38 European Data Protection Supervisor (EDPS), 'A further step towards comprehensive EU data protection - EDPS recommendations on the Directive for data protection in the police and justice sector' (Opinion No. 6/2015).

39 LED, art 3(7).

40 For a scholarly account of the broad limits of the term 'competent authorities', see Plixavra Vogiatzoglou and Stefano Fantin, 'National and Public Security Within and Beyond the Police Directive', in Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke (eds), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Intersentia, Cambridge, Antwerp, Chicago, 2019).

41 Diana Alonso Blas, 'The proposed Directive on data protection in the area of police and justice: A closer look – The omission of Europol and Eurojust from the draft Directive', (ERA Conference: Data Protection in the Area of European Criminal Justice Today – Speakers' Contributions, Trier, November 2012).

42 LED, art 3(7).

20 Territorially speaking, the LED is the first attempt by the EU to regulate both cross-border and internal data processing by law enforcement agencies at the same time and within the same legislation. The territorial scope is therefore extended at the domestic level (including intra- or inter- agencies of the same country) and at the cooperation level between law enforcement agencies based in different Member States of the Union. Such an approach is one of the most important differences between the LED and its predecessor, the CFD, which only applied to the processing of personal data in the context of cross-border police and judicial cooperation.[43] Overall, Article 1(3) of the LED allows Member States to apply higher data protection standards than the ones enshrined in the LED itself. This, in addition to the fact that the legal instrument used by the European legislator requires a national transposition, triggered high expectations among observers about how this potentially fragmented landscape would work in practice at its full operational capacity.[44]

2. Main provisions

21 The LED draws its foundations in the legacy of both the EU and the Council of Europe (CoE) legal instruments dealing with data protection. In particular, the CoE's Convention 108 is amongst the first international legal instruments to lay down, back in 1981, a series of principles which have served as a basis for many developments in the field. Along these lines, the so-called data protection principles play a crucial role in establishing the main safeguards for the processing of personal data in the LED. Those include lawfulness, fairness, purpose limitation, data minimisation and the security of processing.[45] The LED also specifically deals with the retention of data by competent authorities, emphasising that storage and retention periods should be reviewed periodically.[46]

22 The LED establishes specific data categories, which correspond to clear guidelines on the governance of data processing. Accurate distinctions should accordingly be made between different classifications of data subjects (suspects, convicted, victims, other persons)[47] and the diverse nature of the data (personal data linked to facts v. those based on personal assessments)[48]. Moreover, the processing of special categories of data, i.e. data revealing racial or ethnic origin, political opinions, sexual life and orientation, religious or philosophical beliefs, trade union membership and biometrics, is only allowed when strictly necessary and authorised by EU or domestic law, unless the processing is conducted to protect someone's vital interest or if the data was manifestly made public.[49]

23 Chapter IV[50] introduces a series of obligations for controllers. Those provisions mirror, to a large extent, the basic requirements that are also enshrined in the GDPR, and include the duty to implement data protection by design and by default, record-keeping policies, data protection impact assessment exercises, the security of processing, data breach notifications and the appointment of a data protection officer (DPO).[51] Additionally, the sector-specific obligation is imposed to maintain a record of logs when the processing operation is automated, which should be designed to comply with prompt accessibility in case of internal or supervisory audits.[52]

24 Chapter VI describes the governance of supervisory authorities. Interestingly, the LED leaves room for national implementing acts to appoint a different supervisory body than the data protection authority

43 Another significant difference is the legal context under which the LED is adopted (Treaty on European Union (Consolidated version 2016), OJ C202/1 (TEU), art 16), in contrast with the CFD, which was instead adopted in the context of the so-called 'third pillar' (also known as *Justice and Home Affairs-JHA*, then renamed *Police and Judicial Co-operation in Criminal Matters - PJCCM*).

44 Thomas Marquenie, 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', (2017) Computer Law & Security Review: The International Journal of Technology Law and Practice, 33(3), 324–340.

45 LED, art 4.

46 ibid, art 5.

47 ibid, art 6.

48 ibid, art 7.

49 ibid, art 10.

50 In Chapter III, the LED enshrines a series of information rights (more on this will be elaborated in section E.I.2.). Accordingly, law enforcement agencies (LEAs) are required to provide data subjects with information about data processing in a clear, concise, intelligible and easily accessible form. Such information should be made public proactively (LED, art 12), or under the direct request of a data subject, who is entitled to exercise his right of access (LED, art 14), rectification, erasure or restriction (article 16). While a deeper analysis on LED, arts 12 to 17 will be conducted in a separate section, it is useful to mention here that a number of limitations to the exercise of such rights may apply.

51 LED, arts 20, 27, 29, 30-31, 32.

52 ibid, arts 24-25.

established under the GDPR, while it remains possible to designate the same national supervisory authority (NSA).[53] As analysed below, this resulted in a fragmented landscape since some Member States decided to appoint a different supervisory body than the one competent under the GDPR. Nonetheless, according to Chapter VIII, NSAs are tasked with receiving the first instance of data subjects' complaints.[54] Data subjects are also entitled to seek effective remedy before national judicial bodies against decisions of supervisory authorities or alleged violations of the LED.[55]

3. Results from desktop research on national implementing acts

25 All the countries we investigated had transposed the LED between March 2018 – the earliest being Belgium[56] – and August 2019 – the latest being Greece[57]. They all used a wording similar to the LED when circumscribing its scope of application, namely the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties and the protection of public security. Cyprus, however, states that national security activities carried out by police bodies do not fall under the scope of the transposing act. This suggests that the original mandate of the Cypriot police authorities is not limited to law enforcement duties, but also includes national security and intelligence competences (which are excluded by the national LED transposition)[58]. Finally, only six out of the eleven Member States (the UK, Belgium, Portugal, Malta, Cyprus and Italy)[59] name the competent authorities that are included in the scope of such acts, either by explicit mention, such as in the UK[60] where the said list is included as an annex in the law, or by clear cross-reference in the text to the statutory laws establishing or regulating the competent authority, as in the case of Italy[61].

II. The PNR Directive

1. Scope of application

26 The legal basis for the PNR Directive is found in the Area of Freedom, Security and Justice of the Treaty on the Functioning of the EU,[62] and in particular in its provisions on judicial cooperation in criminal matters[63] and police cooperation for the collection,

53 ibid, art 41(3).

54 ibid, art 52.

55 ibid, art 53. For the sake of completeness, the LED includes Chapter V (transfers to third countries or international organizations), Chapter VII (cooperation), Chapter IX (implementing acts) and Chapter X (final provisions).

56 Belgium: Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

57 Greece: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προ- στασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

58 Cyprus: Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα από Αρμόδιες Αρχές για τους Σκοπούς της Πρόληψης, Διερεύνησης, Ανίχνευσης η Δίωξης Ποινικών Αδικημάτων ή της Εκτέλεσης Ποινικών Κυρώσεων και για την Ελεύθερη Κυκλοφορία των Δεδομένων Αυτών Νόμος του 2019, art 2.

59 See scope of application and competent authorities within the following national acts: UK: Data Protection Act 2018; Belgium: see (n 56); Portugal: Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016; Malta: Data Protection Act (CAP. 586), Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations, 2018; Cyprus: see (n 58); Italy: Attuazione della direttiva UE 2016/680 del Parlamento Europeo e del Consiglio, del 27.4.2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

60 UK: (n 59) Schedule 7.

61 Italy: (n 59) art 2(cc).

62 Treaty on the Functioning of the European Union (Consolidated version 2016), OJ C202/1 (TFEU).

63 ibid, art 82(1): "Judicial cooperation in criminal matters

storage and exchange of relevant information[64]. According to its Article 1, the PNR Directive establishes the obligation for air carriers to transfer PNR data to a designated national authority, and regulates the processing by and the exchange of PNR data amongst Member States. While this obligation is imposed only in relation to extra-EU flights, the PNR Directive leaves the possibility for Member States to extend such a system to intra-EU flights.[65] The processing of PNR data pursuant to the PNR Directive is limited to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.

2. Main provisions

27 Air carriers must provide PNR data of every passenger traveling from or landing in the territory of a Member State to the national PIUs.[66] PIUs process PNR data against predetermined assessment criteria to "identify persons who require further examination by competent authorities" as well as analyse PNR data in order to update or provide for new assessment criteria.[67] They are also responsible for transferring PNR data and the processing results to Europol and to the nationally appointed authorities entitled to request or receive them.[68] Such authorities must be competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime and may vary from law enforcement to customs to broader security authorities.[69]

28 The PNR Directive sets a number of safeguards surrounding the processing of personal data.[70] PIUs must appoint a DPO in order to monitor the processing activities and act as a single point of contact for data subjects.[71] The predetermined criteria on the basis of which PIUs further process some passengers' data must not be based on characteristics that consist of discriminatory grounds, such as ethnic origin, health or religion.[72] Automated positive matches and transfers to competent authorities must be reviewed by a human.[73] PNR data must be depersonalised through masking after a period of six months, be retained for a total period of five years and then be permanently deleted.[74] Disclosure of PNR data after the period of six months is only allowed under specific conditions.[75] Competent authorities are bound to process the transferred PNR data only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.[76]

29 Member States should introduce a prohibition on automated decision-making with adverse legal or similarly significant effects on a person.[77] In addition, such decisions may not be based on sensitive characteristics that consist of discriminatory grounds.[78] The PNR Directive points to the CFD – now repealed and replaced by the LED – when it comes to data subject's rights, data security, processing records and notification of data breaches.[79] In addition, it prohibits the processing of special categories of data.[80] Fur-

in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation of the laws and regulations of the Member States in the areas referred to in paragraph 2 and in Article 83. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures to: (a) lay down rules and procedures for ensuring recognition throughout the Union of all forms of judgments and judicial decisions; [..]".

64 ibid, art 87(2): "For the purposes of paragraph 1 [police cooperation], the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may establish measures concerning: (a) the collection, storage, processing, analysis and exchange of relevant information; (b) support for the training of staff, and cooperation on the exchange of staff, on equipment and on research into crime-detection; (c) common investigative techniques in relation to the detection of serious forms of organised crime."

65 PNR Directive, art 2.

66 ibid, arts 4 and 8.

67 ibid, art 6.

68 ibid, art 4.

69 ibid, art 7.

70 ibid, art 6.

71 ibid, art 5.

72 ibid, art 6(4).

73 ibid, art 6(5).

74 ibid, art 12(2).

75 ibid, art 12(3).

76 ibid, art 7(4).

77 ibid, art 7(6).

78 ibid.

79 ibid, art 13.

80 ibid, art 13(4) which states that Member States shall prohibit the processing of PNR data revealing a person's race or

thermore, it includes procedural provisions regarding the exchange of information between Member States,[81] the conditions for access to PNR data by Europol[82] and the transfer of data to third countries.[83] Finally, an NSA must be appointed in each Member State for advising on and monitoring the application of the PNR Directive.[84]

3. Results from desktop research on national implementing acts

30 Out of the investigated countries, only Ireland did not extend the PNR scheme to intra-EU flights.[85] It is noticeable that two Member States, namely Belgium[86] and France[87], expanded the purposes of the PNR scheme to also include border control and the fight against illegal immigration.[88]

31 Most transposing laws adopted the same definitions for PNR data and data categories. Insofar as competent authorities entitled to receive or request PNR data are concerned, most Member States specifically enumerate them in the law, apart from the UK[89]. Nevertheless all of them have notified the list of competent authorities to the European Commission.[90] Interestingly, besides law enforcement authorities, most Member States also include national security/intelligence services (Belgium, Cyprus, Greece, Luxembourg, Malta, the Netherlands and Portugal) as well as customs authorities (Belgium, Cyprus, Greece, Luxembourg, Malta and Portugal) in the list of competent authorities.[91] Cyprus, Greece and Malta have also explicitly included financial and anti-money laundering units in the list, while Ireland and Malta also refer to immigration authorities.[92] Even more strikingly, the list of authorities competent to receive PNR data from PIUs also include the Dutch Military, the Irish Department of Employment and Social Protection, and the Hellenic Coast Guard and Fire Department.[93]

32 Almost half the Member States investigated (Cyprus, France, Greece, Ireland and Portugal)[94] require approval only by a judicial authority before a competent authority can access the data held by the domestic PIU upon expiry of the period of six months. The Dutch law does not explicitly prohibit the competent authorities from taking automated decisions producing adverse legal or similarly significant effects to persons, nor on the basis of

ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. In the event that PNR data revealing such information is received by the PIU, they shall be deleted immediately.

81 ibid, art 9.

82 ibid, art 10.

83 ibid, art 11.

84 ibid, art 15.

85 Ireland: European Union (Passenger Name Record Data) Regulations 2018, arts 3-4.

86 Belgium: Loi du 25 décembre 2016 relative au traitement des données des passagers, Chapitre 11.

87 France: Décret n° 2018-714 du 3 août 2018 relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure (partie réglementaire), art R-232.15.

88 A matter that has been raised by the Belgian Constitutional Court before the CJEU in the pending case *Ligue des droits humains* (n 22).

89 UK: The Passenger Name Record Data and Miscellaneous Amendments Regulations 2018, art 2.

90 Notices from Member States, Passenger Name Records (PNR) — Competent authorities — List of competent authorities referred to in Article 7 of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (This list reflects the authorities entitled, in each Member State, to request or receive PNR data or the result of processing those data from their national Passenger Information Unit (PIU) or for the purpose of Article 9(3) of Directive (EU) 2016/681 directly from the PIU of any other Member State only when necessary in cases of emergency) (2018) OJ C194/ 1.

91 ibid.

92 ibid.

93 ibid.

94 Cyprus: Ο περί της Χρήσης των Δεδομένων που περιέχονται στις καταστάσεις Ονομάτων Επιβατών (ΠΝΡ) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων Νόμος του 2018, art 16; France: (n 87), art 9; Greece: Υποχρεώσεις αερομεταφορέων σχετικά με τα αρχεία επιβατών - προσαρμογή της νομοθεσίας στην Οδηγία (ΕΕ) 2016/681 και άλλες διατάξεις, art 14; Ireland: (n 85), art 11; Portugal: Lei n.º 21/2019 de 25 de fevereiro - Regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros, bem como o tratamento desses dados, transpondo a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e procede à terceira alteração à Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna, art 8.

discrimination grounds, although the overarching prohibition on special categories of data has been included.[95] Nonetheless, the Dutch law refers to the LED implementing law, and subsequently to the conditions for automated decision-making therein.[96] Finally, most Member States name a specific supervisory authority, which is the same one responsible for monitoring the application of the GDPR and the LED provisions (apart from Belgium, France and the Netherlands)[97].

III. Relation between the LED and the PNR Directive

33 Through our desktop research on the national transposition of the PNR Directive, it was uncovered that most Member States repeated the reference to specific data protection rights and obligations by merely adapting the reference to the LED provisions instead of the CFD ones. The applicability of the LED in place of the CFD, however, may be of particular importance for data protection in the context of the PNR Directive. More specifically, as mentioned above, the CFD had a significantly limited scope of application, excluding internal, non-cross-border processing of personal data. Given the limited scope of the CFD and the concerns raised by the European Parliament about adopting such an EU PNR scheme, the reference to core data protection rights and obligations sought to reassure the wary. Nevertheless, the LED that took its place emphatically raised the level of protection of personal data in comparison to the previous framework, by virtue of, inter alia, its applicability to competent authorities at large, as explained above.

34 Pursuant to the definition of competent authorities under the LED[98], it may be deduced that PIUs fall under this definition and are therefore subject to the LED.[99] Consequently, the LED may be considered as *lex generalis* in the sense that, unless explicitly stated otherwise, it should be applicable in its entirety to PIUs. In that way, it is not clear what meaning the reference to specific provisions in the CFD holds now that the latter is no longer applicable, or whether such reference implies a limited applicability of data protection safeguards under the currently-in-force LED. The equivalent reference to specific provisions within the LED should be considered as superfluous rather than restricting its scope of application as *lex specialis*, given that such interpretation would diminish the level of protection. Of course, as both legal instruments consist of directives that must be transposed into national law, leeway is given to Member States. That discretionary power, however, should not be used to the detriment of data protection safeguards.

E. The right of access

I. From theory...

1. The many facets of the right of access

35 The right of access was explicitly incorporated within the provision on the fundamental right to data protection in the Charter[100], which entered into force in 2009. Both the CJEU and the ECtHR have acknowledged that the right of access plays an important role in the protection of other data protection rights. For instance, in its Rijkeboer ruling,[101] the CJEU stated that the right of access is a prerequisite for the exercise of other data subject's rights, a position that the Court confirmed in its subsequent case law (such as YS[102] and Nowak[103]). Moreover, in Nowak, the Court further stated

95 The Netherlands: Wet van 5 juni 2019, houdende regels ter implementatie van richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit (PbEU 2016, L 119) (Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven).

96 ibid, art 17.

97 Belgium: (n 56), art 184; France: (n 87); the Netherlands: (n 95).

98 LED, art 3(7).

99 Discussions on the potential applicability of the LED already to private entities such as air carriers which are obliged to process personal (PNR) data for further law enforcement purposes have also taken place, see for example Nadezhda Purtova, 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships' (2018) 8 International Data Privacy Law 52; Vogiatzoglou and Fantin (n 40).

100 Charter, art 8(2).

101 Case C-553/07 *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* [2009] ECR I-3889, paras 51-52.

102 Joined Cases C-141/12 and C-372/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* [2014] EU:C:2014:2081, para 57.

103 Case C434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994, para 57.

that the right of access under data protection law meets the goal of guaranteeing the protection of "[the individual's] right to privacy with regard to the processing of data relating to him or her".[104] A similar reasoning may be found in the case law of the ECtHR, although in cases related to the right of access to information more broadly rather than the right of access under the data protection regime per se, but nevertheless yielding similar effects as those intended by the CJEU. Examples of that ECtHR case law include Leander[105] and Rotaru[106], which form part of the analysis in sub-section 3 below (on the relevance of the right of access in the context of security).[107] The ECtHR has also indicated that, when access requests are denied or disregarded by actors either in the public or private sector, such behaviour could amount to a disproportionate interference with the right to privacy under Article 8 ECHR, if that decision fails to strike a fair balance between competing interests.[108]

36 Considering the way in which the right of access is framed in the GDPR[109] and the interpretations of the two European courts, it can be argued that the right of access plays at least two essential roles. On the one hand, it provides data subjects with access to their personal data. On the other, it enables the data subject to have his or her data rectified, erased, or to object to the processing, thus becoming not only an end in itself, but also an instrument in support of the exercise of other information rights. In this manner, the right of access is an essential component of the informational empowerment of data subjects and, as the European Data Protection Supervisor (EDPS) put it, can be considered as a "precondition to allow [individuals] more control over their data".[110] In the same vein, the right of access enables data subjects to verify the accuracy of their personal data and the lawfulness of the data processing carried out by controllers. Moreover, it is the first mechanism that data protection law grants data subjects against data protection violations[111], which could make it instrumental in improving transparency of data processing practices.

37 In addition, the right of access can be considered an empowerment mechanism that lends itself for both private and societal interests. On the one hand, it helps citizens to pursue individual interests; namely, to learn more about particular data processing activities involving their personal data through SARs. On the other hand, the right of access serves broader societal interests of addressing existing information asymmetries between controllers and data subjects.[112] For example, the exercise of the right of access could eventually result in an improvement of data processing practices by unveiling illegitimate processing activities or gaps in the practical implementation of the law. To that end, the exercise of data access rights could be particularly effective when realised in a joint effort by several data subjects.[113] The above may be included in the reasoning underpinning the European Commission's consideration of "data protection as a pillar of citizens' empowerment"[114].

38 Furthermore, considering the importance of citizen access to information held by state authorities,[115] access rights can have the potential to serve as a tool for citizens to foster transparency in the processing

104 ibid, para 56.

105 *Leander* (n 10), para 48.

106 *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000, para 46).

107 Other ECtHR case law providing evidence of the importance of access rights to balance conflicting interests are *Gaskin v the UK* App no 10454/83 (ECtHR, 7 July 1989, paras 43 and 49), *Haralambie v Romania* App no 21737/03 (ECtHR, 27 October 2009, paras 86 and 96), and *I v Finland* App no 20511/03 (ECtHR, 17 July 2008, para 47).

108 As stated by the ECtHR in the following rulings: *Leander* (n 10), *Gaskin* (n 107), *Z v Finland* App no 22009/93 (ECtHR, 25 February 1997), *M.G. v the UK* App no 39393/98 (ECtHR, 24 December 2002), *I v Finland* (n 107), and *Haralambie* (n 107).

109 GDPR, art 15.

110 EDPS, 'Opinion 7/2015: Meeting the Challenges of Big Data. A Call for Transparency, User Control, Data Protection by Design and Accountability' (2015) 5 <https://edps. europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf> accessed 20 June 2020.

111 Antonella Galetta and Paul De Hert, 'A European Perspective on Data Protection and the Right of Access' in Norris and others (n 25).

112 Mahieu, Asghari and van Eeten (n 26).

113 ibid.

114 As highlighted in its recent report on the two years of application of the GDPR. European Commission, 'COM(2020) 264 Final Communication from the Commission to the European Parliament and the Council - Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation' (European Commission 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> accessed 4 July 2020.

115 See Paivi Tiilikka, 'Access to Information as a Human Right in the Case Law of the European Court of Human Rights' (2013) 5 Journal of Media Law 79, 81–83.

practices by the government. In other words, the right of access may serve as a means to scrutinise the activities carried out by public authorities[116], as the ECtHR and CJEU case law seems to suggest.[117] The right of access can therefore provide citizens with the awareness of data processing operations carried out by public authorities. This is the case when the exercise of a SAR provides citizens with information necessary to act upon potential unlawful practices or data suggesting potential abuses of power (such as collection or processing of data without a legal basis, for example). Furthermore, the right of access can empower individuals to have a direct impact on policies and legislative initiatives.[118]

39 It should be noted, however, that despite the wide acceptance in scholarly literature regarding the reasoning surrounding the citizen empowerment stemming from data protection law[119], this idea is not supported in all academic works. For example, Koops argued that the correlation between data protection law with the notion of "control" is fallacious.[120] Put briefly, Koops' argument is that the data protection framework cannot provide control over one's own data, particularly because of the complexities characterising modern data processing activities coupled with the intricacies that distinguish the data protection architecture. On a similar note, Lazaro and Le Métayer disputed the potential of the right of access to work as an empowerment mechanism.[121] Lazaro and Le Métayer considered that the correlation between data protection law and the notion of "control" results from a flawed view of the theories concerning privacy and data protection.[122]

40 It is also worth noting that, even if the right of access can be considered as a tool for informational empowerment, the data protection regime does not establish a right of access to any particular document or file containing personal data concerning the individual. This was confirmed by the CJEU in its YS ruling,[123] where the Court provided clarifications as to the scope of the right of access under the now repealed Data Protection Directive[124] but nonetheless relevant for the current understanding of the right of access. In YS, the CJEU held that data subjects are not entitled to have access to a legal analysis made in an administrative document (in the case at hand, the "minute", i.e. a document containing the reasoning of the case officer of a data subject's entitlement to a lawful residence permit). This relates to the fact that such legal analysis is not "personal data" within the meaning of data protection law, as the Court concluded. That clarification gains particular importance in the context of the citizen-state relationship at stake when it comes to the right of access under the LED and the PNR Directive.

2. The right of access under the LED and the PNR Directive

41 The LED in its Article 12(1) requires controllers to implement reasonable measures to provide the necessary information to the data subject in a concise, intelligible and easily accessible form and using clear and plain language. Such information, to be provided by appropriate means, including electronic ones, shall be designed to facilitate the exercise of any data subject's right enshrined in the LED. Article 13(1)

116 As it enables the verification of legitimacy of data practices. Mahieu, Asghari and van Eeten (n 26) 3; European Union Agency for Fundamental Rights, 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Update' (2017) 124 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf> accessed 6 September 2019.

117 As follows from the case law included in the analysis at the beginning of this section, namely *Rijkeboer* (n 101), *YS* (n 102), *Nowak* (n 103), *Leander* (n 10), and *Rotaru* (n 106).

118 As illustrated by the success stories relating to the privacy activist Max Schrems, who has pursued privacy campaigns that started by SARs. Xavier L'Hoiry and Clive Norris, 'Introduction – The Right of Access to Personal Data in a Changing European Legislative Framework' in Clive Norris and others (n 25).

119 See A.O. Steven Lorber, 'Data Protection and Subject Access Requests' (2004) 33 Industrial Law Journal 179, 180; Norris and others (n 25) 1–8; Ausloos and Dewitte (n 25) 7; Ausloos, Veale and Mahieu (n 23) 286; Mahieu, Asghari and van Eeten (n 26) 16; Mahieu and Ausloos (n 24).

120 Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250.

121 Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 SCRIPTed <https://script-ed.org/article/control-over-personal-data-true-remedy-or-fairy-tale/> accessed 27 July 2020.

122 For a similar line of reasoning, see Mark Leiser and Bart Custers, 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680' (2019) 5 European Data Protection Law Review 367.

123 *YS* (n 102).

124 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 [1995] OJ L281/31.

further lists the minimum information to be made available to all data subjects, namely: (a) the identity and contacts of the controller, (b) the contact details of the DPO, (c) the purposes of the processing, (d) the existence of the right to lodge a complaint with the supervisory authority and (e) the existence of rights of access, to rectification, to erasure and to restriction.

42 The requirements prescribed in Articles 12 and 13(1) LED can be considered as ex ante obligations, i.e. obligations that need to be satisfied ahead of the data processing activities by making that information available through, for instance, the website of the competent authority[125]. Those information obligations are complemented with the ex post right of access envisaged in Article 13(2) LED for specific cases and in Article 14 LED. According to the latter, data subjects are entitled to obtain more information about the data processing activities undertaken by the controller than the general information made available to the public on an ex-ante basis. In that way, the right of access entails the possibility for data subjects to require more transparency from the controller on the actual data processing activities concerning him or her. Insofar as the information obligations under the PNR Directive are concerned, the text only refers to the applicability of the CFD (now LED) provisions for the exercise of the right of access.[126] Therefore, it might be inferred that the LED and the PNR Directive differ in their information obligation measures, while the conditions for and limitations to the exercise of the right of access are identical for both instruments. This is an example of how interpreting the reference within the PNR Directive to specific CFD provisions as *lex specialis* (see above section D.III.) may result in lowering the level of protection of personal data.

43 By virtue of Article 14 LED, the LED and the PNR Directive grant data subjects the right to access their personal data.

This means that citizens are entitled to receive from security-related bodies (including competent authorities and PIUs subject to the directives):

- Confirmation as to whether or not personal data concerning them are being processed;
- Where that is the case, access to several categories of information, including:
  - Information at least as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; and
  - Communication in an intelligible form of the data undergoing processing and of any available information as to their source.

44 However, the LED – and the PNR Directive, indirectly – also limit the right of access. According to Article 15 LED, Member State law can implement measures that enable controllers to fully or partially restrict SARs in case such requests interfere with the achievement of security interests in any way (for instance, by potentially obstructing official or legal inquiries, investigations or procedures).[127] These limitations may mitigate or reduce the positive effect of the information empowerment tool granted to individuals in a security or law enforcement context.[128] Hence, the right of access is not absolute, and, since the grounds for denial of access are worded in very broad terms, the limitations that Member States can implement may potentially provide controllers with broad discretionary powers in security.[129]

45 Having said that, it is worth noting that the limitations applicable to the right of access should not be interpreted as the possibility for competent authorities to adopt a blanket approach of refusing to provide any of the data falling under any of the grounds for refusal. This follows from Article 15(3) LED, which provides that, when the right of access is restricted or refused, Member States' laws must stipulate the obligation for controllers to document the factual or legal reasons leading to such a decision. When requested, such information must also be made available to the NSA, which provides an additional layer of control over the justification. The importance of the justification obligation can be illustrated by a recent case concerning the restriction of an SAR by national competent authorities in the UK, where an Administrative Court recently handed

125 LED, rec 42.

126 According to the PNR Directive, art 13(1), the corresponding articles on data subjects' rights of the CFD, which has now been repealed and replaced by the LED, are applicable.

127 It is worth noting that the limitations to the right of access are not exclusive to the processing of data in the security field. The GDPR also contemplates equivalent limitations to the data subject rights enshrined therein, as per its art 23.

128 As De Hert and Papakonstantinou argue in 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) 7 New Journal of European Criminal Law 12–13.

129 Diana Dimitrova and Paul De Hert, 'The Right of Access Under the Police Directive: Small Steps Forward' in Manel Medina and others (eds), *Privacy technologies and policy* (Springer 2018) 122.

down a decision in the Dalton case[130]. One of the main questions was precisely whether the justification supporting the initial refusal – then partial restriction – of the right of access was adequate.[131]

46 In addition, Article 17 LED introduces the so-called "indirect access", which should, in principle, offer an additional path to data subjects for the exercise of their rights. Accordingly, the exercise of a data subject's rights enshrined in the LED can also be performed by the supervisory authority on behalf of the data subject, in cases when the controller denies a data subject the exercise of his or her information rights.[132] In such a case, the NSA acting as a proxy shall inform the data subject at the very least that the appropriate verifications before the law enforcement agency have been undertaken. As we will be able to explain below, such a path was instead chosen and interpreted as a default procedure for the filing of SARs by the authorities of one of the Member States, *de facto* turning the rationale of Article 17 LED from providing an additional choice to data subjects to restricting the actual access to their personal data.

47 Overall, the scope and reach of the right of access in the legal instruments under analysis seem to match the balancing effort between the competing interests at stake.[133] Yet, the possible effects of the right of access in a security context very much depends on the national transpositions of the LED and the PNR Directive.[134] In other words, each Member State may take into account their specific national characteristics and adapt the provisions to their national legal culture. As a result, it is necessary to examine the national implementations of the EU law and the operationalisation of the law in each country to fully understand the potential effects of the right of access in a security context.

3. Relevance of the right of access in the context of security

48 While data protection law grants individuals control over their data and therefore acts as a means to scrutinise government agencies, it can also be used to scrutinise security-related personal data processing. This is particularly the case when considering that data subjects' rights in the LED and the PNR Directive aim at empowering individuals by providing them control over their data held by state authorities. In that sense, the right of access allows citizens to learn more about how the data collection and processing practices take place at the state level.

49 In its Rijkeboer ruling, the CJEU highlighted the importance of the right of access as a mechanism to remedy data protection violations.[135] When it comes to the role that access plays in a security context, the ECtHR has considered that the refusal to grant access to the information stored by public authorities (including security bodies, such as the secret police[136] or the intelligence service[137]) deprives individuals of the opportunity to refute it. That, in turn, entails an interference with the right to privacy, the Court concluded.[138] Moreover, the ECtHR has indicated that authorities have a "positive obligation" to offer citizens an effective procedure to obtain access to "all relevant and appropriate information" they hold, even if the personal information concerned is stored in the archives of the former secret services.[139] Following this line of reasoning, the right of access under the LED and the PNR Directive could operate as a mechanism to empower citizens by addressing information asymmetry issues in the citizen-state relationship. In particular, it arguably provides citizens with the possibility to scrutinise and question data processing practices in a security environment. This appears to be the case at least from a conceptual perspective.

130 *Dalton, R (On the Application Of) v The Crown Prosecution Service (CPS)* [2020] EWHC 2013 (Admin).

131 However, the Court's findings are more about procedural aspects, rather than the merits of the case. As the Court itself expressly said, it is for the NSA to determine whether the restriction was justified based on a necessity and proportionality assessment (ibid, para 70).

132 See also LED, rec 48.

133 As discussed by De Hert and Boehm's analysis of relevant ECtHR case law in relation to security-related processing of data. See Paul De Hert and Franziska Boehm, 'The Rights of Notification after Surveillance Is over. Ready for Recognition?' in Jacques Bus and others (eds), *Digital Enlightenment Yearbook 2012* (IOS Press 2012).

134 Considering that a directive is only binding for Member States as to the results to be achieved, but each Member State is free to decide how to transpose the legal text. This differs from what happens with a regulation, which has binding legal force throughout every Member State (TFEU, art 288).

135 *Rijkeboer* (n 101), para 52.

136 *Leander* (n 10).

137 *Rotaru* (n 106).

138 ibid.

139 *Haralambie* (n 107), paras 85-88.

II. ...to practice

50 The first two sub-sections below focus on the national implementation of Articles 12 and 13(1) LED, which deal with the general modalities through which information must be presented to data subjects. Not only one-to-one communication between controllers and data subjects, but also – and most importantly – the communication between the controller and the general public. Articles 12 and 13(1) therefore detail the practical and procedural steps controllers must undertake to enable data subjects to exercise their prerogatives. The rationale behind these two provisions is captured by Article 12(2) itself, which obliges controllers to "facilitate the exercise of the rights of the data subject". According to the above-mentioned provisions, the modalities surrounding the exercise of the right of access and the information on the processing operations shall be easily accessible. The research undertaken for this study therefore started with an investigation of the national laws implementing both directives as well as of the information made available on the websites of competent authorities and PIUs, through the use of online surveys (Survey 1 and Survey 2, respectively). By combining a legal and an empirical study, we aimed at determining how that information was presented to data subjects. The results are hereby presented separately for the LED and the PNR Directive.

51 The three remaining sub-sections are of purely empirical nature. In particular, they detail the manner in which SARs were submitted in accordance with the information found, the interactions that took place with the controllers, and the final responses we received regarding the processing of our personal data by the respective competent authorities and PIUs. Given the commonalities in approach, the results for submission, follow-up and final responses of the SARs under both the LED and PNR Directive are presented under a common subtitle. All national competent authorities' and PIUs' websites, where information on privacy and data protection policies were sought, as well as the contact details of the addressees to whom SARs were submitted, are included in a comprehensive manner per each country under Annex I.

1. National transposition

a) LED

52 The first step was to look directly into domestic laws to check what pieces of information mentioned in Articles 12 and 13(1) LED were already included in the national transposing acts. With respect to the identity of the controller, only four Member States include the specific competent authority within their respective legislation (Ireland, the UK, Italy, Cyprus)[140]. For all other Member States, the research was focused on the relevant national police authority's website or the relevant Ministry's website.

53 Starting with Article 12 LED, in spite of idiomatic differences across Member States due to language diversity, a handful of countries includes transposing Articles he wording of which differs from the original LED formulation. The Dutch law[141], for instance, does not explicitly mention the duty of the controller to prove the request is manifestly unfounded or excessive before refusing to act on it. Nonetheless, a higher level of granularity in the transposition of Article 12 LED appears when the Dutch law explains the procedure that the competent authority must follow when answering a request for access: data subjects shall be informed in a timely manner by the authority of (i) the reception of the request, (ii) the deadline for referral and (iii) the possibility to lodge a complaint.[142] The Belgian law, furthermore, limits the right of access in two ways. First, it obliges data subjects to exercise their rights indirectly through the "Organe de Contrôle" and, second, the said "Organe de Contrôle" can only let data subjects know that the necessary verification as to the legality of the processing operations have been done.[143]

54 With regard to the implementation of Article 12(3) and (4) LED, which respectively concern timing, fees and denials of requests, we found that national implementations diverge from one another, too. For instance, whilst the Portuguese law[144] requires authorities to respond within thirty days (renewable for another thirty), other countries have adopted the original wording of the LED, i.e. "without undue

140 Ireland: Data Protection Act 2018, sec 69; UK: (n 59) Schedule 7; Italy: (n 59), art 2; Cyprus: (n 58), art 2.

141 The Netherlands: Wet van 21 juli 2007, houdende regels inzake de verwerking van politiegegevens (Wet politiegegevens), arts 24a and 26(1); Wet van 7 november 2002 tot wijziging van de regels betreffende de verwerking van justitiële gegevens en het stellen van regels met betrekking tot de verwerking van persoonsgegevens in persoonsdossiers (Wet justitiële gegevens), arts 17b, 20(1) and 25.

142 As we will explain further, in our application for SARs, the Dutch authorities followed this Article by informing the data subject in writing and via post about such three elements.

143 Belgium: (n 56), art 42(1)-(2).

144 Portugal: (n 59), art 13.

delay". Some slight differences persist with respect to other features. The UK law[145], for instance, stipulates that any delay can be justified until the controller has reasonably ascertained the identity of the applicant. With respect to potential fees to be charged to the data subjects, some countries like Portugal expect the controller to make a "reasoned decision" for refusal[146], whereas the UK delegates the specification of the fee to further regulation by the Secretary of State[147].

55 In general, all national laws scrutinised except for Belgium[148], Portugal[149] and Malta[150], mirror the (almost exact same) formulation of the LED when prescribing that the information must be provided and presented in a concise, easily accessible form, using clear and plain language. Moreover, whilst some countries like Italy[151], Belgium[152] and the Netherlands[153] explicitly state within their national laws that the provision of information shall respect domestic limitations arising from police statutes and criminal procedures, only two Member States' laws explicitly mention how to find the preliminary information to exercise any data subject's rights. In particular, only Greece[154] and Italy[155] expect that the contact details of the controller shall be found online on the controller's website. A similar reference to the controller's website is also present in the Irish Data Protection Act[156], even though the scope of the provision is slightly different, as it requires the whole list (not just the controller's details as per the cases of Greece and Italy) of information ex Article 13(1) LED to be published.

56 With regard to the transposition of Article 13 LED, our research suggests that national formulations differ from the LED for almost half of the investigated Member States. In Portugal, for instance, the controller shall make the information "publicly available and permanently accessible" (as opposed to limiting the provision of that information to data subjects actively engaged in the exercise of their information rights).[157] Furthermore, whereas Article 13(2) LED (additional information to be provided to the data subjects) applies to specific cases, the Belgian Law[158] does not make such a distinction, thereby suggesting that the controller shall in any case provide the information listed in both Articles 13(1) and 13(2) LED.

57 With regard to the modalities of the exercise of the right of access under Article 14 LED, our research revealed a few countries with a different wording and additional requirements in their national laws. In the Dutch law[159] there are extra provisions on the timeframe for a response from the controller: no more than six weeks for a definite answer on the processing of personal data, which can be postponed for no more than four weeks. Additionally, France[160] lays down a very specific discipline for the exercise of the right of access and the procedures to be put in place by the controller when identifying the data subject: he or she must prove his or her identity by any means (including using digital identity) that is deemed sufficient by the controller for the authentication. If the controller has reasonable doubts as to the identity of the person, he may request additional information, including, if necessary, a copy of an identity document bearing the individual's signature. Within such procedures, the response period is suspended if additional information were requested for the identification of the data subject.

58 Finally, whilst all scrutinised Member States seem to have implemented Article 15 LED laying down a framework of exceptions to the right of access for security or investigative reasons, some countries embed noteworthy differences. For example, both

145 UK: (n 59), sec 45.

146 Portugal: (n 59), art 13(5).

147 UK: (n 59), sec 53.

148 Belgium: (n 56), art 36.

149 Portugal: (n 59), art 13.

150 Malta: (n 59), art 12.

151 Italy: (n 59), art 9.

152 Belgium: (n 56), art 37.

153 The Netherlands: (n 141) 2007, arts 24a and 26(1).

154 Greece: (n 57), art 57.

155 Italy: (n 59), art 10.

156 Ireland: (n 140), sec 90.

157 Portugal: (n 59), art 14.

158 Belgium: (n 56), art 37.

159 The Netherlands: (n 141) 2007, art 25.

160 France: Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art 105 and Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art 135.

the Dutch[161] and the Portuguese[162] transpositions of Article 15 LED do not seem to fully implement its paragraph 4, thereby not requiring controllers to document (and make available to the supervisory authorities) the factual reasons for a denial. Nonetheless, the Dutch law adds the explicit requirement that the rejection shall be in writing stating the reasons for the rejection. Interestingly, in Cyprus[163], the denial from the controller must be validated after consultation with the NSA (in casu the Commissioner). Upon request from the controller, the Commissioner may draft and publish a catalogue with processing categories that may be subject partly or wholly to restriction. Similarly, the Irish law[164] includes the possibility for a legislative act to expressly lay down a list of data categories to be restricted from the exercise of the right to access on the same grounds as the ones included in Article 15 LED.

b) PNR Directive

59 As mentioned, the very first step before submitting SARs regarding our PNR data was to identify the relevant controllers. Pursuant to the PNR Directive, all Member States appointed in their national laws a single authority to act as the PIU, which functions as the primary controller receiving PNR data from air carriers. It was then deemed important to investigate whether any detailed information on the modalities of exercising the right of access was foreseen by the domestic laws transposing the provisions on the DPO and on the protection of personal data.[165]

60 All scrutinised Member States refer to the national PIU as the designated competent authority to collect and process PNR data from the air carriers. Either through repeating the directive's wording, or by providing further information on, for example, the qualifications and the procedure for appointing a responsible person or entity, all domestic laws refer to the PIUs' DPO. Moreover, all Member States except from France[166] and the UK[167] ensure that the DPO serves as a single point of contact for data subjects to exercise their prerogatives. Luxembourg and Italy are the only countries that further elaborate on the modalities surrounding the right of access. In particular, the Luxembourgish law[168] imposes a specific transparency obligation upon the PIU to disseminate information on the data controller and the processing operations. The Italian law[169], on the other hand, provides that application should be submitted to the central directorate of criminal police, which communicates to the data subject all acts adopted therein.

61 The most intricate legislative framework proved to be the one applicable to the processing of personal data by the Belgian PIU. In particular, the Belgian law transposing the PNR Directive[170] specifies that the provisions included in the general privacy law apply on the processing of personal data by the PIU. While examining the latter, it was discovered that passengers' rights as data subjects are regulated under Title 3, Subtitle 5 of the general privacy law, which stipulates that data subjects only have the right to ask for the rectification or deletion of their data, or the verification, by the "Comité permanent R" that their data are processed in accordance with the guarantees stemming from the general privacy law.[171] These prerogatives, adds the Belgian law, can only be exercised indirectly through the said "Comité permanent R".[172] In any case, the PIU must legally refrain from mentioning that it is even in possession of personal data.[173]

2. Implementation of information obligations

a) Competent authorities

62 After having analysed the national transposition act for each of the investigated countries, we focused on the existence of adequate ex ante transparency

161 The Netherlands: (n 141) 2007, art 27 and (n 141) 2002, art 21.

162 Portugal: (n 59), art 16.

163 Cyprus: (n 58), art 17.

164 Ireland: (n 140), sec 94.

165 PNR Directive, arts 5 and 13, respectively.

166 France: (n 87), art 1.

167 UK: (n 89), art 4.

168 Luxembourg: Loi du 1er août 2018 relative au traitement des données des dossiers passagers, art 30.

169 Italy: Attuazione della direttiva UE 2016/681 del Parlamento Europeo e del Consiglio, del 27.4.2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e disciplina dell'obbligo per i vettori di comunicare i dati relativi alle persone trasportate in attuazione della direttiva 2004/82/CE del Consiglio del 29.4.2004., n. 53, art 23.

170 Belgium: (n 86), art 15(3).

171 Belgium: (n 56), art 173.

172 ibid, art 174.

173 ibid, art 49(3).

measures on the websites of the relevant competent authorities. We looked for both general information detailing the processing operations happening within a law enforcement context, as well as for the practical details necessary for data subjects to exercise their right of access.

63 Since, as discussed above, very few countries clearly indicate the relevant controller in their national transposing laws, we looked for the website of the centralised entity governing the LEAs (either national police authority or the competent ministry) or of the NSA. Our research team then ranked the ease with which it was possible to find meaningful information detailing the modalities and procedure for submitting access requests. On a scale between 1 (very difficult) to 10 (very easy), the average answer was 5.9. Individually, Member States scored very differently, with some websites providing very easily accessible information (like Cyprus or Luxembourg National Polices) and others a more complex presentation (for instance, Belgium's or the Netherland's authorities).

64 After having identified the appropriate websites, our team looked into each of those to understand if and where privacy-related information about the way LED is implemented were present. Out of eleven websites investigated, only Greece did not include any information of such kind.[174] For all the other authorities, information related to privacy policies was included under a dedicated section on their websites. Some countries gather in a single page different links for each privacy policy of the different police databases (e.g. Italy, referring to Schengen, national criminal database, VIS, etc.) or to the relevant legal frameworks (e.g. Greece). Except for Portugal, all competent authorities included the information requested by Article 13(1) LED (controller's and DPO's contact details, purposes for processing, right to exercise access or to lodge a complaint, contacts of the regulators) within the said dedicated webpages. Furthermore, some websites provided additional information such as general retention policy (Italian Police), basic data protection principles (Irish Police) or security of processing (Luxembourg Police). With the exception of the Portuguese Police, all competent authorities' websites also included instructions on how to file a SAR. Out of such a pool, four competent authorities (Ireland, Italy, the Netherlands, the UK)[175] even provided a template SAR to be filled in by data subjects.

174 A data protection policy notice, not easily accessible, was added to the Greek National Police website at a later stage after our access requests were already sent. However, the contact details remained the same.

175 France provides an interactive template on the data protection authority's website (CNIL.fr).

b) Passenger Information Units

65 Having identified the data controller, i.e. each country's PIU, and established that the PIU's DPO serves as a contact point in most Member States, the next step was to look for the DPO's contact details. While locating the PIU online proved an easy task for most Member States, that was not the case for Portugal, Cyprus and Greece. After a careful analysis of the existing ministry and national police websites, national laws and diverse online sources, it was found that the Portuguese PIU belongs to the Single Point of Contact for International Police Cooperation, which in turn works under the authority of the Secretary-General of the Portuguese Internal Intelligence Service.[176] Accordingly, only the general contact details of the overarching authority, i.e. the Portuguese Internal Intelligence Service, were found. More strikingly, the Cypriot and Greek PIUs did not seem to be functional or have any official presence online.[177] Any further research on Cyprus, Greece and Portugal was therefore ceased. The rest of this section refers only to the Member States PIUs for which official information online was found.

66 Out of the eight investigated PIUs, about half were directly linked to law enforcement, and therefore the official website of national police or ministry of justice or defence (Italy, Ireland, Luxembourg, the Netherlands, Malta), and half were linked to another type of governmental website (Belgium, France, the Netherlands, the UK). Interestingly, the British PIU is linked to visas and immigration

176 According to Portugal: (n 59), art 3, the PIU is created within the Single Point of Contact for International Police Cooperation which works under the authority of the Portuguese Internal Intelligence (Portugal: Decreto-Lei 49/2017, art 1), on the website of which no information on the PIU was found <https://www.sis.pt/> accessed 20 October 2020.

177 Several news posts referred to the appointment of a director for the Cypriot PIU without however pointing to any official website of the Cypriot PIU. In order to confirm the existence or non-existence of the Cypriot and Greek PIUs, the national supervisory authorities (NSAs) were first contacted. The Cypriot NSA responded with a three-month delay that any SAR regarding PNR data may be submitted before the Cypriot Police DPO, in the European Union & International Police Cooperation Directorate (EU&IPCD). Regarding the Greek PIU, no specific information was provided by the Greek NSA. One of the authors contacted and submitted a SAR to an airline via which they had travelled to Greece, asking specifically whether their PNR data had been transmitted to the Greek PIU. In their response, the airline confirmed the non-readiness of the Greek PIU to receive data from airlines at the time.

matters, while information on the use of PNR data by the Dutch PIU is divided between the Ministry of Defence and a governmental website on customs and aviation. All but France included a privacy statement, whether generalised (Ireland, Malta, the UK) or more elaborate and PNR-specific (Belgium, Italy, Luxembourg, the Netherlands).

67 Apart from France, these countries also provided information on how to contact the data controller or DPO on the respective websites. To find the relevant information regarding the French PIU and the process to be followed, a general contact form was submitted, the response to which provided the contact details of the PIU Director, to whom the SAR had to be submitted. For the PIUs linked to law enforcement, the SAR had to be submitted to the police/ministry of justice or the police/ministry of justice DPO (Italy, Ireland, Luxembourg and Malta). Concerning the submission of a SAR regarding PNR data within the Netherlands, the option is given to contact customs, the PIU or the respective airline, while it is also made clear that for any rectification or erasure of data all three entities have to be contacted. In order for the SAR to be submitted, most provided an email address though two Member States requested the submission of a physical letter (France and Italy), while a few Member States provided their own template (Italy, Ireland and the UK). All Member States apart from Belgium and the Netherlands further explicitly required identification documents for the submission of the SARs.

68 Taking into account the steps involved in order for the information necessary for the submission of the SARs to be found, the average level of difficulty for all Member States investigated was assessed at 4.6/10 (with 0 being the most difficult and 10 the easiest). Scores varied a lot, with Italy, Luxembourg and Malta being graded the highest.

3. Initial requests

69 After having analysed the national transpositions of both directives in the selected Member States and assessed their compliance with the various transparency obligations, it was time to move on with the actual SARs. In order to ensure the accuracy and comparability of the findings resulting from six individual submissions, we proceeded as follows. First, we shared the results from Survey 1 (dealing with the national transposition of the LED and PNR Directive) and Survey 2 (compiling the findings relating to the transparency obligations) with all participants. More specifically, we highlighted the information related to the contact details that could be used in order to reach the different competent authorities and PIUs as well as the potential procedural requirements. Rather than starting from scratch, all participants could therefore leverage each other's work. Second, all participants filed their initial SARs using templates drafted by and shared among everyone, depending on the countries assigned. Those were redacted in (one of) the official language(s) of the selected countries, so as to smoothen the communication. Third, and as to the sharing of the workload, we proceeded as follows: for the LED, on the one hand, each participant sent an access request to all the investigated countries; for the PNR Directive, on the other, each participant sent an access request to all the countries they had flown from, through or to in the previous six months.

70 This section briefly outlines the form and procedural requirements surrounding the sending of initial access requests, i.e. the very first contact established with both law enforcement authorities and PIUs. When it comes to SARs submitted under the LED, it is worth noting that most competent authorities accepted submissions made in an electronic format, whether through a dedicated contact form or via email. For three countries, namely France, Italy[178] and the Netherlands, however, we had to send our request via regular post. Interestingly, the French Ministry of Home Affairs came back to us explaining that our requests were inadmissible since it was necessary to submit them via regular post – which we specifically did according to the instructions we found when going through the privacy notice of the French competent authority. For the Netherlands, it was possible to choose from the ten Regional Units of the police since there was no clear indication as to which one to contact to exercise a data subject's rights under the LED. As to procedural requirements, the Irish police asked for a proof of residence in the country as well for as a list of all the addresses where we lived while residing in Ireland. Similary the Luxembourgish authorities asked for an address certificate in order to provide their answer via post.

71 Roughly the same can be said when it comes to access requests formulated under the PNR Directive. While we submitted most of our SARs via email, France and Italy still required us to send them via regular post. Surprisingly, a and unlike the modalities applicable to the submission of the SAR under the LED, the Dutch PIU accepted the use of the electronic format. In terms of procedural obstacles, France asked us to provide a proof of residence, Belgium redirected our request to the Belgian Privacy Commission and the UK asked for a certified photo ID together

178 While it was possible to send the request via email in Italy, the only possibility to do so was via Posta Elettronica Certificata (PEC), which in turn required a residential address in Italy. We therefore decided to send the request via regular post, as this was the only option for non-residents to exercise their right of access.

with a signed declaration by a barrister. It is also worth emphasising once again that no official online presence of the Cypriot nor Portuguese PIUs was detected, while the Greek PIU did not appear to be operational at the time we sent our SARs.

4. Following up on the SARs: reminders

72 The follow-up of our requests required us to engage in active correspondence with the addressees. We sent reminders to authorities that had not reacted to our initial applications after two weeks, except for the SARs submitted by post for which a longer reaction time was expected.

73 For the SARs submitted under the LED, reminders were sent to the Cypriot, Greek and Maltese competent authorities. In Cyprus, one reminder from only one of us was enough to trigger a final response to all our SARs within three days. In Greece, however, we all had to send a reminder to prompt the Greek competent authority to gradually answer our SARs. When it comes to Malta, only one member of our team sent a reminder two weeks after the initial request, which triggered the remaining pending responses.[179] As to the SAR submitted under the PNR, we did not send any reminders to the addressees. This is because we either received responses within a time span of two weeks, or because the said requests at issue were submitted by post.

74 The key takeaways from the submission process relate to the exercise of the right of access under the PNR Directive, notably our experiences in Belgium and Italy. When it comes to Belgium, one member of our team was contacted by phone by the addressee of our requests two week after the initial submission, with the aim of obtaining more information before proceeding with our requests. Interestingly, the staff member showed a certain lack of linguistic flexibility,[180] despite the fact that PNR SARs can be expected from citizens not necessarily speaking any of the official languages of the country at issue. More striking though is the fact that, by the end of that phone interaction, the Belgian official, recipient of our SARs, asked for the phone number of another member of our team.[181] When in comes to our experiences in Italy, we received access to the PNR data of a person who was totally unrelated to our legal-empirical endeavour.

5. Final responses to the SARs

75 Overall, our SARs have been fully processed in most countries, in the sense that we had received a definitive answer - whether positive or negative - by the end of the allocated time frame. The responses we obtained range from a mere refusal to share anything to the disclosure of the personal data being processed. Yet, our successful attempts mostly resulted in the confirmation as to whether or not personal data concerning us were being processed, as analysed below.

76 Regarding our experiences under the LED, the most common response we obtained consisted of the indication that no data about us was being processed. Only SARs submitted to competent authorities in Greece, the Netherlands and the UK resulted in the provision of any information other than (or in addition to) that. The Greek competent authority provided a list of all the categories of data they held as well as the legal basis for the processing (though not the personal data as such). In the Netherlands, the additional information provided contained a detailed account of the databases that were consulted when processing the SARs, as well as a word of explanation on those databases. Lastly, in its response letter to our SARs, the UK competent authority specified that the information provided to us did not involve data held on local police systems, thus implying the possibility of obtaining a different response if the SARs were submitted to local police forces.

77 In two countries (namely France and Portugal), our SARs were dismissed. The French competent authority refused to comply on the grounds that our requests were "manifestly abusive"[182] given their overly broad scope; thus, to proceed with the requests, we had to indicate the exact files we were requesting access to (as indicated in the response letters). The refusals by the Portuguese competent authority, were based on the lack of compliance with all the formal requirements (according to the refusal letters). Surprisingly though, the alleged procedural shortcomings of our SARs relate to

179 Considering that half of our SARs had already received final responses by that time, as specified in the following section.

180 This lack of flexibility relates to the fact that the staff member reluctantly switched to English during the phone interaction.

181 More than strikingly, we find it a worrying practice whereby, while processing a SAR, another data subject's name is mentioned and personal records about that person are attempted to be extracted in that way. This can be considered a reckless manner of processing SARs. As a result, we reacted informing the authority of the reception of such a mishandled response.' after 'SARs.

182 Own translation from the literal words used in the response letters.

formal requirements that are not specified (or referred to) in the national implementation act of the LED in Portugal.[183]

78 It took competent authorities a median of three to 61 days to fully process our SARs under the LED.[184] The fastest final responses were provided by the Belgian, British and Maltese competent authorities (with a median of three, eleven and fifteen days, respectively), while the Irish, French and Italian competent authorities took the longest to respond (thirty-two, fifty-four and sixty-one days, respectively). It should be noted that Luxembourg was the last country to respond to our SARs (in September 2020, i.e. over six months after the initial requests).

79 At this point, it is worth highlighting some practical insights gathered during the research, mostly related to our experiences when exercising our right of access under the LED. In Malta, we had somewhat diverging experiences as regards to the time it took the competent authority to provide final responses to our SARs. The Maltese competent authority provided final response to half of our SARs within three days after submission. The remaining responses were provided in the subsequent days, following a reminder that one member of our team sent two weeks after submission (as specified in the previous section). Given that the addressees of our requests explicitly expressed facing organisational challenges resulting from the COVID-19 crisis, we assume that the differing experiences in Malta might be due to the possible impacts of the pandemic on the follow-up process.

80 Notwithstanding the above, the Maltese addressee responded to our SARs in time, in a friendly manner, and without trying to make data subjects regret attempting to exercise their access rights. The same can be said for the UK where requesting access to our personal data proved a fruitful and straightforward exercise, in particular because of the availability of an online form and the swiftness with which our applications were processed. Thus, the practical evidence gathered at this stage of the research seems to suggest that Malta - among the investigated countries - and the UK are probably two of the European countries where requesting access to personal data under the LED tends to be a straightforward exercise. Ireland and Luxembourg, on the contrary, proved to be more burdensome. In Ireland, we had to satisfy more formal requirements than the ones listed in the national implementing act of the LED and in the template provided on the website of the competent authority. In particular, we were asked to provide a proof of our address (as specified in the template), but also a proof of previous addresses where we "resided while staying in Ireland".[185] In Luxembourg, our exercise was similarly burdensome, time-consuming, and required more interactions with the addressee.

81 As to our SARs under the PNR Directive, the responses we obtained were more varied than those under the LED. Whereas in some countries we only received the information that no data about us was being processed, in France, Italy and the Netherlands, our SARs resulted in the actual disclosure of data undergoing processing. In France, instead of merely confirming that personal data were being processed, the PIU provided the specific flight information held in the PNR system. We obtained a similar response to part of the SARs submitted in Italy.

82 The response to our PNR requests in the UK deserves particular attention. The UK addressee reacted within two days of our initial requests indicating that, to process the SARs, it was necessary to provide a certified photo ID via signed declaration by a barrister. It was impracticable for us to proceed according to the addressee's instructions, especially in times of the COVID-19 crisis. As a result, we did not follow-up on that request. Given our failure to comply with all the formal requirements, it is reasonable to assume that our SARs would eventually have been refused because of a formal defect.[186]

83 It took PIUs a median of two to 87 days to fully process our SARs. The Irish, British and Maltese PIUs were the fastest to process our requests (within two, two and seven days, respectively), while the Dutch, French and Belgian addressees took the longest time to respond (56, 59 and 87 days, respectively).

183 This seems to indicate that in Portugal it can be difficult for a lay person to understand what are all the formal requirements to exercise their subject access rights, unless individuals can obtain the necessary understanding of the law by seeking legal advice.

184 The median was chosen over the average to avoid outliers relating to the current COVID-19 crisis, which coincided with the empirical study.

185 A requirement that seems to suggest that only individuals who reside or have resided in Ireland are entitled to request access to their personal data, which is nowhere to be found in the national implementing law.

186 Although that was never explicitly said by the UK addressee of our requests.

F. Assessment of law and practice

I. Implementing fallacies

84 Our research on information obligations revealed slight differences in the wording and the formulation of the right of access and its limitation in national transposing laws. Whilst the general line is that such implementations remain rather high level, a few countries opted to include practical provisions on how and where to find useful information for the exercise of access requests. With regard to the modalities for the exercise of the right of access, the study points to very different scenarios. Nevertheless, the majority of the competent authorities scrutinised seem to include the basic information for the exercise of SARs within their websites, in compliance with the spirit of "facilitation of data subject rights" substantiated in Article 12(2) LED. A noteworthy finding regarding both the LED and the PNR Directive in Belgium is that it only seems possible to submit indirect SARs. In other words, the request could only be filed through the NSA, rather than directly to the competent authority or PIU, through the legally appointed single point of contact, i.e. the DPO.

85 The transposition of the information obligations under the PNR Directive was not without issue either. Collecting all relevant information before submitting the SARs before the national PIUs scored an average high level of difficulty due to their absence or inaccessibility. Moreover, the reality of the situation was often at odds with the legal fiction. That was the case with the seemingly non-functional Greek PIU. PIUs are intended to function independently and contact the competent authorities when relevant in accordance with their analyses, they may be "seconded" by competent authorities[187] but remain nonetheless distinct. However, in most Member States, PIUs are institutionally linked to LEAs, as they are founded within the same Ministries[188] or within the Police itself.[189]

86 Finally, requirements such as proof of residency, only came up when looking for the means to submit our SARs, without being stipulated in the national laws. Such requirements came across as arbitrary and impeded our SARs, especially given the commonly present language barriers between the residence of the requesting party and the location of the addressee of the request.

II. Inadequate responses

87 For the most part, our practical exercise of the right of access under both the LED and the PNR Directive resulted in the mere confirmation as to whether or not personal data about us were processed, which appears to be the customary response to SARs in the context of security. The responses obtained in our study rarely disclosed anything else. Moreover, none of the responses we received involved any details that could hint at security-related processing practices in the targeted countries. While somewhat short, such customary responses can nevertheless be considered legally compliant. Interestingly though, while national transposing laws essentially coincide with the LED on the information to be made available to data subjects[190], none of the responses we received disclosed all the pieces of information listed in the LED. This was the case even for the responses which provided the actual personal data. The pieces of information that were left out were details such as the recipients to whom the personal data have been disclosed, the envisaged storage period, and the indication of a right to rectification or erasure.

88 Moreover, it is striking that the only "access" to information that we obtained from the Belgian competent authorities and PIU was the indication that the necessary verifications had been made as to the lawfulness of the processing. In other words, our SARs in Belgium did not even result in the customary response we identified in our study (i.e. the confirmation as to whether or not personal data are being processed), but rather the mere indication that the processing of the data (if any) was done lawfully, as the NSA could confirm.

89 The results of this empirical study also show that, in some European countries, it can be difficult for a lay person to decipher all the formal requirements that are necessary for the exercise of the right of access under the LED and the PNR Directive without the advice of legal experts. In some countries, the addressees of our SARs alluded to our lack of compliance with all the formal requirements to make SARs. Yet, in most (if not all) the cases, the alleged deficiencies were not specified (or even referred to) in the national transposing acts. Moreover, the formal requirements at issue were nowhere to be found in the information obligation measures implemented by Member States.

187 PNR Directive, art 4(3).

188 Belgium, Cyprus, Italy, Ireland, the Netherlands, the UK.

189 Greece, Malta, Luxembourg, Portugal.

190 LED, art 14.

G. Ways forward and recommendations

90 Looking back at the findings outlined in this contribution, one can highlight some ways forward and potential recommendations for competent authorities and PIUs, as well as policy makers, to better comply with both their ex-ante and ex-post transparency obligations.

91 First, participants have frequently highlighted the lack, or incompleteness, of proper transparency measures when trying to exercise their right of access. They were often confronted with scarce, hard-to-find or even conflicting information as to the ins and outs of the processing operations taking place in a law enforcement or PNR context. The same goes for the instructions regarding the exercise of data subject's rights. As emphasised in similar empirical initiatives,[191] adequate and comprehensive information is an essential prerequisite for individuals to understand if and how their personal data are processed and, in such case, whether and how to exercise their right to enquire about certain aspects of those processing operations. As such, it is crucial that competent authorities and PIUs implement comprehensive, intelligible and easily accessible transparency measures, since those will pave the way for data subjects to exercise their prerogatives. To that end, it is important to cultivate a data protection culture and understanding amongst security authorities and officers, whereby a data subject's rights do not consist of a and promote data subject's rights that are not a niche reserved to data protection lawyers, but benefit all individuals subject to EU law. Data subjects should, in that sense, not feel bad about exercising their prerogatives; nor should competent authorities and PIUs make them feel so in their answers.

92 Single points of information could, in that sense, prove invaluable by not only providing all the necessary information in one place but also avoiding inconsistencies between the various competent authorities and PIUs, should multiple actors be competent in a single country. This could take the form of a website centralising all the information about the processing of personal data in a security and law enforcement context, together with a dashboard gathering the relevant contact details for individuals to exercise their prerogatives. Similarly, the use of automated submission forms, or the provision of a standardised template, would drastically streamline the process for data subjects who are less familiar with the applicable regulatory framework. Finally, barriers such as the requirement for the SAR to be sent via regular or certified post, as well as the need to provide a certificate of residency or an address in the country, should be lifted – even if that would entail modifying the corresponding transposing legislation.

93 Second, participants experienced significant disparities in the handling of their requests depending on the Member State investigated. Those differences ranged from procedural requirements – as hinted above – to the scope of the right of access itself – as we have seen in Belgium, for instance. While this is inherent to the nature of the regulatory instruments dealing with the matters at stake, it also makes it extremely complex for data subjects to exercise their prerogatives against competent authorities and PIUs in different countries. This is all the more problematic given that the collection and processing of individuals' personal data for law enforcement or PNR purposes is not limited to their country of residence or nationality. As such, data subjects might have an interest in requesting access to their data in multiple jurisdictions.

94 In light of the above, guidance from NSAs, which, according to our research, most commonly act as the oversight bodies for the GDPR but also the LED and the PNR Directive, could orient and complement the transparency measures adopted by competent authorities and PIUs with guidance and best practices as to how to handle requests emanating from data subjects. In the field of law enforcement, such national efforts could also be encouraged and coordinated by the European Data Protection Board on its own initiative, upon request of one of its members or of the European Commission, as foreseen in Article 51(1)(b) LED. This would be especially welcome with respect to the modalities surrounding the handling of a data subject's rights such as the form in which the request should be formulated, the medium to be used for communicating the said data, the appropriate security and identity verification procedure and the extent of the delay to be observed by competent authorities and PIUs.

95 The EU institutions and policy bodies at large are equally entrusted with promoting and facilitating the harmonisation of data protection safeguards in general, and the exercise of data subjects' rights in particular. The European Commission is engaged to disseminate best practices "through its regular meetings with the Member States and the projects financed under the ISF-P Union actions".[192] It is therefore recommended to accentuate the focus on the exercise of data subjects' rights within these best practices, which seem primarily directed to inter-institutional relations. This will become even more important as the expansion of the

191 See Galetta, Fonio and Ceresa (n 25), Norris (n 25), Ausloos and Dewitte (n 25).

192 Commission (n 29).

scope of application of the PNR Directive to other transportation sectors, such as maritime and rail, is currently being considered.[193] National practices regarding air traveling under the PNR Directive will in that case likely consist of the prototypes upon which other domains will be built.

96 Insofar as the relation between the two directives is concerned, the European Commission, in its report "Ways forward on aligning the former third pillar acquis with data protection rules" published in June 2020[194], has provided an assessment of which legislative acts should be modified in order to be better aligned with the LED[195]. In its assessment, the European Commission concluded that the need to align the PNR Directive with the LED will be further assessed, also taking into account the pending cases before the CJEU. A month later, however, the review report on the PNR Directive did not identify the need to amend in any way the directive.[196] Further clarification regarding the relation between the LED and the PNR Directive, in particular regarding the applicability of data protection safeguards, is considered imperative, due to the restricted manner in which the PNR Directive points to specific data protection rights and obligations (in the CFD)[197].

97 Finally, given the discrepancy between the findings of the PNR Directive review report made publicly available until now, and the findings within this paper, we consider that there is room for improvement also in relation to European supervision. In particular, stronger oversight of the implementation of the directives, forcing Member States to fully comply in both law and practice, so as to remedy the identified gaps and fallacies, is strongly recommended.

H. Conclusions

98 This paper sought to outline the legal framework regarding data protection and the data subject's right of access in the contexts of law enforcement and security as well as its implementation under the LED and the PNR Directive. In theory, the right of access is an essential tool that should empower individuals, whilst at the same time preserving the aims of security and security authorities. The process should comprise a careful and well-thought out balancing of interests and informational power asymmetries. Our intent through the empirical study we conducted in eleven Member States was to evaluate the materialisation of the right of access, and point out potential problems and obstacles that may come up during this process in practice. While a valiant effort has been made on behalf of the investigated Member States to properly implement the LED and the PNR Directive, there is still room for improvement in order to facilitate and provide a more transparent and comprehensive procedure to be followed by data subjects who wish to exercise their right to access.

Note: For detailed information about the competent authorities and PIUs websites and Privacy Notices therein see the following page

193 Commission (n 29).

194 European Commission, 'Ways forward on aligning the former third pillar acquis with data protection rules' (Communication) COM (2020) 262 final.

195 LED, arts 60 and 62(6).

196 Commission (n 29).

197 PNR Directive, art 13.

I. Annex: Notice and Addressee per Country

Country	Notice / Addressee	Competent Authorities	Passenger Information Units
Belgium	Notice	Website of the Belgian police) (www.police.be/en/privacy)	Website of the Crisis Centrum (https://crisiscentrum.be/nl/inhoud/belpiu-collection-and-processing-passenger-data)
	Addressee	Organe de contrôle de l'information policière – COC (info@organedecontrole.be)	BelPIU (belpiu.dir@ibz.fgov.b); redirected to Comité permanent de contrôle des services de renseignements – Comité R (info@comiteri.be)
Cyprus	Notice	Website of the Cyprus Police (https://www.police.gov.cy/police/police.nsf/page09_en/page09_en?opendocument)	/
	Addressee	Cyprus Police (police@police.gov.cy)	/
France	Notice	Website of National Police (https://www.police-nationale.interieur.gouv.fr/Presentation-generale/Deontologie-et-controle) linking to the website of the CNIL (https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t)	Website of the Passenger Information Unit (https://pnr.gouv.fr/eng/About-PIU)
	Addressee	Direction Générale de la Police Nationale, Ministère de l'Intérieur, 96 place Beauvau, 75800 Paris CEDEX 08	Directeur de l'UIP, Système API/PNR France, BP 16108, 95701 ROISSY-CDG
Greece	Notice	Website of the Greek Police (http://www.astynomia.gr/index.php?lang=EN) and dedicated webpage only available in Greek (http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=93512&Itemid=114&lang=)	/

Ireland	Notice	Website of the Irish Police (https://www.garda.ie/en/information-centre/data-protection/)	Website of the Irish Immigration Service Delivery (https://www.irishimmigration.ie/irish-passenger-information-unit/)
	Addressee	Irish Police's Data Protection Unit (DataProtection@garda.ie)	Irish Passenger Information Unit (IPIUdataprotection@ipiu.gov.ie)
Italy	Notice	Website of the Italian Police (https://www.poliziadistato.it/articolo/4075de1317ccbefa885830601)	Website of the Italian Police (https://www.poliziadistato.it/articolo/4075dd2a3ecbd99f764225475)
	Addressee	Ministero dell'Interno, Dipartimento della Pubblica Sicurezza, Direzione Centrale della Polizia Criminale, Via Torre di Mezzavia 9, 00173 Roma; holders of a certified email box could also submit an access request electronically using dipps.dcpcufficiocontenzioso@pecps.interno.it	Ministero dell'Interno, Dipartimento della Pubblica Sicurezza, Direzione Centrale della Polizia Criminale, Via Torre di Mezzavia, 9, 00173 Roma; holders of a certified email box could also submit an access request electronically using privacy.pnr@pecps.interno.it
Luxembourg	Notice	Website of the Luxembourgish Police (https://police.public.lu/fr/support/aspects-legaux/2018-rgpd.html)	Website of the Luxembourgish Police (https://police.public.lu/fr/legislation/uip-pnr.html)
	Addressee	Luxembourgish Police's Data Protection Officer (dpo@police.etat.lu)	Direction Générale – Direction des relations internationales – Cellule juridique (dri.cj@police.etat.lu)
Malta	Notice	Website of the Maltese Police (https://pulizija.gov.mt/en/police-force/Pages/Data-Protection-Policy.aspx)	Website of the Maltese Police (https://pulizija.gov.mt/en/police-force/Pages/Data-Protection-Policy.aspx)
	Addressee	Commissioner of Police (dpu.police@gov.mtn)	Commissioner of Police (dpu.police@gov.mtn)

Nether-lands	Notice	Website of the Dutch Police (https://www.politie.nl/algemeen/privacy.html?sid=228463d3-72e3-4434-8947-933a8e3d3756)	Website of the Dutch Government (https://www.government.nl/topics/aviation/air-passenger-travel-information) and a dedicated webpage not available in English (https://www.rijksoverheid.nl/onderwerpen/luchtvaart), and website of Ministry of Defence (https://www.defensie.nl/organisatie/marechaussee)
	Addressee	Landelijke Eenheid, T.a.v., Privacydesk, Postbus 100, 3970 AC DRIEBERGEN and Amsterdam Eenheid, T.a.v., Privacydesk, Postbus 2287, 1000 CG AMSTERDAM	Passagiersinformatie-eenheid (FG-Pi-NL@minjenv.nl)
Portugal	Notice	Website of the Portuguese Police (https://www.psp.pt/Pages/Politica_de_Privacidade/PoliticaPrivacidade.aspx)	/
	Addressee	Inspeção da Polícia de Segurança Pública (inspger@psp.pt)	/
United Kingdom	Notice	ACRO – Police Criminal Records Office https://www.acro.police.uk/SA-Further-guidance	Website of Home Office (https://www.gov.uk/government/publications/requests-for-personal-data)
	Addressee	Form online to be filled on the ACRO website https://www.acro.police.uk/Subject-Access-Online	Online form (https://www.gov.uk/government/publications/requests-for-personal-data) or email contact: SARUOnlineID@homeoffice.gov.uk

Net Neutrality And Free Choice Of Routers And Modems In Europe

by **Lucas Lasota***

Abstract: This paper provides context to the right to choose and use internet access equipment as a fundamental element of net neutrality in Europe. It sheds light on the developments over harmonisation of rules from 2016 to 2020 and analyses the future challenges involving the definition of the Network Termination Point, which will determine whether routers and modems should be treated as aspects of the private or public infrastructure. This study also presents insights regarding the free choice of terminal equipment as reflected in the annual reports prepared by National Regulatory Agencies on net neutrality.**

Keywords: router; modem; network neutrality; network termination point; telecommunications law

Recommended citation: Lucas Lasota, Net Neutrality and Free Choice of Routers and Modems in Europe, 11 (2020) JIPITEC 303 para 1.

A. Introduction

1 Routers and modems are essential hardware for internet access, transferring data packets along the computer networks by determining the paths to their specific destinations. Since this equipment can be placed on the edge between private and public networks, its ownership has been the subject of discussion[1] in the context of the network neutrality (net neutrality) debate for the last five years in Europe[2]. The implementation of rules regulating the use of private equipment for internet access has followed diverse paths among European countries,

* Associate Researcher at the Humboldt University of Berlin and Deputy Legal Coordinator at the Free Software Foundation Europe. This article does not necessarily reflect the views of any organisation the author may represent.

** The author thanks Richard Schmeidler and the anonymous reviewers for the insightful comments.

1 The public debates have coined such terms as "router freedom", "compulsory routers", "device neutrality" and "device freedom" to refer to the right of equipment choice. See e.g.: "Modem Libero" in Italy <www.modemlibero.it/chi-siamo/> and "Routerzwang" in Germany <https://fsfe.org/activities/routers/timeline.de.html> both accessed 25.08.2020.

2 This article will focus mainly on the developments after the adoption of Regulation (EU) 2015/2120, as it represented the introduction of the net neutrality regulatory framework in Europe and, consequently, the right to choose and use routers and modems.

creating a fragmented regulatory patchwork. This panorama is characterised by enhanced complexity due to the looseness of the specification of the location of the Network Termination Point (the NTP), which is the boundary between the end-users' private and the Internet Access Providers' (the IAPs')[3] network equipment. Specifying the location of the NTP is a task of the National Regulatory Agencies (the NRAs). Jurisdictions can have different identifications of the location of the NTP. Choosing can be a source of tension between the interests of consumers and IAPs. This paper captures the notion of free choice of routers and modems as a principle of net neutrality and the challenges of its adoption in Europe. The analysis will refer mainly to the documents produced by the Board of European Electronic Regulators (BEREC) relating to the NTP, as well as the NRAs' annual reports on net neutrality from 2017 until 2020, to evaluate the regulators' performance in reporting issues and solutions concerning the right to freely choose terminal equipment.

2 This article is divided into two parts. First, the free choice of terminal equipment will be put into the context of efforts to implement and harmonise net neutrality rules in Europe. For that, Regulation (EU) 2015/2120 (the Net Neutrality Regulation)[4] and the technical set of rules regarding the NTP prepared by BEREC will serve as the main sources of analysis. Since the European Electronic Communications Code (the EECC)[5] is the most recent set of rules concerning equipment neutrality to be transposed to national jurisdictions, the second part of this article is dedicated to inspection of the NRAs' monitoring of issues of free choice of terminal equipment in 2017-2020, based on the annual reports presented to the European Commission on the NRAs' enforcement activities regarding net neutrality[6].

3 Although this article uses the term Internet Access Providers (IAPs), in art. 2(c) Directive 2002/21/EC (Framework Directive) companies providing the "last mile access" are denominated "Electronic Communications Network Providers". The Board of European Electronic Regulators (BEREC) in its several guidelines related to the freedom of terminal equipment has used the more generic term "Internet Service Provider (ISP)"

4 This article will refer to Open Internet Regulation (EU) 2015/2120 as the Net Neutrality Regulation, as it contains the main source of net neutrality principles.

5 Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code.

6 Commission, 'Annual country reports on open internet from national regulators' (Shaping Europe's digital future, 10.06.2020) <https://ec.europa.eu/digital-single-market/en/policies/open-internet> accessed 08.01.2021.

B. Are end-users allowed to use their own routers in Europe?

3 The right of free choice of terminal equipment has been codified in Europe since 2015 by the Net Neutrality Regulation, which sets out the main principles for internet access for end-users. The terms for its implementation are conditioned by other rules which depend on further specification of the NTP by NRAs in accordance with BEREC harmonisation guidelines. Specifying the location of the NTP is important not only in relation to the free choice of terminal equipment, but also in relation, for instance, to traffic management, transparency, enforcement and monitoring mechanisms. The main elements of this fragmented and complex regulatory patchwork will be analysed below.

I. Free choice of terminal equipment as a net neutrality principle

4 Net neutrality represents the latest phase of a debate over control of communications media in the broader context of the digital transformation of social life through the Internet[7]. The Internet evolved from

7 The public debate in Europe started with the review of the Telecommunications Framework from 2007-2009 extending the discussions already taking place in the US during the 2000s. The European legislative activity culminated with the Net Neutrality Regulation in 2015. For an historical overview on the evolution of the position of the stakeholders in the debate and the elements of the broad definition of the concept, see in the US: M. Lemley / L. Lessig, The end of end-to-end: Preserving the architecture of the Internet in the broadband era. (2000) UCLA L. Rev. 48; T. Wu, Network neutrality, broadband discrimination. (2003) J. Tele-comm. High Tech. Law 2, p. 141–179. In Europe, see: S. Schlauri, Network neutrality – Netzneutralität als neues Regulierungsprinzip des Telekommunikationsrechts, (Baden-Baden 2010); BEREC, Response to the European Commission's consultation on the open Internet and net neutrality in Europe. (BoR (10) 42, 30.09.2010); C. Marsden, Net Neutrality: Towards a Co-regulatory Solution. (Bloomsbury Academic 2010); Cave and P. Crocioni, Net Neutrality in Europe. (2011) Communications & Convergence Review; European Parliament, Network Neutrality: Challenges and Responses in the EU and in the U.S. (Brussels 2011); M. Kloepfer (ed), Netzneutralität in Der Informationsgesellschaft. (Beck 2011); J. Sluijs, Network Neutrality and European Law, (Nijmegen 2012); A. Strowel, 'Net Neutrality: What Regulation for the Internet in Europe and Beyond?' Net Neutrality in Europe - La neutralité de l'Internet en Europe (Bruylant 2013); J. Krämer, L. Wiewiorra

a limited state-controlled project to the largest computer network in the world, encompassing not only information exchange alone, but also a sophisticated multidisciplinary network for human interaction, communication, data processing and storage, and control of digital infrastructure. In this sense, access to the Internet has become a central prerequisite for individuals exercising rights and freedoms in the information society[8]. Net neutrality is intended to protect the basic rights of internet users against opaque and invidious practices by their IAPs. That means, in general terms, no throttling, no blocking of rival content and no discrimination of users, content, platform, application, type of equipment, source address, destination address or method of communication, except under narrowly defined conditions[9].

5 When accessing the Internet, end-users should be free to choose between various types of equipment. IAPs should not impose restrictions on the use of terminal equipment connecting to the network in addition to those imposed by manufacturers or distributors of terminal equipment. These principles are condensed in art. 3(1) of the Net Neutrality Regulation, comprising measures intended to safeguard net neutrality, covering end-users' rights and IAPs' obligations: "*End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service*". As an EU Regulation, it requires no transposition into national law and enjoys primacy in application over national laws. It applies equally in all EU member states and three additional states of the European Economic Area (EEA) (Norway, Iceland and Liechtenstein).

6 For the terms of the Net Neutrality Regulation, "end-users" encompass individuals and businesses, including consumers[10]. "Terminal equipment"[11] relates to devices that directly or indirectly connect to the interface of a public network. This interface, the NTP, is defined as the physical point at which a subscriber is provided with access to a public communications network[12]. The location of the NTP has an impact on whether the router and modem are part of the IAPs' network or end-users can use their own equipment to access the Internet, as seen in Image 1. If the NTP is located at point A, both modem and router are part of the domain of the end-user. At point B the end-user can have only the router and has to use the modem of the network operator. At point C modem and router belong to the network operator. As an element of net neutrality, this article considers that only having the NTP be at point A is compliant to art. 3(1) of the Net Neutrality Regulation. The NTP can be mobile rather than fixed, as when smartphones are used for internet connection[13].

et al, Net neutrality: A progress report. (2013) Telecomm. Policy 37 (9): p. 794–813; J. Osing, Die Netzneutralität im Binnenmarkt. (Nomos 2017).

8 The correlation between net neutrality and human rights became clear with the revelations of 2013 by Edward Snowden which demonstrated the IAPs' long-term cooperation with law enforcement on mass or individual surveillance. See: P. Aust, *Spionage im Zeitalter von Big Data - Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht.* (2014) AVR 52; M. Peuker-Minecka, *Netzneutralität als grundrechtliche Gewährleistungspflicht*. (Univ. Dissertation, Jena 2014); W. Schulz / J. van Hoboken, *Human Rights and Encryption* (UNESCO 2016); C. Marsden, *Network Neutrality: From Policy to Law to Regulation.* (Manchester University Press 2017); M. Reglitz, *The Human Right to Free Internet Access*. (2019) J. Appl. Philos., 37: p. 314-331. For the definition of the term "information society", see: J. Feather. *The Information Society: A study of continuity and change.* (Facet 2017).

9 Net neutrality encompasses complex and multi-faceted concepts, involving several regulatory arenas. Together with freedom of terminal choice, privacy and data protection issues involving traffic management by the IAPs, differential pricing practices (zero-rating) and "specialised services" are central topics in the broader spectrum of the debate. The Net Neutrality Regulation brought a review clause, by which the Commission must issue a report every 4 years starting in 2019 to monitor the implementation of net neutrality in Europe. For the first one, the law firm Bird & Bird, in consortium with the research and consultancy company Ecorys, was tasked by the Commission to conduct a review based on inquiries to various stakeholders ranging from NRAs to operators and civil society organisations. See: Commission, *Study on the Implementation of the Open Internet Provisions of the Telecoms Single Market Regulation.* (Publications Office of the European Union 2019). The historical Covid-19 pandemic affected net neutrality. In 2020, internet traffic greatly increased following confinement measures. The Commission and BEREC set up monitoring mechanisms for traffic treatment and internet access. To prevent network congestion, exceptional traffic management measures were allowed. See: Commission, 'Reports on the status of internet capacity during coronavirus confinement measures'. (*Shaping Europe's digital future*, 29.04.2020) <https://ec.europa.eu/digital-single-market/en/news/reports-status-internet-capacity-during-coronavirus-confinement-measures> accessed 26.11.2020.

10 Art. 2(n) of the Framework Directive.

11 Art. 1(a) of Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment.

12 Art. 2(a) and (d) of the Framework Directive.

13 This paper deals mostly with fixed NTPs. For mobile NTPs,

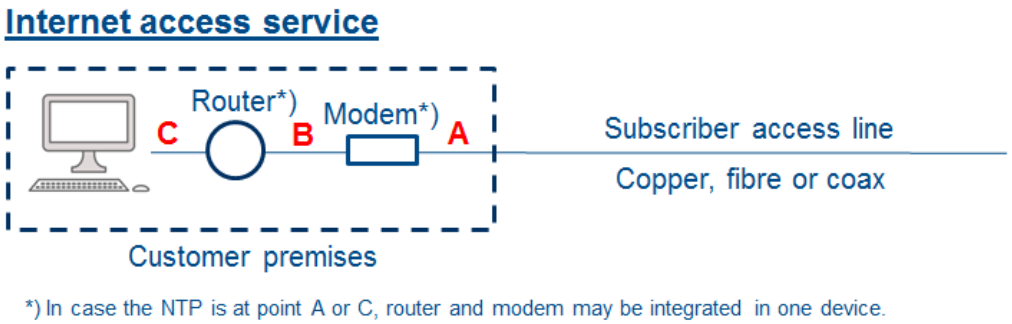

Image 1: The three possible locations of the fixed NTP according to BEREC[14].

7 Normally, all internet-based communication passes through routers[15]. While the modem brings the information in, the router distributes (or "routes") it to different devices. Routers share information between computers and connect to the internet through a modem. Since routers can handle other functions too, for instance WiFi, Voice over IP (VoIP) and TV streaming, and also technical details such as port forwarding, dynamic DNS or VPN tunnelling, routers and modems are quite often offered by IAPs in the same device. All major consumer IAPs are vertically integrated to some extent with content (video, streaming, audio, etc.) services, in such a way that routers and modems represent important elements in their business models[16]. End-users connect to the Internet mainly through the IAPs' networks[17]. Therefore, IAPs hold a position of power for providing unique public service, demand special treatment from governments and impose their own equipment on consumers with relative flexibility[18].

8 Freedom of terminal equipment is considered a fundamental element of net neutrality. This is based on principles of freedom of choice, privacy, compatibility, fair competition, security and data protection. Although a combined router/modem unit provided by an IAP can be a simpler option for most end-users, some of them may wish for features not provided by the IAP to meet security and privacy requirements . Besides, end-users regularly change their IAPs. Only if they can continue using their own devices, can they port their existing settings and devices to the new provider . If the devices are owned by the IAPs, compatibility to other providers and their specific requirements might be limited . End-users should also profit from the free and fair competition that guarantees free choice and steady improvement of products. The lack of competition can come at the expense of the user because security features would be continually reduced and the user-friendliness would drop .End-users should also profit from the free and fair competition that guarantees free choice and steady improvement of products. The lack of competition can come at the expense of the user because security features would be continually reduced and the user-friendliness would drop[19].

9 Freedom of terminal equipment encompasses the physical aspect of internet connections. This freedom requires setting standards for IAPs' practices to-

BEREC has stated that "*since end-users use their mobile equipment (e.g. smartphones) for internet connection in the 27 EU member states, there is no objective technological necessity for mobile equipment to be considered as part of the public mobile network*". BEREC, *Guidelines on Common Approaches to the Identification of the Network Termination Point in Different Network Topologies*. (BoR (20) 46, 05.03.2020), p. 24.

14 BEREC, *Location of the Network Termination Point*. (BoR (18) 159, 04.10.2018), p. 7.

15 This article focuses on routers and modems used by end-users for personal purposes. For other roles of routers in networks, see e.g.: C. Severance, *Introduction to Networking: How the Internet Works*. (Sue Blumenberg, 2015).

16 For economic integration of routers and modems into IAPs' business strategies, see: W. Lehr, *Understanding Vertical Integration in the Internet*. (EURO CPR 1998) J. Kranz / A. Picot, 'Internet Business Strategies', *Handbook on the Economics of the Internet*. (Edward Elgar, 2016); F. Schuett, *Network neutrality: A survey of the economic literature*. (2010) Rev. Network Econom. 9 (2): p. 1-15; N. Economides / B. Hermalin, *The economics of network neutrality*. (2012) Rand J. Econom. 43 (4): p. 602–629.

17 See e.g.: B. Leiner, V. Cerf et al, *A Brief History of the Internet*. (2009) ACM SIGCOMM Computer Communication Review, p. 22–31.

18 Marsden (n 8), p. 2.

19 For competition concerns affecting end-users raised by stakeholders during the BEREC public consultation on the NTP Guidelines, see: BEREC, *Report on the Outcome of the Public Consultation on Draft BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in Different Network Topologies*. (n 21), p. 34–39.

wards end-users in order to safeguard open, neutral and secure access to the Internet. The next section addresses the harmonisation process of this right across Europe.

II. BEREC's role in harmonising EU rules on the NTP

10 Since 2015, the European Union has formally implemented net neutrality rules encompassing free choice of routers and modems. The regulatory framework is intended to protect end-users and guarantee the continued functioning of the internet ecosystem as an engine for innovation. However, the effectiveness of this framework will depend on how NRAs deal with the harmonised concepts proposed by BEREC in its guidelines and reports on the NTP. BEREC is commissioned by EU laws in two respects to provide guidance on the implementation of the obligations of NRAs[20]. While NRAs "must take utmost account" of BEREC decisions[21], they are not legally required to follow BEREC guidelines[22]. Particularly for the choice of terminal equipment, the following set of documents can serve as basis for calibrating the future regulatory behaviour of NRAs:

1. The BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, 30.08.2016[23];
2. The BEREC Report on the Location of the Network Termination Point, 04.10.2018[24]; and
3. The BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies, 05.03.2020 (the Guidelines on the NTP)[25].

III. The BEREC guidelines on the Implementation by National Regulators of European Net Neutrality Rules, August 2016

11 By art. 5(3) of the Net Neutrality Regulation, BEREC was commissioned to provide guidance on the implementation of the net neutrality obligations of NRAs. These Guidelines represent the first document on interpretation of net neutrality rules issued by BEREC. Following the principles contained in the Regulation, the Guidelines set up the first regulatory environment for NRAs. Notwithstanding that it recognises the prohibition against limiting the choice of terminal equipment, BEREC only mentions that NRAs should consider whether there is an "objective technological necessity for the obligatory equipment to be considered as part of the IAP network". If there is no objective technological necessity, an IAP's subjective desire to limit router freedom would be in conflict with the Net Neutrality Regulation (paragraphs 26 and 27)[26].

12 As will be discussed below, limiting the NRAs' discretionary power to determine a vague and unproved necessity will be the major challenge for end-users to meet in their effort to be able to choose routers and modems during the national implementations.

IV. The BEREC Report on the Location of the Network Termination Point, October 2018

13 The BEREC Report on the Location of the Network Termination Point (the Report) is much denser and more detailed. The Report aims to foster knowledge transfer between NRAs and to give a deeper insight into the rules applicable to NRAs regarding mobile and fixed NTPs. The Report provides a view of the complex panorama in Europe regarding terminal equipment. While the BEREC Guidelines on the NTP

20 According to art. 5(3) of the Net Neutrality Regulation and art. 61.7 EECC.

21 According to art. 61.7 EECC.

22 Originally, BEREC was created with competence to override national telecommunications regulators, but the political debate over the proper balance of powers between the Commission and NRAs led to its restriction to a 'regulatory network'. It is, therefore, not a law-making body but a consultative body for the Commission. For more on BEREC's nature, see: P. Parcu / V. Silvestri, *Electronic Communications Regulation in Europe: An Overview of Past and Future Problems.* (2014) Utilities Policy 31, p. 246-255; Commission, *European Electronic Communications Code and BEREC Regulation.* (Directorate General for Communications Networks, Content and Technology 2018); Marsden (n 8), p. 119.

23 BEREC, *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules.* (BoR (16) 127, 30.08.2016).

24 BEREC, *Location of the Network Termination Point.* (n 14).

25 BEREC, *Guidelines on Common Approaches to the Identification of the Network Termination Point in Different Network Topologies.* (n 13).

26 BEREC, *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules.* (n 26), p. 8.

state how to harmonise the rules on the NTP, the Report presents a description of what has been done by the NRAs in specifying the location of the NTP or solving disputes between end-users and IAPs.

14 The Report clarifies that some NRAs (Cyprus, Germany, Italy, Latvia and the Netherlands) have specified or are about to identify the location of the NTP. In the other 22 EU countries the situation is mixed. In 13 of them, the NRA has the legal power to identify the NTP but has not done so because, according to the information provided by the NRAs, there have been no (or only minor) complaints by end-users that they cannot use their own routers or modems. The report mentions but does not clarify the situation for eight of these 13 countries, where the location of the fixed NTP has been chosen by the IAP at a point which allows end-users to use their own modems or routers (point A or B, as seen in Image 1; if the NTP is at point B, users will have to use the IAPs' modems to connect to the Internet). Besides, the location of the fixed NTP can be diverse. While in Germany and Italy routers and modems are part of the domain of the end-user, in Latvia the location of the fixed NTP depends on the ownership of equipment and cables, which means that the modem and the router could still be part of the public network.

15 Most importantly, the Report explains that the efforts to specify the location of the NTP were not a response to complaints from end-users or other market players, but were necessary to clarify the existence of an objective technological necessity for routers to be considered as part of the public network. This necessity would have been determined by factors including the interoperability of the networks, the simplicity of the equipment used, security of the equipment, and data protection. Some of the criteria employed by NRAs were used later by BEREC in the NTP Guidelines to orientate the future harmonisation on the NTP location.

V. The BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in Different Network Topologies, June 2020 (the Guidelines on the NTP)

16 As the most recent and important BEREC document regarding the free choice of terminal equipment, the NTP Guidelines are designed in accordance with Article 61(7) of the EECC to provide guidance to NRAs when they specify the location of the NTP. The NRAs should "take utmost account" of the Guidelines during the implementation in their jurisdictions. The Guidelines are intended to harmonise defining the location of the NTPs in the EU by providing the criteria NRAs should follow when specifying the location of the NTP, including conformity of the definition of the fixed NTP location with the EU legal provisions, the impact on the market for router/modems, and whether there is any technological necessity for equipment to be part of the public network.

17 Differently from its approach in the earlier documents, BEREC recognises that the immediate context of the Guidelines in the EECC is "regulation of internet access and interconnection". Competition issues, especially bottleneck conditions in access to networks, affect the methods to be used when identifying the NTP location and interpreting the EU legal provisions that refer to the NTP. Therefore, to consider terminal equipment like the modem, router and media box part of the accessed infrastructure, the NRA should prove the existence of an objective technological necessity. The assessment criteria are[27]:

- Interoperability between the public network and the terminal equipment;
- Simplicity of operation;
- Network security;
- Data protection;
- Local traffic;
- Fixed-line services based on wireless technology.

18 On the other hand, the BEREC Guidelines on the NTP fail to set very narrow and restrictive standards for setting the NTP at points B or C (see Image 1), which can deny the rights of end-users, reflecting a lax approach which prioritises IAPs' commercial interests over end-users' liberties[28]. The allowance of NRAs' discretionary power to set the NTP at three different positions can impose significant barriers to end-users effectively using their equipment. As the next part of this article will show, most NRAs in Europe have been careless with end-users' interests when they do not prioritise the enforcement of net neutrality principles.

27 BEREC, *Guidelines on Common Approaches to the Identification of the Network Termination Point in Different Network Topologies.* (n 13), p. 11-24.

28 Marsden's book cites BEREC's pro-commercial behaviour on other occasions: "*This does reflect the technocratic and commercial nature of [BEREC's] interactions with telecommunications companies, rare interactions with IT and broadcast content providers, and extremely rare interactions with civil society, user groups and consumer representatives*". Marsden (n 8), p. 120.

C. Net Neutrality and the NTP

19 The debate over net neutrality has resulted in regulatory solutions that have limited themselves to interoperability and competition. The Guidelines on the NTP, which have the "immediate context in regulation of access and interconnection", are an example of that[29]. However, the multi-faceted questions surrounding internet access, including issues of privacy and free expression, urge the consideration of end-users-orientated legal principles in the development and enforcement of net neutrality policies. Freedom of equipment choice is one of the central elements of net neutrality, dealing with last mile internet access, allowing end-users to choose and use their own trusted equipment. The promulgation of the EECC marks the revision of the EU framework for telecoms regulation, which was aimed to include long pre-existing objectives that have been the core of the telecoms framework (promoting competition, the internal market and interests of citizens). Nevertheless, the inclusion of such elements of the transposition of the EECC into an effective and enforceable framework in national jurisdictions depends heavily on NRAs' discretionary understanding of the BEREC Guidelines on the NTP, specifically what the NRAs identify as objective technological necessities. End-users' interests can be negatively impacted by the NRAs' poor record of transparency in supervising the market actors and low performance in imposing sanctions on net neutrality violations.

I. The NRA annual reporting on net neutrality and issues of net neutrality and free choice of terminal equipment

20 BEREC was given the task to define the aspects related to the position of the NTPs and to prepare guidelines to orientate the NRAs for defining the NTP in their jurisdictions. However, a fair assessment of positioning must take into consideration the real characteristics of the market, the overall technical infrastructure of the national networks and the commercial practices to which end-users are subjected. The NRAs' annual reports to the Commission on net neutrality would demonstrate the regulators' degree of readiness to engage with stakeholders in a democratic process to determine the rules regarding the hardware for internet access[30].

21 As an obligation imposed by art. 5(1) of the Net Neutrality Regulation, the NRAs should annually inform the Commission about their activities in monitoring and enforcing the net neutrality rules[31]. The reports would serve as summaries for the Commission on the state of affairs in national jurisdictions and would serve to provide a minimum level of transparency and comparability of the implementations across Europe. Among the things expected to this end from the reports are the overall description of the national situation regarding net neutrality, the description of the NRAs' monitoring activities, the number and types of complaints, IAPs' infringements related to the Regulation and results of surveys, evaluations, and technical measurements implemented by the NRAs[32].

22 Below, this research assesses the documents produced by the NRAs from the first reporting period until the last to date (2017-2020)[33] on topics concerning terminal equipment. More precisely, which kind of efforts the NRAs employed to build a structured source of information on the experience of the first years of net neutrality monitoring. The analysis searched for topics concerning terminal equipment, including:

- Information on surveys and public consultations for gathering data on the experience and opinion of stakeholders, e.g. end-users, expert circles, equipment manufacturers, IAPs, other regulators, and civil society organisations;
- Reporting about IAPs' infringements and end-users' complaints on the right to choose terminal equipment, including numbers and types of complaints, as well as the measures adopted for conflict resolution and enforcement;
- Results of research regarding IAPs' commercial practices involving terminal equipment and assessments regarding the locations of the NTP (positions A, B or C, as seen in Image 1).

29 BEREC, *Guidelines on Common Approaches to the Identification of the Network Termination Point in Different Network Topologies.* (n 13), p. 6.

30 The Austrian charity epicenter.works has produced a report about the implementation of net neutrality rules in Europe by Member States. Their work provides a complete overview of the content of the NRAs' reports during the first two years. Besides, their study has analysed the quality of the NRAs' reports in general and whether they are compliant with the basic requirements from BEREC. See: epicenter.works, *The Net Neutrality Situation in the EU.* (Vienna 2019), p. 13-16.

31 The reports are found on the European Commission Open Internet website. Commission, 'Annual country reports on open internet from national regulators' (n 6).

32 See BEREC, *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules* (n 26), p. 42-43.

33 The most recent set of reports covers the time frame from 1 May 2019 until 30 April 2020.

23 To ensure comparability, only the English-language reports were evaluated. From a total of 112 reports, only 42 had an English version. The findings are summarised in Table 1.

NRA Annual Reports on Net Neutrality
References to Free Choice of Terminal Equipment and Related Topics

Legend: Topic related to free choice of equipment? **yes/no**
Report not available in English: **n.a.**

Country	2017	2018	2019	2020	Topics related to free choice of equipment
Austria	n.a.	no	no	n.a.	
Belgium	n.a.	yes	yes	no	(2018) Free choice of terminal equipment. (2019) Tethering restriction.
Bulgaria	n.a.	n.a.	yes	n.a.	(2019) Free choice of terminal equipment.
Croatia	n.a.	n.a.	yes	n.a.	(2019) NTP specification issues.
Cyprus	n.a.	n.a.	yes	n.a.	(2019) Free choice of terminal equipment.
Czech Republic	n.a.	yes	yes	n.a.	(2018) Free choice of terminal equipment. (2019) NTP specification issues.
Denmark	n.a.	n.a.	n.a.	n.a.	
Estonia	n.a.	n.a.	no	n.a.	
France	n.a.	yes	yes	yes	(2018) Device neutrality issues. (2019) Device neutrality issues. (2020) Device neutrality issues.
Finland	n.a.	n.a.	n.a.	n.a.	
Germany	yes	yes	yes	n.a.	(2018) Free choice of terminal equipment. (2018) Device neutrality issues. (2019) Device neutrality issues. (2019) Free choice of terminal equipment.
Greece	n.a.	n.a.	n.a.	n.a.	
Hungary	n.a.	yes	yes	n.a.	(2018) Free choice of terminal equipment. (2018) Tethering restriction. (2019) NTP specification issues. (2019) Tethering restriction.
Ireland	yes	yes	yes	yes	(2017) Free choice of terminal equipment. (2018) Free choice of terminal equipment. (2019) Free choice of terminal equipment. (2020) Free choice of terminal equipment.
Iceland	n.a.	n.a.	n.a.	n.a.	
Italy	n.a.	n.a.	n.a.	n.a.	
Latvia	n.a.	n.a.	no	n.a.	
Liechtenstein	n.a.	n.a.	n.a.	n.a.	
Lithuania	n.a.	n.a.	no	n.a.	
Luxembourg	n.a.	n.a.	n.a.	n.a.	
Malta	n.a.	n.a.	no	n.a.	
Netherlands	n.a.	no	yes	no	(2019) NTP specification issues.
Norway	no	no	yes	yes	(2019) Tethering restriction. (2020) Tethering restriction.
Poland	n.a.	no	no	no	
Portugal	n.a.	n.a.	n.a.	n.a.	
Romania	n.a.	n.a.	n.a.	n.a.	
Slovakia	n.a.	n.a.	yes	n.a.	(2019) Free choice of terminal equipment.
Slovenia	n.a.	n.a.	n.a.	n.a.	
Spain	n.a.	n.a.	n.a.	n.a.	
Sweden	n.a.	no	n.a.	yes	(2020) Free choice of terminal equipment.
United Kingdom	yes	yes	yes	no	(2017) Free choice of terminal equipment. (2018) Free choice of terminal equipment. (2018) Tethering restriction. (2019) Free choice of terminal equipment. (2019) Tethering restriction.

Table 1 NRA Annual Reports on Net Neutrality – References to Free Choice of Terminal Equipment and Related Topics.

24 From 2017 to 2020, not all NRAs submitted the required reports. Although some of these reports offer valuable insights into the enforcement activities carried out by the regulator, others demonstrate complete inactivity, with almost no information regarding free choice of equipment in the year being reported on.

25 The majority of the NRAs have been silent and have provided no data on concrete issues involving violation of or compliance with art. 3(1) of the Net Neutrality Regulation. Some of the reports provided superficial information on complaints but failed to provide details on the numbers of violations, the different forms of remedy and the solutions provided. Very few reports offer concrete numbers on the disputes between end-users and IAPs regarding terminal equipment. The vast majority of the reports contain no data on commercial practices restricting use of private terminal equipment or the reasoning behind them. With the exception of a few reports, no results of surveys or technical measurements were provided, nor were any such efforts mentioned. Some reports state, however, that some IAPs consider terminal equipment to be part of their network. Almost all reports contain no information on research or surveys regarding the consequences of application of art. 3(1) to contracts and other commercial practices. In the last four years, the majority of NRAs did not provide information about the status of the NTP in their jurisdictions or the plans to determine its location in the different network topologies. In general, the reports confirm the lack of coordination among the NRAs on identifying interests of stakeholders in public debates on the NTP. Some reports have manifested the IAPs' position on terminal equipment location, but fail to express the position of other stakeholders, mainly end-users and civil society organisations.

26 These summaries show the opacity of the NRAs' reporting involving terminal equipment. The data are too sparse to justify more analysis than just these samplings.

27 On the other hand, some NRAs presented overviews of their practices relating to end-users' free choice of terminal equipment with surveys with stakeholders, market analysis or inspection of contracts. Some provided insights on the number and nature of complaints and infractions involving routers or modems and indicated the status of the NTP in their jurisdictions. Other regulators provided substantial information on the circumstances of the market, the IAPs' commercial practices, the process of specification of the location of the NTP, and the end-users' complaints related to free choice of terminal equipment. Below is a short summary of the reports which provided more detailed information regarding the status of free choice of terminal equipment[34].

Croatia

28 In the one evaluated report (2019), the regulator reported a survey regarding the choice and use of terminal equipment. The majority of IAPs consider the modem and router as part of the electronic communications network but only the modem is an integral part of the network[35]. In its turn, the Croatian regulator finds reasonable the imposition of obligatory equipment by the IAP for managing and monitoring network security (through PPPoE authentication), providing quality of bundle services (voice, internet, IPTV), and supporting equipment and service through remote access. However, it would be possible for end-users to have their own router/modem. No further information on complaints, infractions and measures adopted for conflict resolution was provided, however.

Cyprus

29 In the only report analysed (2019), the regulator states that in a formal survey IAPs have reported that they impose their terminal equipment on consumers to ensure configuration and support of the devices and of commercial purposes (bundle services - internet, voice, TV). Authentication credentials are not provided to customers but are built into the terminal equipment (PPPoE authentication). The regulator has not provided further information on complaints, infractions, and enforcement measures adopted.

Czech Republic

30 The Czech regulator, in the two analysed reports (2018 and 2019), provided an overview on the commercial practices that could lead to restrictions on end-user rights to use terminal equipment. Inspection of contractual practices found that: (i) Some IAPs enforced contracts with clauses for acquisition (usually purchase) of terminal equipment offered by the provider; (ii) Other contract terms could lead customers to a wrong conclusion about

34 Only reports submitted in English were analysed. The reports from Austria, Belgium, Estonia, Ireland, Latvia, Lithuania, Malta, Norway, the Netherlands, Poland and Sweden have brought only superficial information on free choice of terminal equipment and the definition of the NTP in their jurisdictions. Some of the reports mention complaints and other issues but fail to provide details, measures adopted and conclusions on the cases.

35 According to BEREC Guidelines on the NTP, the location would be considered point B (see Image 1).

the connection between the service and the terminal equipment; (iii) The use of private terminal equipment was often tied to the service provider's prior approval. The regulator also reported the number and status of proceedings involving terminal equipment.

France

31 In the three analysed reports (2018, 2019 and 2020), the French regulator broached several aspects of net neutrality in detail and proposed the widening of the debate on freedom of terminal equipment to embrace "device neutrality"[36]. The regulator proposes a holistic view of internet policy and the multiple factors that influence user choice and innovation, arguing how restrictions regarding end-users' devices and software (browsers, search engines and OS) could affect the free choice of access equipment.

32 Device neutrality issues fall outside the scope of the current net neutrality framework in Europe. The Regulation is directed at the behaviour of IAPs on the premise that they are uniquely situated to act as gatekeepers of internet access. However, the French regulator proposes a course of action that could be taken as methodological reference for other NRAs to approach issues regarding terminal equipment and the definition of the NTP. Although the regulator reported surveys, meetings and discussions with a wide range of stakeholders, no concrete information on limitation of end-users' rights and other practices involving terminal equipment was provided.

Germany

33 The German regulator published three reports (2017, 2018 and 2019) in English which provided superficial information on the number and type of end-users' complaints regarding terminal equipment. As in France, the NRA mentioned the increasing importance of device and data neutrality issues and made references to complaints submitted by end-users but excluded the applicability of the Net Neutrality Regulation to settle the disputes. Regarding the location of the NTP, although Germany has a law for locating the NTP on point A (see Image 1), the regulator has provided no information about plans to update the national legislation according to BEREC Guidelines on the NTP[37].

Hungary

34 In the two analysed reports (2018, 2019), the regulator disclosed the results of market research among end-users and a survey to understand the general public's opinion on net neutrality. The market research revealed that three IAPs indicated that the point of delivery of the service is understood as the ethernet port of the modem[38]. The market research also ascertained that some modems or routers contain proprietary software of the service provider, and therefore free choice of equipment can be limited.

II. Can NRAs specify the location of the NTP on a fair basis?

35 Regarding the central element for the right of choosing terminal equipment, the NTP represents the boundary between the end-user private network and the IAP's domain. Leaving the specification of the location of the NTP for the NRAs opened a broad space for their discretionary action. In the absence of case law[39] of the Court of Justice of the

36 As early as 2011 the difference between "open Internet" and "net neutrality" was discussed in Europe. While the first relates to applications that could compromise the open character of the web, the second is about commercial treatment of consumers by network operators. Device and data neutrality are the natural extension and merger of both debates about user freedom in the several layers of the Internet. Data and device neutrality can encompass topics such as, for instance, that search engines could rank search results giving preference to their own or affiliated services. Non-neutral practices can also be involved with operating systems imposed on consumers depending on hardware. Web browsers, including their associated plug-ins, could interfere in the neutrality of how content is displayed. For a broader discussion, see: J. van Hoboken, 'Search Engines, Pluralism and Diversity: What Is at Stake and How to Move Policy Forward?' Media Pluralism and Diversity: Concepts, Risks and Global Trends (Macmillan 2015); J. Krämer, D. Schnurr et al, Internet Platforms and Non-Discrimination (CERRE 2017); R. Easley, H. Guo et al, Research Commentary - From Net Neutrality to Data Neutrality: A Techno-Economic Framework and Research Agenda. (2018) Information Systems Research; BEREC, Report on the impact of premium content on ECS markets and the effect of devices on the open use of the Internet (BoR (18) 35 08.03.2018); A. Kak / J. Ben-Avie, 'ARCEP report: "Device neutrality" and the open internet' (Mozilla Corporation 29.05.2018). <https://blog.mozilla.org/netpolicy/2018/05/29/arcep-report-device-neutrality/> accessed 28.11.2020; J. Krämer, Device Neutrality: The missing link for fair and transparent online competition? (CERRE 2019).

37 The draft of the implementation law for the EECC in Germany recognizes exceptions for point A according to the BEREC Guidelines on the NTP. See footnote 45.

38 According to BEREC Guidelines on the NTP the location would be considered point B (see Image 1).

39 Worth noting is that in September 2020 the CJEU handed down the first decision on net neutrality in Europe. The

European Union on an enforceable rule on the freedom of terminal equipment, the NTP Guidelines is the authoritative document on router freedom in Europe. The enforcement can be harmonised to the extent that the Guidelines offer clear rules, but there are topics open for further interpretation (e.g., technological necessity issues), leading to uncertainties.

36 The EECC entered into force on 11 December 2018 and the transposition into national law by each of the member states has a deadline of 21 December 2020. By then all NRAs should have specified the location of the NTP in their jurisdictions according to the three possible locations identified by BEREC (points A, B or C, as seen in Image 1). The EECC marks not the end of the discussion of the right to choose terminal equipment, but the start of a new chapter in the history of this right in national jurisdictions. Specifying the location of the NTP is important not only in relation to the free choice of terminal equipment, but also in relation to traffic management, transparency, enforcement and monitoring mechanisms. Diverging interpretations of the location of the NTP create uncertainties as to the rights of end-users. There are 23 EU countries in which the location of the NTP has not been specified, in which the respective NRAs have not decided to use this legal power for lack of complaints of end-users. The end-users' interests, therefore, can be negatively impacted by the passive approach of the NRAs.

37 As the results in Section I above have shown, IAPs have an interest in considering routers and modems to be part of their networks in order to monitor network security and to guarantee quality of service[40]. All major consumer IAPs are vertically integrated to some extent with digital video, voice and web services. Incorporating the router and modem into their infrastructure allows them to discriminate against private equipment with negative consequences for end-users. The NRAs have been flexible in their enforcement of art. 3(1), allowing IAPs to consider at least the modem to be their equipment, as the annual reports demonstrate. Therefore, NRAs could interpret the technological necessity criteria of the NTP Guidelines to be aligned with commercial interests of IAPs. This might be done in specifying the management of the network, granting a dominant position to bundle services (voice, IPTV) and commercial practices, such as price levels and providing extra support for the equipment.

38 Net neutrality from the perspective of internet access hardware does not lack regulatory tools on the European level per se. However, the potentially complex implementation by the NRAs endangers end-users' interests. The end-users face the IAPs' unreasonable discrimination in commercial practices involving terminal equipment. No matter how clearly art. 3(1) of the Net Neutrality Regulation asserts the neutrality of devices, in practice national regulators can completely prevent the possibility of end-users having their own devices.

39 In countries where laws relating to end-users' choice of terminal equipment have been passed[41], the specifications of the location of the NTP can vary from those already implemented – definitions that have served as bases for end-users' rights. In Germany, for instance, the current NTP is located at point A (see Image 1) and customers can demand from their IAP that they be permitted to use their own equipment – backed up by national courts[42]. However, with the new elements provided by the BEREC Guidelines, the German NRA has new opportunities to consider the relocation of the NTP, which might lead to the restriction of end-users' rights[43]. Customers can only be formally secure in

court ruled that zero-rating practices are incompatible with art. 3(2) and (3) of the Net Neutrality Regulation. See: CJEU, Joined Cases C-807/18 and C-39/19 *Telenor v Nemzeti* (2020) ECLI:EU:C:2020:708.

40 As shown by results of surveys conducted by some NRAs and related in their annual reports. The report evaluation from the Commission reached similar conclusions. See: Commission, *Study on the Implementation of the Open Internet Provisions of the Telecoms Single Market Regulation.* (n 9), p. 52.

41 Germany is an example with the "Gesetz zur Auswahl und zum Anschluss von Telekommunikationsendgeräten" of 01.08.2016. For an analysis of the act, see: T. Sörup, *Routerzwang adé? – Der Referentenentwurf zur Endgerätewahlfreiheit.* (2015) 31 Computer und Recht 217, p. 217–222.

42 See, for example, in Germany: G. Kiparski / S. Wettig, *Nicht Ohne Meinen Router?! – Routerfreiheit Im Spannungsverhältnis Der Anschlussbündelangebote.* (2020) Computer und Recht, p. 265–268. However, the court ruled that free choice of equipment depends upon customer requests and IAPs are not required to actively inform end-users of the possibility of using a third-party device. See: OLG Koblenz: *Routerfreiheit* (2020) OLG Koblenz 9 U 1407/19.

43 The draft of the law for implementation of the EECC (TKG-E) allows in its Paragraph 70(2) the introduction of exclusions on free choice of terminal equipment based on BEREC Guidelines on the NTP after years of accumulated good experience of the NTP at point A (see Image 1). See: Bundesministeriums für Wirtschaft und Energie, Bundesministeriums für Verkehr und digitale Infrastruktur, *Entwurf eines Gesetzes zur Umsetzung der Richtlinie(EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts* (2020)

the ability to be able to choose their router freely. In practice, IAPs' commercial strategies can hinder the formally free choice even when the IAPs are acting legally. IAPs may fail to inform end-users about the right to choose other devices and may engage in legal but manipulative advertising practices[44].

40 Powerful methods of inferior decision-making lead to solutions detrimental to end-users' rights, impairing not only internet access but also their privacy, security, and data protection[45]. Assuring freedom of choice, therefore, requires end-user focused policies in the NRAs' decision-making processes. Decisions concerning the NTP, for instance, impact directly upon what is increasingly declared a human right: access to the Internet. Following the good example of the French regulator, ARCEP, the NRAs' decision-making should take into consideration a balance among the interests of stakeholders, but an emphasis should be given to the needs of the end-users. Therefore, the implementation of the EECC in national jurisdictions should involve proposals to accommodate the interests of operators and other market players, but at the same time maintain the ability of end-users to freely choose their equipment. For this purpose, the NRAs should at least:

- Employ data-driven mechanisms for decision-making, including impact assessments, surveys, public opinion polls, market research, contract inspection measures and self-evaluation reports. The collected data and the overall outcome should be made openly accessible in formats that allow review and comparability;

- Develop an accessible information base for the reporting on the number, type and nature of end-users' complaints and IAPs' violations regarding terminal equipment. Conduct legal research on national case law involving terminal equipment cases and make the results available. Monitor IAPs' contractual restrictions imposed on end-users and publicly take action;

- Take into consideration competition policies to safeguard market liquidity but remain vigilant about consumer law and human rights law, especially when abiding by the criteria proposed by the BEREC Guidelines on the NTP.

41 Employing such a methodology, the NRAs could improve their communication to stakeholders on the subjects impacting their rights, increasing the quality of the public debate. The current lack of transparency inhibits a fair and well-balanced judgement of the state of interests in their jurisdictions. Better understanding of the free choice of terminal equipment in the context of net neutrality in Europe depends on the European Commission exercising closer supervision over the NRAs' monitoring and enforcement by taking swift action against their ineffective reporting on their activities and by imposing higher standards on the annual reports, since the reports represent an important information channel for end-users as well.

D. Conclusion and future work

42 Free choice of terminal equipment is a fundamental principle of net neutrality. It enables end-users to remain autonomous in their physical capacity to access the Internet, employing devices they trust for security, privacy and data protection. Although art. 3(1) of the Net Neutrality Regulation clearly sets forth the principle of device freedom, the EECC requires further specification of the location of the NTP. Notwithstanding the efforts BEREC has made to harmonise the concept of device freedom on the European level, the national implementations are challenged by the untransparent behaviour of the NRAs. A fair assessment of the criteria to identify the location of the NTP and of the further monitoring requires clear and data-driven approaches by the NRAs and a higher commitment by the European Commission to the supervision of compliance with the Net Neutrality Regulation's rules.

43 The conclusions of this paper have limitations which may prompt future research. First, further review on the different approaches during the implementation processes of the EECC depends on verifiable data on how the NRAs will approach the BEREC Guidelines on the NTP and which elements will be taken into consideration to determine objective technological necessity in their national jurisdictions. Second, this research has not developed any argument in relation to device neutrality concepts. Since some NRAs comprehend the topic as related to terminal equipment, the scope and limits of the debate on data neutrality and terminal equipment need further clarification.

<https://www.bmvi.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/referentenentwurf-zum-telekommunikationsmodernisierungsgesetz.pdf?__blob=publicationFile> accessed 28.11.2020.

44 See e.g.: M. Mehl / L. Lasota, 'Fear, Uncertainty, and Doubt - the Barriers to Router Freedom in Germany' (*Free Software Foundation Europe*, 03.02.2020) <https://fsfe.org/news/2020/news-20200302-01.en.html> accessed 29.08.2020.

45 As also noticed by Marsden: "*End-users are sometimes poorly motivated economic actors and imperfectly rational" [...] "Without comprehending that users view Internet access as a more utilitarian and therefore profound service than that of social networks or Internet search, it is impossible to understand the net neutrality debate*". Marsden (n 8), p. 75.

Direct Copyright Liability As Regulation Of Hosting Platforms For The Copyright-Infringing Content Uploaded By Their Users: *Quo Vadis*?

by **Bianca Hanuz***

Abstract: The potential direct liability of hosting platforms such as YouTube and Dailymotion, which provide the technical conditions for their users to upload and share copyright-protected content, for the infringement of the right of communication to the public (CTTP) in Article 3(1) Directive 2001/29/EC (and pre-Directive 790/2019) represents one of the most complex and controversial aspects of current European Union (EU) copyright law. The test in Article 3(1) is opaque and may even support opposing conclusions on the matter. Doctrinally, the appropriateness of Article 3(1) to regulate hosting platforms is shaky as it is unclear how the regulation of platforms via Article 3(1) may reflect the balance of interests of rightsholders, of platforms, and internet users. Hosting platforms facilitate both the legal and illegal sharing of copyright content indiscriminately and in an automated fashion. When legal content is shared through their service, hosting platforms play an important role in facilitating the exercise of user's freedom to send and receive information safeguarded by Article 11 of the EU Charter of Fundamental Rights. The potential application of direct copyright liability to hosting platforms, including the spectre of damages, may chill technical innovation in the area. Some platforms may even close and the opportunities for internet users to share legal content reduces as a result. To address these issues, this article analyses the three alternatives for limiting the responsibility of hosting platforms under Article 3(1). The article first analyses the complex test for CTTP under Article 3(1). To balance the application of liability, Alternative 1 explores the option of integrating a 'duty of care' element conditioned by a standard of proportionality within the test for CTTP. Alternative 2 challenges the notion that direct responsibility may be attributed to operators of hosting platforms. It analyses, but ultimately dismisses, the situation where host providers may be considered as mere providers of facilities for enabling communication. Alternative 3 advances a novel application of the test under Article 3(1) which shows that operators of certain hosting platforms do not engage in acts of "communication" of the illegal copyright material uploaded by their users. The purpose of the paper is to bring attention to particular possible constructions of hosting platform liability and their broader implications.

Keywords: copyright infringement; host; internet; communication to the public; fundamental rights

Recommended citation: Bianca Hanuz, Direct copyright liability as regulation of hosting platforms for the copyright-infringing content uploaded by their users: Quo vadis, 11 (2020) JIPITEC 315 para 1.

A. Introduction

1 The sharing of content on the internet is ubiquitous. Hosting platforms such as YouTube, Dailymotion and VMEO enable their users to store and share all kinds of videos, from a recording of a lecture to a video spoiler from a Hollywood film. The spectre of copyright infringement often appears. For example, a YouTube user's uploads that consists of game-plays of the video game Fortnite were removed from the platform because of copyright infringement and the user was subjected to an injunction.[1] The rights of reproduction in Article 2 and communication to the public (CTTP) in Article 3 of Directive 2001/29/EC[2] (InfoSoc) are preventative so that any use of copyright works by third parties requires the rightsholder's authorisation.[3] A user's act of uploading content that includes copyrighted works to a platform's server may breach the reproduction right in Article 2. In addition, the release – that is the sharing of that content to the online audience – may constitute the making available aspect of the CTTP right in Article 3(1). Infringement occurs if the rightsholder's consent is not obtained in advance and none of the exceptions and limitations in the list in Article 5 InfoSoc apply. While the *prima facie* copyright liability of internet users is often easy to establish, enforcement is more problematic. On the internet, individuals' identities can easily be cloaked in anonymity. It is difficult and economically unrewarding for rightsholders to identify and pursue copyright-infringing internet users. It also makes for poor business practice to alienate infringing internet users as infringers are also consumers of copyright-protected content.[4]

2 A more rewarding approach may be to address internet users' infringement via the hosting platforms that store uploaded content and facilitate the sharing of content, including that which may infringe copyright. There are several typologies of hosting platforms. One provides video sharing services, such as YouTube or Dailymotion. They store and index uploaded content, provide search facilities, categorise uploaded content and supply automatic preference-based recommendations to users. A related type includes social media sites such as Facebook and Instagram that enable the storage and sharing of pictures and short videos. Both types generate advertising revenue from the uploaded content.

3 Another type of hosting platform is represented by cyberlockers, also known as file hosting services. Examples are RapidShare or FilesAnywhere which offer free storage and file-sharing services for all types of data. Unlike video sharing services, content uploaded on cyberlockers is not categorised and a search function is not provided. Instead, for each file uploaded a download link is made and sent to the uploading user. The link can be shared on other websites such as blogs, forums or "link collector" websites. Download speeds are limited for those with free accounts and unlimited for paid subscriptions. Some cyberlockers offer an incentive for users to upload desirable content.[5]

4 The operators of these hosting platforms do not check the content that is uploaded by users and lack any specific knowledge of copyright-infringing content and specify in their terms and conditions that no infringing content should be uploaded. Video sharing and social media platforms also filter their networks and remove copyright-infringing content.

5 Article 3(1) InfoSoc sets out a general exclusive right of CTTP for authors to "authorise or prohibit any CTTP of their works". The *travaux préparatoires* of the InfoSoc Directive identifies two objectives of the right: to permit new exploitations of works; and to ensure that rightsholders are satisfactorily protected.[6] Using this right, the Court of Justice of the European Union has regulated situations where developments in technologies or new uses of existing technologies have led to the exploitation of works in a manner unforeseen by the rightsholders.

* Dr., University of Liverpool.

1 Ernesto Van Der Sar, "YouTuber 'Golden Modz' Settles Lawsuit Over Fortnite Cheats" (TorrentFreak, 19 March 2019) <https://torrentfreak.com/youtuber-golden-modz-settles-lawsuit-over-fortnite-cheats-190319/> accessed 25 April 2020.

2 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive) [2001] OJ L167/10.

3 *Soulier v Ministre de la Culture et de la Communication* (C-301/15) EU:C:2016:536 [2016] 7 WLUK 126 at [33].

4 J.P. Quintais and J. Poort, "The Decline of Online Piracy: How Markets – Not Enforcement – Drive Down Copyright Infringement" (2019) 34 American University International Law Review 807, 820.

5 Opinion of Advocate General Saugmandsgaard Øe in *Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH and C-683/18 Elsevier Inc. v Cyando Ag (YouTube/Cyando)* (*YouTube/Cyando*) (Joined C-682/18 and C-683/18) EU:C:2020:586 at [31].

6 Commission, "Green Paper on Copyright and Related Rights in the Information Society," COM (1995) 382 final, 65.

Whether hosting platforms perform copyright exploitation under Article 3(1) is a matter currently pending in front of the CJEU in the joined *YouTube/Cyando* referrals.[7]

6 Hosting platforms perform socially desiable functions, for example they may foster the excercise of freedom of expression and information. Both the CJEU and the European Court of Human Rights (ECtHR) have recognised the importance of the internet for freedom of expression and information, safeguarded by Article 10 of the Charter of Fundamental Rights and Article 11 of the European Convention on Human Rights (ECHR).[8] The ECtHR found that YouTube is a platform that enables information of specific interest to be broadcast – particularly on political and social matters – and citizen journalism to emerge.[9] The ECtHR, in a case involving the temporary shutdown of a website following accusations of a criminal copyright breach, observed that Article 10 ECHR guarantees freedom of expression to "everyone" and applies "not only to the content of information but also to the means of dissemination since any restriction imposed on the latter necessarily interferes with the right to receive and impart information".[10]

7 The application of a strict liability standard for hosting platforms under Article 3(1) InfoSoc would increase copyright protection and could generate massive financial liability. This may have a chilling effect on technological innovation in the area and foster monopolies.[11] The problem is that the rules triggered in response to hosting large platforms such as YouTube would apply to all types of hosting platforms irrespective of size or financial position, or the level of innovation involved in the provision of their service. When only the big players are in the position to pay damages or to enter into licenses for the uploaded illegal content, smaller platform providers in weaker positions may close down. The problem is further compounded by the potential unavailability of a licence that platforms can pay for and that covers all the infringing content uploaded by users.[12] A reduction in the number of such platforms may in turn reduce the avenues of internet users to engage in legal exchanges of information and engage in public debate on matters of general interest.

8 This article shows that potential direct liability of those hosting platforms that provide the automatic technical setup for their users to upload and share content – including copyright-infringing content – while only having general knowledge that infringing content may be uploaded, may be curbed under Article 3(1) InfoSoc. This article first untangles the complex web of elements that form the test for CTTP under Article 3(1). Against this background, Sections C to E discuss the various interpretations of the CTTP right to curb the potential liability of certain host providers.

9 Section C offers a new perspective on the proposal that the regulation of hosting providers may be achieved via the application of a duty under Article 3(1) InfoSoc for platforms to remove copyright-infringing content on their network. This is set out as Alternative 1. Although various options exist to impose such a duty, such an imposition may create incentives for the overenthusiastic removal of content, hence safeguards to this are paramount.

10 Section D analyses the proposition of AG Saugmandsgaard Øe in the *YouTube/Cyando* referral which sees hosting platforms such as YouTube and Cyando excluded from the scope of the CTTP right as they may engage in an activity covered by Recital 27 InfoSoc, which states that "the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication".[13] The section, set out as Alternative 2 in this article, concludes that the scope of Recital 27 may not be wide enough to accommodate the activities of hosting intermediaries. Instead, Section E advances Alternative 3 which is a novel application of the CTTP test which shows that certain hosting platforms may not be seen to perform an act of "communication" as certain hosts do not perform "an intervention in full knowledge of the consequences".

11 This article only analyses the situation of potential copyright infringement by hosting platforms under Article 3(1) and pre-Directive 790/2019 (DSMD).[14]

7 *YouTube/Cyando* EU:C:2020:586.

8 *GS Media BV v Sanoma Media Netherlands BV* (*GS Media*) (C-160/15) EU:C:2016:644 [2017] C.E.C. 442 at [45]; *Times Newspapers Ltd v. the United Kingdom* (nos. 1 and 2), nos. 3002/03; and 23676/03 (ECHR 2009) at [27] and *Ahmet Yıldırım v. Turkey*, no. 3111/10 (ECHR 2012) at [48].

9 *Cengiz v Turkey* App. No 48226/10; 14027/11 (ECHR 2015).

10 *Case of Pendov v. Bulgaria* App. No. 44229/11(ECHR 2020) at [53].

11 For the US perspective on peer-2-peer technology see *MGM Studios, Inc. v. Grokster, Ltd*., 545 U.S. 913 (2005) at [960].

12 M. Leistner, "Copyright law on the internet in need of reform: hyperlinks, online platforms and aggregators" (2017) 12(2) Journal of Intellectual Property Law & Practice 136, 144.

13 Opinion of Advocate General Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [86]-[89].

14 Directive (EU) 2019/790 of the European Parliament and of

Certain host providers such as YouTube and Dailymotion may be covered by the concept of online content-sharing service providers (OCSSP) in Article 17 DSMD which states that OCSSPs are liable for CTTP unless they conclude licences or comply with prescribed measures.[15] This article is limited to the CTTP right in Article 3(1) InfoSoc, as the legality of the regime under Article 17 DSMD is pending before the CJEU.[16] Should Article 17 be struck out, the CTTP right in Article 3(1) alone would remain relevant to host providers. The relationship between the CTTP right in Article 17 DSMS and the CTTP right in Article 3(1) InfoSoc is also not yet fully clarified and is an entirely different topic already covered by other authors.[17]

B. The controversial contours of the legal test under Article 3(1) InfoSoc

12 Article 3(1) InfoSoc implements Article 8 of the WIPO Copyright Treaty.[18] It introduces a general exclusive right which enables authors to authorise or prohibit:

> *...any CTTP of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.*

13 Although the wording "any" indicates the broad scope of the right, the text of the Article does not specify what activities fall within the remit of the right. Only limited clarification is available in Recitals 23 and 27. Recital 23 excludes communications to those present at the place where the communication originates – such as public representation and performance – and communications that involve only physical proximity, where the transmission of the work is missing.[19] Recital 27 limits the scope of the right by excluding the mere provision of physical facilities for enabling or making a communication.[20]

14 The Article 3(1) definition was expected to "stand the test of changing technology".[21] The architects of the Directive foresaw that the communication right, including "making available", and the other rights, would take on other "characteristics" and that it would be necessary to "adjust" them as a result.[22] The CJEU has been instrumental in carving the offline and online dimensions of the CTTP right. The methodology of the CJEU in applying Article 3(1) InfoSoc is key to the application of the right. To determine the existence of an act under Article 3(1) under a specific set of facts, the CJEU follows an individual assessment.[23] The same methodology applies to identify the user under that provision.[24] Following the individual assessment, two cumulative elements must be met: an "act of communication" which is directed to "a public".[25] The analysis is supplemented by other criteria which include: "the indispensable role" of the user; the "deliberate" nature of their "intervention"; "in full knowledge of the consequences of [their] actions"; "the new public"; and the "for-profit" nature of the communication.[26]

---

the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

15 DSMD Article 17(1) Article and Article (4)(b)and (c) DSMD.

16 *Republic of Poland v European Parliament and Council of the European Union* (C 410/19).

17 M.Husovec and J.P. Quintais, "How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms" (September 2014) < https://ssrn.com/abstract=3463011> accessed 30 September 2020.

18 Adopted 20 December 1996 (entered into force 6 March 2002) 2186 UNTS 121.

19 *Football Association Premier League Ltd v QC Leisure* (C-403/08) EU:C:2011:631 [2011] ECDR 11 at [201]-[203].

20 It is unclear who would qualify as a purely technical intermediary. For an explanation, see M. van Eechoud, P. B. Hugenholtz, S. van Gompel, L. Guibault, N. Helberger, *Harmonising European Copyright Law: The Challenges of Better Lawmaking* (Kluwer Law International 2009) 125.

21 Opinion of the Economic and Social Committee on the "Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the information society" OJ C 407 (28.12.1998) at [3.5]

22 See Commission, "Green Paper on Copyright and Related Rights in the Information Society" 17, COM (1995) 382 final at [17].

23 *Reha Training v GEMA* (C-117/15) ECLI:EU:C:2016:379 [2016] 3 CMLR 40 at [35] and [44]; *Phonographic Performance (Ireland) Ltd v Ireland and Others* (C-162/10) EU:C:2012:141 [2012] Bus LR D113 at [30].

24 *SCF* EU:C:2012:140 [2012] ECDR 16 at [76] and [78]; *Phonographic Performance* EU:C:2012:141 [2012] 2 CM.LR. 29 at [28].

25 *ITV Studios Ltd* EU:C:2013:147 [2013] Bus LR 1020 at [21] and [31]; *Nils Svensson* EU:C:2014:76 [2014] WLR(D) 67 at [16]; when one criterion is not met there is no CTTP *Reha Training* ECLI:EU:C:2016:379 [2016] 3 CMLR 40 at [45].

26 Ibid at [64].

These criteria are complementary, interdependent, are not autonomous, are present in "widely varying degrees", and are applied both individually and in combination with each other.[27] The test was applied to various technical scenarios such as the transmission or retransmission of signals[28] and broadcasts;[29] the transmission of broadcasts by direct injection;[30] the online retransmission of broadcasts;[31] the hyperlinking to legal[32] or illegal content;[33] the embedding of legal content; the provision of cloud time-shifting service;[34] the sale of a media player that gives access to illegal copies;[35] the management of an online platform that indexes peer-2-peer torrents;[36] and the reposting of a work already online with consent freely and for free.[37]

I. The CTTP elements applicable to facilitators of access to illegal copyright content which may be relevant to hosting platforms

15 One way to organise the extensive CJEU case law on CTTP is to split between cases where the original communication or making-available of works is made with the rightsholder's consent and cases where the original communication is made without. The latter category includes the case law on facilitation of access to illegal copies of works in *GS Media*,[38] *Filmspeler*[39] and *TPB.*[40] In *GS Media*, the CJEU found that hyperlinking to protected works freely available on a third-party website where they had been published without consent can fall within the scope of Article 3(1). Liability occurs when such a link-provider knew or should have known of the unauthorised nature of the linked content, or when the link is provided for financial gain, the knowledge of the unauthorised nature of the linked content is presumed and the link-provider does not rebut the presumption by conducting the "necessary checks".[41] In *Filmspeler*, the sale of a media device customised with links that give access to content published without rightsholder consent fell within the scope of Article 3(1).[42] In *The Pirate Bay* (TPB), the CJEU found that the management and operation of the TPB platform used by users to store and share torrent files necessary for P2P file sharing is an act of CTTP within the meaning of Article 3(1).[43]

16 Hosting providers generally do not upload and share the copyright-infringing material on their servers, but they still increase the risk of copyright infringement because they provide the technical structures for their users to upload and share all types of content.[44] Thus potentially court the realm of application of the CTTP case law on facilitation of access to illegal copies of works under Article 3(1).

27 Ibid at [35]; *SBS Belgium* EU:C:2015:764 [2016] ECDR 3 at [15] and case law cited there; *Phonographic* EU:C:2012:141 [2012] 2 CM.LR. 29 at [30].

28 *Sociedad General de Autores y Editores de Espana (SGAE) v Rafael Hoteles SL (SGAE)* (C-306/05) EU:C:2006:764 [2007] Bus LR 52; *Ochranný svaz autorský pro práva k dílům hudebním, os (OSA) v Léčebné lázně Mariánské Lázně* as (C-351/12) EU:C:2014:110 [2014] [2014] 2 WLUK 931.

29 *FAPL* EU:C:2011:631 [2011] ECDR 11; *SCF* EU:C:2012:140 [2012] ECDR 16; *Reha Training* EU:C:2016:379 [2016] 3 CMLR 40; *Autoren, Komponisten und Musikverlegerregistrierte Genossenschaft mbH (AKM) v Zürs.net Betriebs GmbH* (C-138/16) EU:C:2017:218 [2017] MR 75.

30 *SBS Belgium* EU:C:2015:764 [2015] WLR(D) 466.

31 *ITV Studios Ltd* EU:C:2013:147 [2013] Bus LR 1020.

32 *Nils Svensson* EU:C:2014:76 [2014] WLR(D) 67; *GS Media BV* (C-160/15) EU:C:2016:644 [2017] C.E.C. 442.

33 *BestWater International GmbH v Mebes* (C-348/13) EU:C:2014:2315; [2014] 10 WLUK 615.

34 *VCAST Ltd v RTI SpA* (C-265/16) EU:C:2017:913 [2017] 11 WLUK 694; [2018] 2 CMLR 12.

35 *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816.

36 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237.

37 *Land Nordrhein-Westfalen v Renckhoff* EU:C:2018:634 [2018] Bus LR 1815; [2018] 8 WLUK 56.

38 *GS Media* EU:C:2016:644 [2017] C.E.C. 442.

39 *Stichting Brein v Jack Frederik Wullems (Filmspeler)* EU:C:2017:300 [2017] Bus LR 1816.

40 *Stichting Brein v Ziggo BV, XS4ALL Internet BV (Ziggo)* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237.

41 *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [49] and [51].

42 *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816.

43 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237.

44 As hosting providers do not originate the stored copyright infringing content, they should not be placed under strict liability

II. The expansion of the "act of making available" to activities that facilitate access to works

17 An act of communication online requires two aspects: an objective act of making available protected works by "any technical means of communication";[45] and the "indispensable" "intervention" "in full knowledge of the consequences of its action" [46] to give access to the works to other users who would otherwise not be able to enjoy the works, or for whom accessing them would be more complex. By way of example, an act of making available covers on-demand communications such as connection to a server from which works may be accessed individually by members of the public at their will.[47] The making available right is also triggered by the possibility of access: it is "sufficient to make works available (for example, by transferring a work to an electronic bulletin board)".[48] The notion of making available in Article 3(1) is expressed in technically neutral terms.[49] The focus on technical neutrality is described by Advocate General (AG) Trstenjak in *SCF* as "the functional approach" which "emphasises the aim of adequate protection of authors, irrespective of the technical details"[50] and which may lead to the enlargement of the right. Yet, the disregard of technical details appears to be only rhetoric. For example, if the technical nature of the underlying acts that make copyright-protected works available are irrelevant, then it is unclear why it is necessary to check whether an act amounts to the "mere provision of physical facilities" and is therefore excluded from the meaning of a relevant "communication".[51]

18 At the heart of the CJEU's jurisprudence on "making available" is the finding that the provision of access to works amounts to an act of "communication", which is introduced in *Svensson*, a case on hyperlinking to material made available online freely and for free and with the rightsholder's consent.[52] In *Svensson,* the CJEU relies on the access theory to justify the existence of an objective act of making available. The "access theory" defines an act of making available as the provision of direct access to protected works.[53] This proposition is arguable, since hyperlinks only facilitate access to works stored somewhere else, direct access is provided by the person who initially makes the work available online.[54] The access theory is however perpetuated in the *GS Media* and *Filmspeler* decisions.[55] In *Filmspeler*, the provision of access was technically complex. The device:

> *...enable[d], in view of the add-ons pre-installed on it, access via structured menus to links that those add-ons which, when activated by the remote control of that multimedia player, offer its users direct access to protected works without the consent of the copyright holders.*[56]

19 The *Filmspeler* decision clarifies that direct access describes the users' experience in accessing the works. In other words, the indirect provision of

45 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899 at [34].

46 *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [35]; *Ziggo*EU:C:2017:456 [2017] Bus LR 1899 at [36].

47 Jörg Reinbothe and Silke von Lewinski, *The WIPO Treaties on Copyright: A Commentary on the WCT, the WPPT, and the BTAP* (Oxford University Press 2015) point 7.8.26.

48 WIPO, "Report of the Seventh Session of the Committee of Experts on a Possible Protocol to the Berne Convention" (Geneva, 22-24 May 1996) WIPO Doc BCP/CE/VII/4-INR/CE/VI/4, 4.<www.wipo.int/mdocsarchives/BCP_CE_VII_INR_CE_VI/BCP_CE_VII_4_INR_CE_VI_4_S.pdf> accessed 23 January 2016; see also *Nils Svensson et al v Retriever Sverige AB* (C-422/12) EU:C:2014:76 [2014] WLR(D) 67 at [19]; *Stichting Brein v Wullems (t/a Filmspeler)* (C-527/15) EU:C:2017:300 [2017] Bus LR 1816 at [20] and the case-law cited; *Land Nordrhein-Westfalen v Renckhoff* (C-161/17) EU:C:2018:634 [2018] Bus LR 1815 at [29].

49 WIPO, "Diplomatic Conference on Certain Copyright and Neighbouring Rights Questions, Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference" (10 December 1996) WIPO CRNR/DC/4 at [10.14]; Mihaly Ficsor, "The Spring 1997 Horace S. Manges Lecture—Copyright for the Digital Era: The WIPO "Internet" Treaties" (1997) 21 Colum JL & Arts 197, 210.

50 See Advocate General Trstenjak in *Societa Consortile Fonografici (SCF) v Del Corso* (C-135/10) EU:C:2012:140 [2012] ECDR 16 at [102]. The functional approach is contrasted by AG Trstenjak with the "technical approach" which considers technical details.

51 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899 at [38].

52 *Nils Svensson* EU:C:2014:76 [2014] WLR(D) 67 at [20].

53 Ibid at [18].

54 S. Dusollier, "Les Hyperliens en Droit d"Auteur Européen: Quand tout Deviant Communication" (2014) 54 *Revue du Droit des Technologies de l"Information* 49, 57.

55 *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [35]; *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816 at [48].

56 *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816 at [48], see also Arnold J in *Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd* [2013] EWHC 3479 (Ch) at [34].

access from a technical perspective can qualify as "direct access" when access to works is perceived directly by users on their screens.

20 In the *TPB* decision, the CJEU removes the "direct access" requirement in the situation of an online platform that enables internet users to locate torrent files in a Peer-2-Peer network and the platform is specifically designed for copyright infringement. The CJEU changed the focus from the objective act of communication and placed the onus on the mental state of the entity which performs a CTTP. *TPB* re-interprets *Svensson, GS Media,* and *Filmspeler* to introduce the rule that:

> *...any act which provides access to works by a user acting with full knowledge of the relevant facts, is liable to constitute an 'act of communication" for the purposes of Article 3(1) of Directive 2001/29.*[57]

21 In the case of hosting platforms, it is indubitable that access is given to the content uploaded by the platform's users. Following *TPB*, the relevant question is who is legally responsible for the provision of access to works hosted on the platforms: the platform operators or the uploading users, or both?

III. The "indispensable intervention of the user who acts in full knowledge of the consequences"

22 In the case law on facilitation of access to illegal copies of works, the CJEU emphasises "the indispensable role played by the user and the deliberate nature of his intervention".[58] This criterion was first introduced in the *SGAE* decision in 2006 and the subsequent case law application suggests that it serves as a causation test to identify who is a "user" responsible for the act of CTTP under the CTTP test.[59] In cases of the facilitation of access to illegal copies of works, causation is "central" to the assessment.[60] The intervention aspect establishes the factual cause, observable due to the use of contra-factual inference "in the absence of [which], those customers would not be able to enjoy the broadcast work, or would be able to do so only with difficulty".[61] An intervention needs to be "indispensable" or "essential"; terms bearing different levels of intensity, which are sometimes used interchangeably and are assessed within the confines of the factual context of the case.[62] In particular, an act can be essential to the provision of access to a work even when there are other technical means online to access it.[63]

23 The indispensable intervention by the user is "deliberate" and performed "in full knowledge of the consequences of his action, to give his customers access to a protected work". This may mean that the user intended to cause the consequences, and the user is not acting in error or from a lack of understanding.[64] This *means rea* serves to establish who is legally responsible for the provision of access to copyright-infringing works and may sometimes overlap with 'knowledge' in the context of the 'new public' element discussed below.[65]

24 In cases of facilitation of access to illegal copies of works, the standard of intention is obscured. Although Mr. Wullems in *Filmspeler* and the operators in *TPB* intervene with intention to give access to illegal copies of works, the language of the decisions point to various standards of knowledge. The *Filmspeler* decision appears to refer to Mr Wullems's knowledge that he installs "add-ons that specifically enable purchasers to have access to protected works published — without the consent of the copyright holders of those works", without having the knowledge of specific copies of works being made

57 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; at [34].

58 *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816 at [31]; *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; at [26].

59 *SGAE* EU:C:2006:764 [2007] Bus LR 52 at [42]; see also the user mentioned in *SCF* EU:C:2012:140 [2012] ECDR 16 at [75].

60 *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [35]; *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816; [2017] 4 WLUK 447 at [31]; *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237 at [26].

61 *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816; [2017] 4 WLUK 447 at [41]; *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237 at [26].

62 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237 at [26] and [37].

63 J. C. Ginsburg, "The Court of Justice of the European Union Creates an EU Law of Liability for Facilitation of Copyright Infringement: Observations on *Brein v. Filmspeler* [C-527/15] (2017) and *Brein v. Ziggo* [C-610/15] (2017)" Columbia Law and Economics Working Paper No. 572, Columbia Public Law & Legal Theory Paper #557, 4-5.

64 See for example "[i]f an act is done deliberately and with knowledge of the consequences, I do not think that the actor can say that he did not "intend" the consequences or that the act was not "aimed" at the person who, it is known, will suffer them". *Bourgoin SA v Minister of Agriculture* [1986] 1 QB 716, 777. FAPL EU:C:2011:631 [2011] ECDR 11 at [196]; *Reha Training* ECLI:EU:C:2016:379 [2016] 3 CMLR 40 at [48].

65 *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [48]-[51];

available.[66] This suggests that Mr. Wullems has only general knowledge that access is given to illegal copies of works. Although not mentioned in the decision, it is reasonable to assume, however, that Mr Wullems would also have a degree of knowledge of the specific illegal copies of works made available via the add-ons as he would have needed to test the hyperlinks leading to those works are working before shipping the customised device. In *TPB*, the level of knowledge required in the "intervention in full knowledge" implies specificity, as the operators check if works are included in the categories and perform other editorial checks.[67] The intervention in full knowledge element will be elaborated on in Alternative 3, which will detail based on existing case law which shows that hosting platform operators do not engage in a copyright relevant "intervention in full knowledge of the consequences".

IV. The "public" and the "new public"

25 Following the test for CTTP, once an act of communication is established, the next step is to assess whether the communication is aimed at "a public", which is an indeterminate number of people that can access the communication.[68] The public is assessed cumulatively, according to the number of people that can access the work in succession.[69] As a *de minimis*, groups of people that are too small or insignificant are excluded. Both purchasers of a device that give access to illegal works and the users of TPB amount to "a public".[70]

26 It is not enough for a work to be communicated to a given public, as the public must be "new". The notion of the "new public" was transplanted from the 1978 World Intellectual Property Organisation Guide by AG La Pergola in the *EGEDA* case in the context of the CTTP right in the SatCab Directive.[71] The notion is subsequently adopted by the CJEU in the context of Article 3(1) in 2006 in the *SGAE* decision.[72] Since then, the application of the "new public" element in CTTP is controversial, not only because the notion of "new public" lacks basis in binding legal texts but also because the application of the "new public" is protean.[73] For example, in the situation where the act of communication takes place via a "new technical means" there is an irrebuttable presumption of a "new public".[74] When the communication is done via the same technical means, such as the internet, the "new public" test needs to be satisfied.[75]

27 The new public test assesses whether the communication of copyright works targets "a public which was not taken into account by the authors of the protected works when they authorised their use by the communication to the original public".[76] A limitation to the literal application of this test appears in cases where access is given to illegal copies of works: if there is no consent for the original communication, it is not clear how it can be assessed if the secondary communication targets a different public to the one the rightsholder had in mind when consenting to the initial communication. The CJEU avoids this conundrum by recognising that there is no public taken into account by the rightsholder where infringing

66 *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816; [2017] 4 WLUK 447 at [41].

67 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237 at [38]. See also J. C. Ginsburg and L.A. Budiardjo, "Liability for Providing Hyperlinks to Infringing Content" (2018) 41 Colum JL & Arts 153, 167.

68 *SGAE* EU:C:2006:764 [2007] Bus LR 52 at [38]; *SCF* EU:C:2012:140 [2012] ECDR 16 at [84]; *ITV Studios Ltd* EU:C:2013:147 [2013] Bus LR 1020 at [32]; *OSA* EU:C:2014:110 [2014] [2 WLUK 931 at [27]; *SBS Belgium* EU:C:2015:764 [2015] WLR(D) 466 at [22]; *Reha Training v GEMA* ECLI:EU:C:2016:379 [2016] 3 CMLR 40 at [41]; *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [36].

69 *Phonographic Performance* EU:C:2012:141 [2012] 2 CM.LR. 29 at [35]; *OSA* EU:C:2014:110 [2014] at [28]; *Reha Training* ECLI:EU:C:2016:379 [2016] 3 CMLR 40 at [43] and the case-law cited; *Filmspeler* EU:C:2017:300 at [44];

70 Ibid at [45]; *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237 at [42].

71 Opinion AG La Pergola in *Entidad de Gestión de Derechos de los Productores Audiovisuales (Egeda) v Hostelería Asturiana SA (Hoasa)* (C-293/98) EU:C:2000:66 [2000] ECRI-629 at [12]; Claude Masouyé, 'Guide to the Berne Convention for the Protection of Literary and Artistic Works' (Published by the World Intellectual Property Organisation, Geneva 1978) 71.

72 *SGAE* EU:C:2006:764 [2007] Bus LR 52 at [42].

73 ALAI Executive Committee, "Opinion on the criterion 'New Public', developed by the Court of Justice of the European Union (CJEU), put in the context of making available and CTTP", proposed to the Executive Committee and adopted at its meeting, 17 September 2014 (ALAI 2014); Bernt P Hugenholtz and Sam van Velze, "Communication to a New Public? Three Reasons Why EU Copyright Law Can Do Without a 'New Public'"(2016) 47(7) *IIC* 797, 808.

74 M. Cock and B. Van Asbroeck, "Le Critere du 'Public Nouveau' dans la Jurisprudence Recent de la Cour de Justice" (2015) 4 IRDI 259, 276.

75 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237 at [28].

76 *FAPL* EU:C:2011:631 [2011] ECDR 11 at [197].

copies of works are communicated:[77] "[t]he same finding" (that the authors' consent to the making available has included all internet users as the public and thus there is no new public) cannot be deduced "from those judgments failing such an authorisation". In these cases, the "new public" is assumed and the CJEU assesses whether the user knows that their intervention "provides access to works published without authorisation of the rightsholders".[78]

V. Knowledge

28 In cases of facilitation of access to illegal copies of works, the knowledge of the user also modulates the responsibility of the entity which communicates to a "new public". The considerations over knowledge balance the strict application of the "new public" test which would lead an automatic finding of "new public" which is a disproportionate result for the users involved in the communication of works and for third parties.[79]

29 The application of the knowledge in the context of the "new public" is fraught with uncertainty. Under the banner of knowledge, the language in the decisions oscillates between various standards. In *GS Media*, the CJEU introduced a test of actual and constructive knowledge – whether the link-provider knew or ought to have known that the image freely available on a third-party site to which they link was not published with the rightsholder's consent.[80] The knowledge of the hyperlink-provider needs to relate to specific works made available without consent. The CJEU held that when the link-provider knows or ought to have known that the link at issue provides access to a copyright-infringing work, such a link may fall under the scope of Article 3(1).[81] When the link is provided for-profit or financial gain, the link-provider ought to have known that the link leads to illegal copies of a work, hence there is a rebuttable presumption of knowledge because the link-provider is expected to carry out all "necessary checks" to ensure that the work has not been published without consent.[82] Acts of linking to works for financial gain thus impose a duty on the link-provider to ascertain whether the work is licensed or not.[83] The scope of the duty is a source of academic debate which will be explored below.[84]

30 In the subsequent *Filmspeler* and *TPB* decisions, the CJEU also refers to the profit-making nature of the activities, suggesting the application of a presumption of knowledge as in *GS Media*.[85] Yet, the CJEU decisions confusingly also refer to other forms of *mens rea*. It is clear from advertisements and other statements by the seller of the *Filmspeler* device and operators of TPB that they intended to enable access to illegal copies of works.[86] In *TPB*, the site operators "could not be unaware" that the platform provided access to illegal copies of works given the high number of torrents on the platform.[87] This points to a standard of constructive and general knowledge that access is given to copyright-infringing works. Overall, the references to various constructions of knowledge in those situations arising wherein the user clearly intends the infringement obfuscates the very assessment of the mental state required with the "new public". Standards such as actual and constructive knowledge also steer the CTTP test in a direction that overlaps with un-harmonised national notions of indirect and criminal liability as these doctrines also consider the mental state of the infringer.[88] It remains to be seen if those doctrines will be displaced by the CJEU decisions on CTTP and facilitation of access to illegal copies of works.

77 *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816; [2017] 4 WLUK 447 at [48].

78 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237 at [45].

79 A. Ohly, "The broad concept of 'CTTP' in recent CJEU judgments and the liability of intermediaries: primary, secondary or unitary liability?" (2018) 13(8) Journal of Intellectual Property Law & Practice 664, 673.

80 *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [47].

81 Ibid at [49].

82 Ibid at [51].

83 B. Hanuz, 'Linking to unauthorised content after the CJEU GS Media decision' (2016) 11(2) Journal of Intellectual Property Law and Practice 879, 880.

84 P. Savola, 'EU Copyright Liability for Internet Linking' (2017) 8 JIPITEC 139.

85 *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816; [2017] 4 WLUK 447 at [51]; *Ziggo* EU:C:2017:456 [2017] Bus LR 1899 at [46].

86 *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816; [2017] 4 WLUK 447 at [50].

87 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237 at [45].

88 J. C. Ginsburg, "The Court of Justice of the European Union Creates an EU Law of Liability for Facilitation of Copyright Infringement: Observations on *Brein v. Filmspeler* [C-527/15] (2017) and *Brein v. Ziggo*" (2017) 7. [C-610/15] (2017) Columbia Law and Economics Working Paper 572, Columbia Public Law & Legal Theory Paper #557, 2-3.

VI. "For-profit"- a non-essential element with important implications

31 Finally, the "for-profit" element is considered "not irrelevant" for the existence of an act of CTTP.[89] Yet profit plays an important role in setting the scope of liability as *GS Media* links profit with the presumption of knowledge and the corresponding duty of care. In the case of hyperlinking to illegal copies of works, it is unclear if the posting of a link carried out "for-profit" which is connected to the presumption of knowledge refers to direct profits gained from the act of linking or the general operation of the website.[90] In *GS Media*, as the hyperlink provider the GeenStijl newspaper could financially benefit directly from hyperlinking the leaked Playboy images of the Dutch starlet, it is advanced that a connection should be necessary between the act of hyperlinking to illegal content and the profit made which triggers a presumption of knowledge.[91] Yet in many situations, it may not be possible in practice to show a connection between the hyperlink and profits made by the hyperlink-provider.

32 In *Filmspeler*, the sale and offer for sale of the customised media device were considered to be "for-profit". In *TPB*, the CJEU referred to the significant advertising revenue gained by the platform.[92] Although not clearly specified by the CJEU, these references to "for profit" invite the inference that the presumption of knowledge that access is given to illegal copies of works applies to platforms.[93] The link between profit and the presumption of knowledge underlies the application of duties of care to hosting platforms under Alternative 1 below.

89 *SGAE* EU:C:2006:764 [2007] Bus LR 52 at [44]; *FAPL* EU:C:2011:631 [2011] ECDR 11 at [204]; *ITV Studios* EU:C:2013:147 [2013] Bus LR 1020 at [42]-[43]; *Reha Training* ECLI:EU:C:2016:379 [2016] 3 CMLR 40 at [49]; *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816; [2017] 4 WLUK 447 at [34]; *Ziggo* EU:C:2017:456 [2017] Bus LR 1899 at [28].

90 T. E. Synodinou, "Decoding the Kodi box: to link or not to link? The findings of the court in the decision—a confirmation of recent case law" (2017) 39(12) European Intellectual Property Review 733,735.

91 *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [54].

92 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899 at [46].

93 E. Rosati, "The CJEU Pirate Bay judgment and its impact on the liability of online platform" (2017) 39(12) European Intellectual Property Review 737, 745

C. Alternative 1: Hosting platforms and duties of care under Article 3(1)

33 The complex CTTP test analysed above may be applied to hosting platforms in several configurations, some reaching opposing solutions that generate differing consequences for rightsholders, platforms, technical innovation and the freedom of expression and information of the internet users active on these platforms. In this paper, possible interpretations are offered in Sections C-E. Under a first interpretation, the liability of hosting platforms that provide technical tools for users to upload content may be constructed based on joint tortfeasance. In EU CTTP case law, joint tortfeasance was first applied by the CJEU in *Airfield*, a case concerning satellite broadcasting.[94] A single indivisible act of communication of TV content to subscribers may be legally attributed both to the broadcasting organisation that supplies the signal carrying copyright works and to the satellite package provider that gives subscribers access to works being indispensable to making those works available to the public and is not a mere provider of facilities.[95] In *TPB*, the users and the operators of TPB together engaged in a single act of CTTP infringement which could be split between the uses and operators of the TPB platform. The users originated the torrent files that led to copyright files stored on the nodes of the peer-2-peer network. Then, the *TPB* operators intervened "with full knowledge of the consequences of their conduct, to provide access to protected works"[96] by indexing torrent files which enabled users to locate works in the context of a P2P network, therefore playing an essential role in making the works available. On this basis, in TPB Advocate General Szpunar argued that platform operators should be simultaneously and

94 *Airfield and Canal Digitaal v Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (Sabam)* (C-431/09) and *Airfield NV v Agicoa Belgium BVBA (Airfield)* (C-432/09) EU:C:2011:157 [2012] ECDR 3. In the context of the CTTP, the legal construction where a single act of CTTP may be performed jointly by two parties originates from French 1970s copyright literature. For example, C. Masouyé, "The place of copyright in the use of space satellites" (1972) 72 Revue Internationale de Droit d'Auteur 26, cited in S. Voudsen, 'Airfield, Intermediaries and the Rescue of EU Copyright Law' (2012) 4 I.P.Q. 311, 321.

95 On joint responsibility see also Advocate General Jääskinen in *Airfield* (C-432/09) EU:C:2011:157 [2012] ECDR 3. at [87].

96 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899 at [36]- [37].

jointly liable with the users of the network making available the works shared.[97] The CJEU decision appears to endorse this view of CTTP.[98]

34 Hosting platforms may represent a borderline situation as the platforms perform a socially desirable role, but at the same time provide the technical tools for users to upload and share content, some of it copyright-infringing, but without themselves encouraging copyright infringement.[99] When the provision of the technical conditions for users to upload and share content may be seen as an act of CTTP, to avoid joint liability with their users, a limitation on liability via a duty of care to conduct "necessary checks" of the uploaded content could be imposed.[100] Such an option is available if the decisions in *GS Media*, *Filmspeler* and *TPB* harbinger a duty of care within the CTTP right which may be applicable to hosting platforms.[101] It may be argued that hosting platforms gain advertising or other revenue, therefore a "for profit" element exists to the operation of these services, which may justify the application of a duty of care. Alternative 1 thus explores the application and limits of a duty of care under Article 3(1) to limit the liability of hosting platforms under the same provision.

35 With hosting platforms, experts argue that the scope of the duty of care should be moderated by a standard of reasonableness assessed case-by-case.[102] Under an objective test, the extent of the duty would depend on the type of hosting provider and the provider's propensity for infringement, the commercial nature of the activity, and what measures are reasonable in the circumstances.[103] The size of the provider and its financial resources should also be taken into account. Reasonableness would also prevent the imposition of measures that are technically impossible for the host.[104]

36 The standard of reasonableness resembles a proportionality assessment. In the case law on injunctions against intermediaries whose services are used for copyright infringement in Article 8(3) InfoSoc and the corresponding provision in the third sentence of Article 11 of the Enforcement Directive, the Court sought to establish a "fair balance" between the protection of copyright and the protection of the fundamental rights of individuals affected by such measures.[105] In *L'Oreal v eBay* the CJEU held that the measures taken should be "sufficiently dissuasive, but avoid creating barriers to legitimate trade, and offer safeguards against their abuse".[106] In assessing what is proportionate, courts would have to balance the effect of the duty of care on rightsholders and platforms and the interests of internet users.

37 Rightsholders' copyright as intellectual property is protected under Article 17(2) of the EU Charter of Fundamental Rights. Yet that protection is not inviolable nor absolute, as the CJEU repeatedly found that the protection of copyright needs to be balanced against other fundamental rights.[107] Given that legal content is also shared via hosting platforms, these benefit from the right to conduct business set out in

97 Opinion of Advocate General Szpunar, *Ziggo* EU:C:2017:456 [2017] Bus LR 1899 at [53].

98 E. Rosati, "The CJEU Pirate Bay judgment and its impact on the liability of online platform" (2017) European Intellectual Property Review 737,745.

99 M. Leistner, "Copyright law on the internet in need of reform: hyperlinks, online platforms and aggregators" (2017) 12(2) Journal of Intellectual Property Law & Practice 136, 144.

100 A. Ohly, "The broad concept of 'CTTP' in recent CJEU judgments and the liability of intermediaries: primary, secondary or unitary liability?" (2018) 13(8) Journal of Intellectual Property Law & Practice 664, 672.

101 A. Metzger and M. Senftleben "Comment on the Implementation of Article 17 CDSM Directive" (2020) European Copyright Society p.4. https://europeancopyrightsociety-dotorg.files.wordpress.com/2020/04/ecs-comment-article-17-cdsm.pdf accessed 328 January 2020. Accessed 28 April 2020.

102 E. Rosati, 'The CJEU Pirate Bay judgment and its impact on the liability of online platform' (2017) 39(12) European Intellectual Property Review 737, 746; C. Angelopoulos and J.P. Quintais, "Fixing Copyright Reform A Better Solution to Online Infringement" (2019) 10 JIPITEC 147 para 1, para 55; Ohly (n 103) 673.

103 A. Ohly, "The broad concept of 'CTTP' in recent CJEU judgments and the liability of intermediaries: primary, secondary or unitary liability?" (2018) 13(8) Journal of Intellectual Property Law & Practice 664, 673; for a variety of criteria under German law see also J. B. Nordemann, 'Liability for Copyright Infringements on the Internet: Host Providers (Content Providers) – The German Approach'(2011) 2(1) JIPITEC 37, 37.

104 *YouTube,* District Court of Munich (5 U 87/12) at [61] stating that a word filter is within YouTube's technical ability and does not endanger the business model.

105 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (Netlog)* (C-360/10) ECLI:EU:C:2012:85 [2012] 2 CMLR 18 at [43].

106 *L"Oreal SA v eBay International AG* (C-324/09) EU:C:2011:474; [2012] Bus LR 1369; [2011] 7 WLUK 313 at [144].

107 *Netlog* ECLI:EU:C:2012:85 [2012] 2 CMLR 18 at [42].

Article 16 of the Charter of Fundamental Rights.[108] This involves the right for any business to be able to freely use, within the limits of its liability for its own acts, the economic, technical and financial resources available to it.[109] An infringement of the freedom of a hosting service provider to conduct its business would take place if the provider has to install a complicated, costly, permanent filtering system at its own expense.[110]

38 The interests of internet users are also protected by law. Internet users benefit from protection against infringements of their right to protection of their data provided under Article 8 of the EU Charter of Fundamental Rights. Anti-copyright infringement measures that involve the identification, systematic analysis and processing of information connected with users' profiles created on social media platforms amounts to use of protected data as information regarding user profiles is personal data as it allows users to be identified.[111] Users have additional rights provided by the exceptions and limitations to copyright protection under Article 5 InfoSoc. In *Panier*, the CJEU held that the quotation exception in Article 5(3)(d) reflects users' exercise of the fundamental right to freedom of expression which in that case gained precedence over the rights of authors.[112] In *Deckmyn*, the exception for caricature, parody, or pastiche in Article 5(3)(k) InfoSoc fosters the exercise of freedoms of expression for their beneficiaries.[113] The CJEU recently recognised in *Funke Medien* and *Spiegel Online* that the exceptions and limitations in Article 5 InfoSoc "confer rights on the users of works or of other subject matter".[114] Therefore the application of the duty of care would have to respect the fundamental rights of users and the application of exceptions and limitations under Article 5 InfoSoc.

39 Various possibilities exist to tailor a potential duty of care for hosting platforms under Article 3(1) that balances all these rights to various degrees. Under the duty of care, Ohly argues that at least a duty to take down copyright infringements following a notification from rightsholders may be available.[115] This duty could be extended to an obligation to block the same infringing content from resurfacing on the platform. The duty of care could also be extended to include equivalent infringements from those notified by the rightsholders from resurfacing, provided that the notion of equivalent infringements is interpreted strictly.[116] Removal obligations may be triggered once the provider gains "awareness" and the behaviour expected may be that of a "diligent economic operator" as in the *L'Oréal v eBay* decision on the application of the hosting limitation in Article 14 Directive 2000/3 (E-Commerce Directive).[117] Finally, the duty of care may also include the application of preventative mechanisms to ensure that no copyright-infringing content surfaces on the platform. The following sections will address aspects of a duty of care that involve the duty to check content before it appears live on the platform and obligations as to notice and take-down and stay-down.

I. The duty to check content before it appears live on the platform is illegal

40 Some argue that the activity of YouTube, which organises search results into categories and rankings and recommends videos to its users based on user preferences may be similar to the activity performed by the operators of The Pirate Bay (TPB) where the CJEU had held that such operators "rank, they categorise, they display overviews and they recommend".[118] YouTube acts with constructive

108 See also *Scarlet Extended v Société Belge des Auteurs Compositeurs et Editeurs* (C- 70/10) EU:C:2011:771 [2011] E.C.R. I-11959 paras 44-49.

109 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* (C-314/12) EU:C:2014:192 [2014] Bus LR 541 at [49].

110 *Netlog* ECLI:EU:C:2012:85 [2012] 2 CMLR 18 at [46].

111 Ibid at [49].

112 *Painer v Standard Verlags GmbH* (C-145/10) ECLI:EU:C:2011:798 [2011] ECDR 13 at [135].

113 *Deckmyn v Vandersteen* (C-201/13) EU:C:2014:2132 [2014] Bus LR 1368 at [27], *Pelham GmbH v Hutter* (C-476/17) EU:C:2019:624 [2019] Bus LR 2159 at [60].

114 *Funke Medien NRW GmbH v Germany* (C-469/17) EU:C:2019:623 [2020] 1 W.L.R. 1573 at [70]; *Spiegel Online GmbH v Beck* (C-516/17) EU:C:2019:625 [2019] Bus LR 2787 at [54].

115 A. Ohly, "The broad concept of 'CTTP' in recent CJEU judgments and the liability of intermediaries: primary, secondary or unitary liability?" (2018) 13(8) Journal of Intellectual Property Law & Practice 664, 673.

116 J.P. Quintais, G. Frosio, S. van Gompel, P. B. Hugenholtz, M.Husovec, B. J. Jütte, M. Senftleben, "Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics" (2020) 10 JIPITEC 277 at para 24.

117 E. Rosati, 'The CJEU Pirate Bay judgment and its impact on the liability of online platform' (2017) 39(12) European Intellectual Property Review 737, 746.

118 International Literary and Artistic Association, Opinion in respect of some questions for preliminary ruling by the

knowledge, which can be presumed based on advertising revenue generated from user uploads or with the general knowledge that copyright-infringing content may be uploaded to the website.[119] If hosting providers such as YouTube may be seen as analogous to blatant infringers such as TPB operators, this justifies the expectation that these hosting providers are under a stringent duty of care to check the content. Rightsholders argue that a high level of copyright protection as provided under Recitals 4 and 9 InfoSoc may be ensured only when the duty to check applicable to host providers to check the legality of content *before* it is uploaded.[120]

41 The argument that host providers such as YouTube and Cyando can be legally expected to proactively check for copyright infringement content before it is uploaded on the platforms and without the need for rightsholder cooperation in identifying the copyright-infringing content was convincingly rejected by AG Saugmandsgaard Øe in his Opinion in the *YouTube/Cyando* referral. The AG opposes the analogy between YouTube and TPB on the basis that, in the case of YouTube, technical features such as searching and indexing do not show the operator's intention to infringe copyright.[121] He also rejected the presumption of knowledge as introduced in *GS Media* as it is only applicable to acts of hyperlinking and overall is unfit for hosting platforms such as YouTube and Cyando.[122] This was because, in *GS Media*, the website operator posted the link himself, and hence had specific knowledge of the linked content. In the case of platforms such as YouTube and Cyando, this presumption is unworkable as it would entail the assumption that the host provider who generates profit has both knowledge of the files stored on its servers by its users and awareness of whether or not they are illegal, thus requiring the operator to perform the "necessary checks".

42 If the presumption of knowledge in *GS Media* could be applied to host providers such as YouTube, it would have the effect of creating an *ex-ante* obligation to monitor uploaded content. As AG Saugmandsgaard Øe points out, such an obligation would amount to imposing a general obligation to monitor the information it stores and to actively seek illegal acts or circumstances indicating illegality by, for example, monitoring all files provided by the users of the platform before they are adopted. This outcome is barred by Article 15(1) of the E-Commerce Directive which prohibits Member States from imposing general monitoring obligations on providers covered by liability exemptions in Articles 12-14 of the Directive.[123] General monitoring refers to the active monitoring of all data of each of the platforms' users to prevent any future infringement of intellectual-property rights.[124] It may be argued that hosting platforms such as YouTube should perform the function of host providers as per the definition of a host in Article 14 E-Commerce Directive which refers to information society services that provide, amongst other activities, the transmission or storage of information supplied by a recipient of the service.[125] Therefore, the prohibition on general monitoring applies to hosting platforms such as YouTube.

43 AG Saugmandsgaard Øe also found that an obligation on hosting platforms to pre-emptively check the content their users intend to publish "would introduce a serious risk of undermining" the fundamental rights of the platforms to conduct business as set in Article 16 of the Charter, the right of users to receive and impair information under Article 11 and the freedom of the arts under Article 13 when users upload their creations.[126] Implementation of such a measure where platforms manually check content would also be impossible to achieve given the vast amount of content uploaded. Platforms would also be tempted to err on the side of caution and over-remove content to avoid liability.[127] The implementation of such preventive checks at the point of upload by filtering would also infringe users' fundamental rights as filters are imperfect at distinguishing copyright-infringing from non-infringing content.[128]

CJEU in case C-682/18 (YouTube) (25 February 2019) 5 < https://www.alai.org/en/assets/files/resolutions/190225-opinion-youtube-en.pdf> accessed 01 March 2019.

119 Ibid.

120 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [238].

121 Ibid at [125].

122 Ibid at [113] and footnote 102.

123 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [112]-[115].

124 *Netlog* ECLI:EU:C:2012:85 [2012] 2 CMLR 18 at [26] and [34].

125 CJEU held that online social media sites Netlog and Facebook, are hosts within the meaning of Article 14 E-Commerce Directive in relation to content uploaded by users see *Netlog* ECLI:EU:C:2012:85 [2012] 2 CMLR 18 at [27] and *Eva Glawischnig-Piesczek v Facebook Ireland* (C-18/18) EU:C:2019:821 [2020] 1 W.L.R. 2030 at [22].

126 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [240]-[241].

127 Ibid at [242].

128 Ibid at [243].

However, as the obligation to check content before it appears live on the platform breaches EU law, less intrusive measures may be possible under the duty of care approach.

II. A duty of care to remove specific content may be available under EU law

44 Article 14(1) of the E-Commerce Directive places hosting platforms under an obligation to remove specific illegal content once they have actual knowledge of its existence. An analogous obligation may be included within the scope of the duty of care under Article 3(1) InfoSoc Directive. Yet, such an obligation to remove content may generate tension with the application of exceptions and limitations in Article 5 InfoSoc Directive. When operators of hosting platforms need to remove a specific piece of infringing content following notification from rightsholders, the notification should state the work which is infringed, the exclusive rights or licences the notifier has over the work and a reasonable explanation as to why no copyright exception is applicable.[129] In the case of notifications that concern blatantly infringing content, for example, a video containing a Netflix show episode, the reliability of rightsholders' assessment over the illegality of the content is straightforward. Problems begin in borderline situations where exceptions and limitations in Article 5(3) InfoSoc may apply. Arguably, most relevant exceptions and limitations in relation to uses of works on hosting platforms may be Article 5(3)(d) concerning quotations, Article 5(3)(k) concerning parodies, and Article 5(3)(i) concerning the incidental inclusion of a work or other subject matter in other material. Copyright holders may not possess the requisite legal knowledge to make an informed assessment regarding the legal status of the work's use. Rightsholders are not a homogenous group and whereas some such as Hollywood studios have extensive legal advice, individual rightsholders cannot be assumed to understand the intricacies raised by the application of copyright exceptions and limitations. All rightsholders may also be tempted to err on the side of caution in their assessments.

45 Instead, hosting platforms may be required to employ trained staff that assesses the accuracy of the rightsholders' notifications regarding specific infringing content made available on hosting platforms.[130] Given that millions of bits of content are uploaded on hosting platforms' servers daily, the expense of checking all notifications raises operations costs, hence the legality of this obligation is not clear. Under EU law, the costs of copyright enforcement bourn by a platform are relevant to the proportionality of a measure. The CJEU has held that measures imposed on an intermediary can restrict the free use of their resources because it obliges them to take measures which may represent a significant cost, have a considerable effect on their activities or require difficult and complex technical solutions.[131] The platforms' freedom to conduct a business enshrined in Article 16 of the Charter is, however, only impaired when "the very substance" of that freedom is affected. [132] This does not take place when the intermediary has the flexibility to put in place measures that are "best adapted" to the provider's resources and abilities and are compatible with other challenges raised in its other activities. [133] The use of trained staff to assess the validity of a copyright notice does not seem out of line with the daily operations of many hosts who already have to employ staff to assess the illegality of other types of content, such as terrorist communications, hate speech, and other indecent communications. However, given the volumes of data involved, and the potential for copyright notifications, the assessment of each rightsholder notification by a human reviewer may be too onerous in practice.

46 One cost-effective way to automatically remove content on notification by rightsholders is via automated systems, such as YouTube's ContentID. The disadvantage is that such tools may remove content that would normally be covered by an exception or limitation. A well-known example is the YouTube takedown of a copyright lecture by Professor William Fisher of Harvard. The lecture contains snippets of various sound recordings to demonstrate a point on compulsory licencing, and this use of sound recordings may be exempt by the fair use doctrine in the US.[134] Most problematic is the

129 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [190].

130 J. B. Nordemann, "Liability for Copyright Infringements on the Internet: Host Providers (Content Providers) – The German Approach" (2011) 2(1) JIPITEC 37, 41.

131 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* (C-314/12) [2014] Bus LR 541 at [50].

132 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* (C-314/12) [2014] Bus LR 541 at [51].

133 Ibid at [52].

134 M. Mansink, "Sony Music Issues Takedown On Copyright Lecture About Music Copyrights By Harvard Law Professor" (Torrent Freak 2016)< https://www.techdirt.com/articles/20160214/08293233599/sony-music-issues-takedown-copyright-lecture-about-music-copyrights-harvard-law-professor.shtml> accessed 02 May 2020.

safeguard of mechanically non-verifiable exceptions. In particular, the application of exceptions such as for caricature, parody or pastiche in Article 5(3)(k) InfoSoc requires a degree of legal sophistication which cannot easily be programmed into a filter. Any accidental removal of exempt uses may, in theory, be mitigated by the provision of a complaint and redress mechanism for internet users. Should a work be taken down which is covered by the exception, the user could appeal.[135]

47 The effectiveness of such a complaint and redress system is also questionable. Data from internet user counterclaims against the takedown of content reveals that very few appeal. Google's Transparency Report shows that between January and March 2020, a total of 6,111,008 videos were automatically removed from YouTube, of which 165,941 were appealed and subjected to human review, with 41,059 subsequently reinstated.[136] Although the Report is not specific to copyright takedowns, the information therein is still revealing. Given that very few users appeal takedowns, the implication is that the availability of complaints and redress mechanisms in practice largely serves to support the legitimacy of automatic notice and takedown procedures.

48 One way to safeguard the application of exceptions and limitations in Article 5(3) InfoSoc Directive may be seen in the definition of "specific content" in *Glawischnig-Piesczek*, a defamation case, where the CJEU found that Article 15(1) E-Commerce Directive allows an injunction that requires Facebook to remove and monitor specific content declared illegal in court.[137] Under the terms of that injunction, Facebook has to remove content identical to that deemed illegal; content which is equivalent to it or block access to it, and the injunction can have an effect worldwide.[138] The definition of a "specific" case is interesting for our purposes. In *Glawischnig-Piesczek*, the CJEU found that a "specific case" may consist of a particular piece of information stored by the host provider at the request of a certain user of its platform, the content of which was examined and assessed by a court having jurisdiction in the Member State, which, following its assessment, declared it to be illegal.[139] This approach could be followed in the area of copyright in a situation where the duty of care would also cover borderline situations where exceptions and limitations in Article 5(3) InfoSoc may apply. The aplication of the duty could be conditioned on rightsholder's submitting a court's decision to the platform which identifies an infringement and hence the non-application of a specific exception. By subjecting the application of the duty of care to a court finding of infringement in the underlying uploaded material, the scope for the removal of content covered by exceptions and limitations is largely mitigated.[140]

49 Again, there are limitations to this approach. Court proceedings are expensive, slow, and impractical for rightsholders and therefore not suitable for high volume infringements. In addition, due to the territorial application of copyright, a finding of infringement in one Member State does not apply cross-border. The list of exceptions in Article 5(3) InfoSoc is also optional, and an exempted use in one EU Member State may not be exempted in the next, therefore rightsholders would have to know where to bring proceedings. Yet these drawbacks may be mitigated by the fact that the bulk of infringement consists of identical copies of copyright-protected works.[141] Therefore subjecting the removal of suspected and borderline infringement cases to court scrutiny may not detract substantially from the efficacy of the duty of care. Rightsholders would go to court only when they felt they had a real case against a specific use, which would reduce the potential for opportunistic takedown requests. This approach would also allow for the sharing of information between users of these platforms whilst protecting against the most serious offences. The reduction of copyright enforcement efficacy would be offset by fundamental rights gained by users and platforms.

III. A duty of care to include the stay-down of identical infringements may be available under EU law

50 A stay-down duty would require hosting platforms – after receiving notice from rightsholders regarding copyright infringements – to remove the content and

135 The CJEU has previously provided for a redress system for internet users in the case of blocking injunctions. See *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* (C-314/12) EU:C:2014:192 [2014] Bus LR 541.

136 Google Transparency Report, "Appeals" <https://transparencyreport.google.com/youtube-policy/appeals?hl=en> accessed June 2 2020.

137 *Eva Glawischnig-Piesczek* EU:C:2019:821 [2020] 1 W.L.R. 2030

138 Ibid at [37]- [38] and [50].

139 Ibid at [35].

140 J. Urban and others, "Notice and Takedown in Everyday Practice" (2017) 41 UC Berkeley School of Law 41.

141 J. B. Nordemann, "Liability for Copyright Infringements on the Internet: Host Providers (Content Providers) – The German Approach" (2011) 2(1) JIPITEC 37, 41.

take measures to ensure that it does not resurface on the platform.[142] This measure appears in line with EU law in *L'Oréal v eBay* where the CJEU allowed for the imposition of measures aimed at preventing "further infringements of that kind".[143]

51 Fulfilment of the duty of care in this context once again requires the application of content recognition technology such as filtering, as the manual removal of re-appearing infringing content is near-impossible.[144] The application of these technologies to prevent copyright infringements from resurfacing raises the emergence of general monitoring, which is prohibited by Article 15(1) E-Commerce Directive. In *SABAM and Netlog*, the CJEU rejected the collecting society SABAM's injunction which required the social media site Netlog to install a filtering system that monitored its servers for copyright infringement in musical, cinematographic or audiovisual works stored by Netlog's users. The monitoring was to be applied to all users for an unlimited period as a preventative mechanism and at the expense of the platform.[145] However, Recital 47 E-Commerce Directive states that monitoring duties in specific cases are legal. For example, when the provider would have to prevent the reposting of illegal copies of specific works on the provider's network. Yet the line between general monitoring and monitoring in specific cases is not a clear one. In particular, when rights holders request the stay-down of numerous specific titles the cumulation of specific works amounts to general monitoring.[146]

Further clarification regarding the line between monitoring in specific cases and general monitoring is necessary.

IV. Additional systemic advantages and disadvantages of a harmonising the liability of hosting platforms via duty of care in the context of Article 3(1)

52 The duty of care approach may introduce a conditional responsibility regime within the scope of Article 3(1). This might be a balanced solution as the fulfilment of the duty of care would remove the application of direct liability. The duty of care solution supports the Digital Single Market as it provides a unified solution to the longstanding difficulties of reconciling the liability of hosting platforms for copyright-infringing content uploaded by users at the national level. By bringing the activities of hosting platforms under the scope of the exclusive right under Article 3(1), they come within the scope of the EU's harmonisation mandate.[147] According to the AG in *TPB*, the discrepancies in national approaches "undermine the objective of EU legislation in the relatively abundant field of copyright, which is precisely to harmonise the scope of the rights enjoyed by authors and other rightsholders within the single market".[148]

53 From the perspective of rightsholders, applying a liability standard based on duties of care is that it involves a negligence standard. Normally, the subsistence of the exclusive right of CTTP requires an act which amounts to a use of the work. The violation of certain standards of conduct relating to the duty of care are performance-based aspects and have never before been linked to the elements of an exclusive right. The European Copyright Society considers this a "remarkable deviation from the traditional way of tailoring exclusive rights".[149] The duty of care applied for the CTTP right in Article 3(1) may be perceived as watered-down once subject to a strict standard.

142 Angelopoulos and S. Smet, 'Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability" (2016) 8(2) JML 266, 287-288.

143 *L'Oréal SA v eBay International AG* (C-324/09) EU:C:2011:474; [2012] Bus LR 1369; [2011] 7 WLUK 313 at [127].

144 European Commission, "Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online, Towards an enhanced responsibility of online platforms" COM (2017) 555 final, p.19. Content recognition technology, such as YouTube's Content ID or Audible Magic compares uploaded content with a database of copyrighted works to identify matches.

145 *SABAM* (EU:C:2012:85) [2012] 2 CMLR 18 at [26] and [62].

146 M. Senftleben, "Bermuda Triangle: licensing, filtering and privileging user-generated content under the new Directive on copyright in the digital single market" (2019) 41(8) EIPR 480, 484.

147 On maximum harmonisation see also J. Koo, *The Right of CTTP in EU Copyright Law* (Hart Publishing 2019) 138.

148 Advocate General Szpunar, *Ziggo* EU:C:2017:456 [2017] Bus LR 1899.

149 A. Metzger and M. Senftleben 'Comment on the Implementation of Article 17 CDSM Directive' (2020) European Copyright Society, 4 < https://europeancopyrightsocietydotorg.files.wordpress.com/2020/04/ecs-comment-article-17-cdsm.pdf> accessed 03 May 2020.

54 From the perspective of internet users, another problem is that the duty of care approach – where hosting platforms work to reduce the availability of copyright-infringing content on their servers – privatises copyright enforcement and may open the gates for private censorship. Were the duty of care to be placed within the scope of Article 3(1), a breach would expose platforms to primary liability and damages for their failure to act against copyright-infringing uploads, with potentially expensive consequences. This would incentivise platforms to remove or block content at the merest suspicion of copyright infringement and the potential effects on freedom of expression and information under Article 11 of the Charter are clear. Over-zealousness enforcement would increase the likelihood that non-copyright-infringing content would be removed or blocked, including content covered by exceptions and limitations. Caution, therefore, should be exercised when setting the scope of the duty of care and safeguards for users should become paramount.

D. Alternative 2: Could hosting platforms be exempt from joint liability for communicating works to the public via Recital 27 InforSoc?

55 A separate interpretation sees the activities of hosting platforms as the provision of "physical facilities" as per Recital 27 InfoSoc Directive, with the consequence that the platforms are not performing an act of communication and therefore not open to duties of care within the context of Article 3(1).[150] Recital 27 states that "[t]he mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Directive". In CJEU jurisprudence on CTTP, the mere provision of facilities as in Recital 27 InfoSoc, is set out as the opposite to an intervention "in full knowledge of the consequences of its action, to give access to the protected work to its customers" required for an act of "communication".[151] Although Recital 27 is not an element of the test for CTTP in Article 3(1), it was explained by AG Sharpson in *SGAE* that the recital acts as an "unequivocal" limitation to the establishment of an act of communication, which is a requirement for CTTP liability[152]

56 Although the wording "physical facilities" suggests an application limited to the provision of technical equipment, there is a suggestion in the literature that Recital 27 may also apply to certain intermediaries.[153] This point has also been raised at the national level, in particular in the Netherlands in the case of a supplier of Usenet services.[154] At the CJEU level, the only indication that Recital 27 may apply to hosting platforms appears in *TPB* where the CJEU invokes Recital 27 to justify the existence of an "intervention in full knowledge" by the operators of the P2P sharing platform.[155] If Recital 27 only applies to physical carriers of data, then it is a *non sequitur* that an online platform may be a provider of facilities, unless recourse to Recital 27 is only cosmetic to reinforce the idea that TPB operators were engaging in a copyright relevant intervention.

57 The opinion of AG AG Saugmandsgaard Øe in the *YouTube/Cyando* referral makes a strong case for the application of Recital 27 to hosting platforms. The AG explains that any CTTP involves a chain of interventions by several players in different capacities and to different degrees. In that chain, a distinction needs to be drawn between operators of the platforms performing an "active intervention" in the content uploaded by users, which contributes to the operators' primary liability under Article 3(1), and the provision of physical facilities under Recital 27. YouTube and Cyando were seen as mere providers of physical facilities under Recital 27. The intervention by the operators of hosting platforms is limited to the provision of "server space" or "an electronic communication service", activities considered to fall within the application of Recital 27.[156] This is the most expansive application of Recital 27 at the CJEU level.

150 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [68]-[88].

151 *SGAE* EU:C:2006:764 [2007] Bus LR 52 at [40] and [42]; *FAPL* EU:C:2011:631 [2011] ECDR 11 at [194]; *Reha Training* ECLI:EU:C:2016:379 [2016] 3 CMLR 40 at [46].

152 Advocate General Sharpson in *SGAE* EU:C:2006:764 [2007] Bus LR 52 at [27].

153 K. Koelman and P. B. Hugenholtz, "Online Service Provider Liability for Copyright Infringement" (1999) WIPO Workshop on Service Provider Liability, World Intellectual Property Organisation, 13; Pamela Samuelson, " Regulating Technology Through Copyright Law: A Comparative Perspective" (2020) 42(4) EIPR 214, 215.

154 *News-Service Europe B.V. (NSE)*, Court of Appeal of Amsterdam, ECLI:NL:GHAMS:2014:3435 at [3.3.2]– [3.3.3].

155 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237 at [38].

156 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [74] and [80] and footnote 46.

I. An active intervention

58 In the view of AG AG Saugmandsgaard Øe in *YouTube/Cyando*, the entity which performs an act of communication (as opposed to a provider of facilities) "is the one who voluntarily intervenes to transmit works to an audience so that, in the absence of its intervention, that audience would not be able to enjoy it", thus playing an essential role.[157] This includes the person who decides to transmit the work to an audience and who actively initiates the communication, such as the internet users of the services.[158] To perform an act of communication, "a service provider goes beyond the role of intermediary when he intervenes actively in the 'CTTP' of works". An active intermediary "selects the content transmitted, determines it in some other way or presents it to a public in such a way that it appears to be his own". Here, the reasoning of AG Saugmandsgaard Øe draws a parallel between active intervention and liability for "making content one's own" which applies to content providers in Germany.[159] An active intermediary can also be a provider engaging in a "subsequent use of that "communication", by retransmitting it to a "new public" or according to a "different technical mode". In all these situations the provider does not merely provide installations but plays an essential role by voluntarily communicating works to an audience.[160] An active intermediary is communicating jointly with the users that provide the illegal content.

II. Recital 27 and hosting platforms

59 Intermediary providers whose services are used to carry out a CTTP following the instructions of their users do not decide on their own initiative to transmit the works supplied to an audience and are thus covered by Recital 27.[161] YouTube/Cyando do not perform an active intervention in the content provided and are hence covered by Recital 27. Firstly, the AG Saugmandsgaard Øe finds that it is the platforms' users who play an indispensable role as they decide to make works available via the platforms by choosing the adequate option in the context of YouTube and by sharing the download links online in the case of Uploaded.[162] Internet users perform an intervention without which platforms could not transmit the works or users could not enjoy the same works.[163] Secondly, due to the automated nature of the uploading system, the platforms do not determine the content uploaded and are not engaging in a selection of the uploaded works.[164] The control exercised *a posteriori*, for example, to react further to a notification cannot amount to a selection of content *a fortiori*.[165] *Ex post* control over certain content can also not reflect the choice of the operators to communicate that content.[166] Thirdly, there is no subsequent use of the works by the platforms to a new public or according to a different technical means, as at issue, there is only one communication initiated by the users.[167]

60 In addition to these points, AG Saugmandsgaard Øe also refutes the argument put forward by the rightsholders that the structuring of user-uploaded content, integrating that content into a viewing interface, indexing the content in categories, the provision of a search function which processes search results, and the classification of content are relevant to a finding of CTTP.[168] He argues that the structuring of content uploaded by users does not preclude the conclusion that Recital 27 applies as there is nothing in the Recital to suggest that provision of facilities needs to be "simple"; a degree of sophistication is allowed to facilitate its use. These activities are designed to optimise access and facilitate the platform's use, and this does not amount to an active intervention in the CTTP initiated by the users.[169]

61 The AG differentiates between optimising access to the uploaded content and optimising the uploaded content itself:

157 Ibid at [72].

158 Ibid at [73] and [77].

159 Ibid footnote 49.

160 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [75].

161 Ibid at [74].

162 Ibid at [77].

163 Ibid at [77].

164 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [78].

165 Ibid footnote 59.

166 Ibid at [78].

167 Ibid at [79].

168 Ibid at [81].

169 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [82].

> *The fact that a platform such as YouTube has a standard viewing interface does not, in my view, lead to the conclusion that its operator presents the content to the public in such a way that it appears to be its own, provided that this interface indicates, for each video, which user has posted it.*[170]

62 In relation to Cyando, the argument cannot apply as the platform did not structure the content stored by its users, and that a third-party site acted as link collections are irrelevant to the legal status of the upload platform.[171]

63 Recommended videos such as by YouTube are automatically generated based on previous views and do not reflect the operator's decision to communicate works.[172] The stipulation in the general conditions of use of the platform, that each user grants YouTube a free non-exclusive worldwide license for the uploaded videos does not show that the operators are actively involved in the content, as the stipulation applies automatically to all content uploaded.[173] This would not be the case if the operators of the platforms re-used the content.

64 Finally, the remuneration received by YouTube via advertising revenue, or by Cyando by subscription revenue, does not affect the conclusion that they are not providers of facilities within the meaning of Recital 27.[174] Following the decision in *Reha Training*, the AG opined that the for-profit element is not relevant to the existence of a CTTP. The AG also opined that the for-profit nature of a provision of facility enabling a communication does not cancel the application of Recital 27.[175] Secondly, he argued that the link between profits and the attractiveness of uploaded content does not lead to a finding of CTTP, as it is the users who decide what content is uploaded.

65 The AG largely drew on case law which advances a distinction between an active and passive service provider as developed in the CJEU Article 14 E-Commerce. For example, in *Google France*, it was the user of the service who chose the trademark signs as keywords, not the search engine provider itself, who was passive.[176] Similarly, in *L'Oréal v eBay* the user of the marketplace published the sale offers consisting of trademark-infringing goods.[177] Following the *L'Oréal v E-Bay* decision, the AG was not persuaded that structuring the presentation of the offerings and indexing and the provision of a search function was relevant, hence should not be relevant in the case of CTTP.[178] The AG, therefore, found that operators of YouTube and Cyando were not directly liable under Article 3(1), but may attract secondary liability at the national level.

III. The scope of Recital 27 InfoSoc is not sufficiently wide to limit the direct liability of intermediaries

66 It is not clear cut that Recital 27 is best placed to constrict the liability under Article 3(1) of hosting platforms such as YouTube and Cyando. The legislative history, wording and CJEU case law application of Recital 27 suggest that the inclusion of intermediaries such as YouTube and Cyando within the scope of that recital is strained. When the InfoSoc Directive was being drafted, hosting platforms were unheard of. Recital 27 InfoSoc implements phrase 1 of the Agreed Statement on Article 8 of the World Copyright Treaty (WCT) which states that: "It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention".[179] The Agreed Statement is "intended to clarify the issue of liability of service and access providers in digital networks like the Internet".[180] It was introduced following intensive lobbying by non-governmental organisations representing internet service providers (ISPs) and telecommunication companies. These parties

170 Ibid at [83].

171 Ibid footnote 61.

172 Ibid at [84].

173 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [85].

174 Ibid at [86].

175 Ibid at [87].

176 Ibid at [89].

177 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [90].

178 Ibid at [91].

179 WIPO Copyright Treaty (WCT) (1996) with the agreed statements of the Diplomatic Conference that adopted the Treaty and the provisions of the Berne Convention (1971) referred to in the Treaty at footnote 8 <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_226.pdf> accessed 21 June 2018; Agreed Statement with Art. 8 of the WIPO Copyright Treaty, WIPO document CRNR/DC/96 (23 December 1996).

180 WIPO, *Intellectual Property Handbook: Policy, Law and Use* (WIPO 2004) 272.

sought to obtain some guarantee concerning liability limitations for infringement committed by their users on their networks. [181] The Statement clarifies that there is no direct liability for entities covered by it, with contributory and vicarious liability still available at the national level.[182] It reflects the idea of Basic Proposal I of 1996 Note on Article 10 WCT (which subsequently became Article 8 WCT). The Basic Proposal extends the right of CTTP to making available right of works and it is explained that "what counts is the initial act of making the work available, not the mere provision of server space, communication connections, or facilities for the carriage and routing of signals".[183] This is understood as providers who sell cables or computers or devices for online communications.[184]

67 The Statement is implemented in the EU by Recital 27 InfoSoc. The ethos of that recital was expressed by AG Trstenjak in *SCF*: "persons who provide players, but do not at the same time control access to copyright works, do not make any communication to the public".[185] Examples of activities that may be covered by Recital 27 that have filtered through the CJEU case law include the sale of TV sets and the mere installation of TV sets without the distribution of signals;[186] placing a computer with an internet connection at the disposal of the public in a cybercafé or library;[187] the sale or rental of televisions or radios; or where an ISP merely provides access to the internet.[188] These parties are too removed from the chain of causation to attract responsibility for communications to the public.

68 Recourse to Recital 27 in CJEU judgements on CTTP largely serves to reinforce, by contrast, the existence of an intervention in full knowledge by a user.[189] A technical act falling under Recital 27 also has the role to maintain "the quality of the reception in the signal catchment area" for an audience covered by the initial authorisation of the rightsholder.[190]

69 The CJEU has only twice limited the application of CTTP in Article 3(1) by recourse to Recital 27, which has received strict interpretation. This is unsurprising given the wording "mere" and "in itself" in Recital 27. In *SBS Belgium*, the Court held that direct injection transmissions by broadcasting organisations to distributors of signals who give access to subscribers to those broadcasts are not a CTTP performed by the broadcasting organisation but by the distributors who may transmit signals via decoders or other transmission technologies.[191] Yet in some cases, responsibility for transmissions by direct injection is not carried out by distributors when they are not independent of the broadcasters, and their intervention is purely technical; it is just a means to improve the reception of the broadcast.[192] These distributors could be ISPs involved in the distribution of broadcasts communicated by broadcasting organisations.[193] In *Stim*, a car rental company offering short-term rental of cars equipped with radio receivers, was not intervening in full knowledge of the consequences of its action to give

181 M. Ficsor, *The Law of Copyright and the Internet* (Oxford University Press 2002) 509.

182 M. Ficsor, "Copyright for the Digital Era: The WIPO Internet Treaties" (1997) 21(3-4) Columbia-VLA Journal of Law & Arts 197, 214.

183 Basic Proposal for the Substantive Provisions of the Treaty on certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference CRNR/DC/4 note 10.10.

184 J. Reinbothe and S. von Lewinski, *The WIPO Treaties on Copyright: A Commentary on the WCT, the WPPT, and the BTAP* (Oxford University Press 2015) point 7.8.43.

185 Advocate General Trstenjak in *SCF* EU:C:2012:140 [2012] ECDR 16 at [95].

186 Ibid at [95]; *Organismos Sillogikis Diacheirisis Dimiourgon Theatrikon kai Optikoakoustikon Ergon v Divani Acropolis Hotel and Rousin AE* (C–136/09) EU: C: 2010: 151 [2010] ECRI-37 at [40]; Case C-136/09 Sillogikis para 40 -check; *SGAE* EU:C:2006:764 [2007] Bus LR 52 at [46].

187 Advocate General Kokott in *FAPL* EU:C:2011:631 [2011] ECDR 11 at [204]; Advocate General Trstenjak in *Phonographic Performance* EU:C:2012:141 [2012] 2 CM.LR. 29 at [164].

188 Ibid at [164]. Indeed, in Belgium, the Court of First Instance of Brussels found internet access providers to fall within the scope of Recital 27 see *Etat Belge v SABAM* (13/12839/A) Bruxelles Court of First Instance (2015) at [51].

189 See for example *SGAE* EU:C:2006:764 [2007] Bus LR 52 at [42]; FAPL para 194; *ITV Studios Ltd* EU:C:2013:147 [2013] Bus LR 1020 at [30].

190 *SGAE* EU:C:2006:764 [2007] Bus LR 52 at [42].

191 The "direct injection" of signals represents a technology to transmit broadcast signals directly to distributors without those signals being accessible to the public until they have been supplied by the distributor to its subscribers see *SBS Belgium* EU:C:2015:764 [2015] WLR(D) 466 at [7] and [34].

192 Ibid at [32].

193 The SBS Belgium decision was codified in Directive 2019/789 of 17 April 2019 laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes, and amending Council Directive 93/83/EEC, OJL 130.

their customers access to a protected work.[194] Recital 27 applies as there is no "additional intervention" from the car hiring company which makes it possible to receive via the radios pre-installed in the vehicle the terrestrial broadcasts available in the area where the vehicle is located.[195] In both *SBS Belgium* and *Stim*, the entity potentially covered by Recital 27 acts as a mere carrier in the strict sense for the works communicated by the broadcasting organisation. This suggests that the application of Recital 27 requires that the interference with the content of the communications transmitted needs to be kept to a minimum.

70 Services such as YouTube and Cyando go beyond the minimum level of involvement specified by CJEU case law in *SBS Belgium* and *Stim.* Hosting platforms automatically structure, categorise and provide recommendations in the case of YouTube, and Cyando provides automatic access links to the uploaded content. Although these processes are automated, they nevertheless foster a closer contact with the individual works uploaded by the platforms' users than the degree of contact that providers covered by Recital 27 such as ISPs apply. Although ISPs automatically engage with the data that is uploaded by users on their networks, for example by routinely filtering the internet for spam or blocking access to illicit sites, the nature of their involvement is different from that of hosting platforms. The EU has taken note of different levels of interaction with the data transmitted by the various information society services. The E-Commerce Directive specifies in Articles 12-14 a graduated system of exemptions from liability at the national level for internet intermediaries that qualify. The application of the limitation from liability at the national level of hosting services that store content provided by their users (such as hosting platforms) is predicated upon an additional condition which requires hosts to expeditiously remove or disable access to illegal content uploaded by their uses on their networks upon gaining actual knowledge or awareness that illegal content is available therein.[196] Such a condition does not exist in the case of the liability limitation in Article 12, applicable to mere conduits such as internet access providers. The reason for this difference in legal treatment between hosts and mere conduits is "based on providers' degree of involvement with the content transmitted and their scope for monitoring content."[197] Abstracting the role of hosting platforms with the content uploaded by their users to that of a mere provider of facilities would stretch the purpose and CJEU application of Recital 27. This does not mean that hosting platforms are liable for an act under Article 3(1), rather, Alternative 3 below will show that the limitation to the liability of hosting platforms paper may be achievable within the range of the test for CTTP itself.

E. Alternative 3: Hosting platforms do not intervene in full knowledge to give access to copyright-infringing copies of works

71 The interpretation advanced under this alternative departs from the opinion of AG Øe that the intervention of YouTube and Cyando in the communication initiated by their users amounts to "the mere provision of facilities" as per Recital 27. Instead, it advances a new alternative of application of the CTTP test under which operators of certain hosting platforms that provide the technical conditions for internet users to upload content are not performing an act of communication for the purposes of Article 3(1) InfoSoc Directive. Although content is made available by users via these platforms, that act may only be attributed to users that upload content. Under the evaluation advanced in this section, the operators of certain hosting platforms do not act "in full knowledge of the consequences of his conduct to give customers access to a work illegally posted on the internet".[198] Hence, there is no need to look further at whether the platform operators communicate to a new public and corresponding knowledge element.

I. Platform operators may not perform a copyright relevant "intervention" in "full knowledge" with the copyright-infringing content uploaded by their users

72 The CJEU has emphasised the essential role played by the user who intervenes, in full knowledge of the facts, to give the public access to protected subject

194 *Foreningen Svenska Tonsattares Internationella Musikbyra upa (Stim) v Fleetmanager Sweden AB* (C-753/18) EU:C:2020:268 [2020] 4 WLUK 20 at [32]- [34].

195 *SBS Belgium* EU:C:2015:764 [2015] WLR(D) 466 at [33].

196 Recital 26, Article 14(1)(b) E-Commerce Directive.

197 Opinion of the Economic and Social Committee on the Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market, 1999 O.J. (C 169) at 4.11.1.

198 *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [47]-[48].

matter,[199] but the notion of "intervention" in CJEU jurisprudence on CTTP remains undefined. The Court has repeatedly described a copyright-relevant intervention with adverbs such as "indispensable" or "essential" implying that, in the absence of that intervention, the public can access the works only with difficulty.[200] At first sight, any intervention in the chain of causation which leads to accessing copyright content may be seen as "indispensable" or "essential", as the ISP that supplies internet to TPB servers is performing an indispensable intervention, bar Recital 27; but a close look at the application of the "intervention in full knowledge" element across CTTP case law reveals various thresholds for copyright-relevant interventions.

1. Hyperlinking case law

73 Control over the provision of access to works by manually triggering that access is the essence of an intervention in hyperlinking cases. In *Svensson*, an intervention was held to take place when the hyperlink "allow[ed] users of the website on which it is [manually] posted [by the user] to circumvent the restrictions taken by the site where the protected work is posted to restrict the public's access to its own subscribers"[201] In *GS Media*, the provision of a hyperlink amounted to a deliberate intervention when the link-provider acts with the requisite knowledge or is placed under the presumption of knowledge and does not conduct the necessary checks.[202] The CJEU states that:

> *...rightsholders, in all cases, have the possibility of informing such persons [i.e. hyperlink-providers] of the illegal nature of the publication of their work on the internet and of taking action against them if they refuse to remove that link.*[203]

74 Although in *GS Media* the onus was on knowledge, it is only because the link-provider controlled access to the work in the first place via the link that the CJEU recommended the takedown of the link as a viable course of action. In *Filmspeler,* Mr Wullems:

> *"with full knowledge of the consequences of [its] conduct, pre-installs onto the 'Filmspeler' multimedia player that he markets add-ons that specifically enable purchasers to have access to protected works published – without the consent of the copyright holders of those works – on streaming websites and enable those purchasers to watch those works on their television screens"*[204]

75 In other words, Mr. Wullems took control over access to the illegal copies of works by customising its device with hyperlink-carrying add-ons which it then sold as a service that facilitated direct access to those works.

2. Case law on a joint act of CTTP

76 In the case law on a joint act of CTTP performed by two players, there is an additional layer to an intervention in the supply of works initiated by third parties. It can be seen from the decisions in *Airfield* and *TPB* that in addition to the personal involvement of the operators in triggering access to the works supplied by a third party, the operators of exercised decision-making over the content provided in their own service and for-profit. In *Airfield*, the CJEU found that the activities by Airfield, a satellite television provider which sold a package of satellite channels that can be accessed by subscribers using a satellite decoder, amounted to an intervention in the signal supplied by a broadcast organisation. The intervention targeted a "new public" as its action to encrypt the signals or supply access keys created a link between the broadcast organisation and the subscribers.[205] This act did not ensure or improve reception but made works available to an additional public than the public originally envisaged by the rightsholder.[206] Airfield also bundled several channels from different broadcasting organisations into a new audio-visual product, deciding on the composition of the package created.[207] This largely follows the opinion of AG Jääskinen that the broadcasting organisations lost control of the operations following Airfield's intervention.[208] Furthermore, Airfield had the discretion to include or exclude the television programmes in its service.[209]

199 *Reha Training* ECLI:EU:C:2016:379 [2016] 3 CMLR 40 at [46]; *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [36]; *Ziggo* EU:C:2017:456 [2017] Bus LR 1899 at [26].

200 Ibid at [26].

201 *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [50], *Nils Svensson* EU:C:2014:76 [2014] WLR(D) 67 at [27] and [31].

202 *GS Media* EU:C:2016:644 [2017] C.E.C. 442 at [49]-[51].

203 Ibid at [53].

204 *Filmspeler* EU:C:2017:300 [2017] Bus LR 1816; [2017] 4 WLUK 447 at [41].

205 *Airfield* (C-432/09) EU:C:2011:157 [2012] ECDR 3. At [78].

206 Ibid at [79].

207 Ibid at [81].

208 Opinion of Advocate General Jääskinen in *Airfield* (C-432/09) EU:C:2011:157 [2012] ECDR 3 at [87] and [88].

209 Ibid at [87].

77 With peer-2-peer file sharing, TPB jointly with their users provided access to unauthorised copies of works in a peer-2-peer network. The operators intervened by making available the platform that indexed and provided a search engine for the torrents leading to illegal works, thus playing an essential role in the file-sharing.[210] They also "indexe[d] torrent files in such a way that the works to which the torrent files refer may be easily located and downloaded by the users of that sharing platform "with the goal of aiding users to find the files". [211] This way the administrators controlled access to the illegal copies of works on the network as they provided the technical structures to access them and checked "to ensure that a work has been placed in the appropriate category. In addition, those operators delete obsolete or faulty torrent files and actively filter some content".[212] When the operators delete obsolete or faulty torrents, they personally exercised content control over the uploaded torrent files. These aspects also contributed towards identifying the *mens rea* to give access to illegal copies of works. The operators must have acquired some specific knowledge from personally curating the categories and from being involved in the deletion of files.

78 Considering CJEU case law on a joint act of CTTP, the activities of hosting platforms such as YouTube that provide the technical conditions for users to upload and share licenced and unlicensed content by indexing, providing a search engine, automatically categorising contents, and providing recommendations but without the platform operators exercising choice over the copyrighted content uploaded and made available, do not amount to a copyright-relevant intervention in the communication. The platforms do not match the level of intervention achieved on a joint CTTP. In *Airfield*, the operators exercised choice over what content was supplied. In *TPB,* in addition to the provision of the platforms, the operators were personally involved in curating the files. When hosting platforms provide an automatic upload process, "and without material being seen in advance or controlled by the operator",[213] the intervention is technical and does not involve decision-making by the operators over the individual uploaded content. In the case of YouTube, the classification of uploaded videos is done automatically based on the information provided by the user. Video recommendations are made via an algorithm using machine learning and recommendations are provided on objective factors which do not include considerations over the legal nature of the content.[214] The operators are not personally involved with curation of the uploaded content and therefore do not intervene within the meaning of existing case law.

79 In the case of cyberlockers such as Cyando, a hyperlink is issued automatically to a user when that user uploads content. In this case, the control over the access to the work is exercised by the platform user who decides to make the link issued to her public to other users on designated link sites. The intervention in full knowledge may be attributed to the internet user who uploads content and manually shares the hyperlink with third parties. Consequently, the providers of cyberlockers may also not be placed under the presumption of knowledge and require conducting the "necessary checks". [215]

II. Operators of hosting platforms may lack the requisite knowledge that they provide access to illegal content of works

80 In *Filmspeler* and *TPB,* the providers acted with intention to give access to illegal content and boasted about the infringing purpose of their services. The standard of intention is also in line with the standard embraced by the Grand Chamber of the CJEU in *Reha Training* at this point of the CTTP analysis.[216] With hosting platforms such as YouTube, the use of automatic processes and lack of involvement of operators leads to the conclusion that the operators only have general knowledge that copyright infringing content is hosted and shared on the platform. Hosting providers' operators do not act with intention to give access to illegal content

81 Should anything less than the intention to give access to illegal copies be acceptable, then the CJEU will have to clarify which knowledge standard is applicable. AG Szpunar, in *TPB*, advised against the

210 *Ziggo* EU:C:2017:456 [2017] Bus LR 1899; [2017] 6 WLUK 237 at [36]-[37].

211 Ibid at [38].

212 Ibid at [36].

213 *YouTube* (C-682/18) Summary of the request for a preliminary ruling, question 1.

214 P. Covington, J. Adams, and E. Sargin, "Deep Neural Networks for YouTube Recommendations" (Proceedings of the 10th ACM Conference on Recommender Systems, 2016) <http://static.googleusercontent.com/media/research.google.com/en//pubs/archive/45530.pdf> accessed 18 September 2020;

215 See also João Pedro Quintais, "Untangling the hyperlinking web: In search of the online right of CTTP" (2018) 21 The Journal of World Intellectual Property 385, 410.

216 *Reha Training* ECLI:EU:C:2016:379 [2016] 3 CMLR 40 at [48].

application of a presumption of knowledge to peer-2-peer indexing platforms as this may lead to a general obligation to monitor indexed content.[217] The same argument was extended by AG Saugmandsgaard Øe in *YouTube/Cyando*.[218] Although not binding on the CJEU, at the national level the liability of hosting platforms based on general knowledge of infringement has been rejected.[219] In this case, a standard of specific knowledge may be more appropriate and potentially in line with one of the CJEU knowledge inferences in the *TPB* decision. This could be coupled with a standard of actual knowledge acquired following a notification from the rightsholder. If the platform does not take down the content in question, it may be seen to have intended to facilitate access to it by omitting to remove it.

82 Rightsholders may argue that Alternative 3 does not deliver the high level of protection required by Recitals 9 and 10 InfoSoc and does not help the purposes of the Digital Single Market. However, they are not left empty-handed. Rightsholders can also apply for injunctions against hosting platforms under Article 8(3) InfoSoc and the third sentence of Article 11 Directive 2004/48 (the Enforcement Directive). In particular, hosting platforms may be held to certain obligations concerning infringing content along the lines of the measures discussed under the duty of care approach discussed in Alternative 1.[220] Rightsholders may also apply under their right to information in Article 8(2)(a) of the Intellectual Property Enforcement Directive (2004/48)[221] to request information from hosting platforms regarding the identity of platform users who infringe.[222] Unharmonised forms of secondary liability or equivalent may also be available at the national level.

F. Conclusions

83 The question of whether hosting platforms that provide the technical tools for users to upload infringing material amounts to a relevant use by the platforms under Article 3(1) may be answered in several ways. This article opposes a broad application of the CTTP test to hosting providers based on strict liability. In this case, the sledgehammer of liability for damages may have longstanding implications for technological innovation in the area. Ultimately, only the big providers would be able to pay the damages and ensuing licence, therefore entrenching pre-existing dominant positions in the area. Internet users would also miss out on opportunities to engage in online information exchanges.

84 The solutions proposed in this article analyse three interpretations of the communication right in Article 3(1), which would achieve a nuanced outcome more in line with the fair balance objectives of Recital 31 InfoSoc. The duty of care approach in Alternative 1 provides a solution based on a conditional liability for hosting platforms. This way hosting platforms that oblige are saved from paying damages. The flip side is that a regulatory regime based on duties of care moves copyright away from its property rights status and closer to torts such as unlawful completion. Considering the dynamic evolution of the internet and the flexible nature of the CTTP elements as developed in case law, it is possible to envisage other possibilities. Alternative 2 considers but ultimately dismisses a solution to hosting provider liability based on Recital 27. Instead, Alternative 3 clarifies that in some situations hosting platforms do not perform an act of CTTP as they may not be engaging in an "intervention in full knowledge of the consequences to give access to illegal copies" element of the test. This means that some hosting platforms may not perform a copyright relevant act of "communication" to the public.

85 The direct infringement copyright claims against hosting platforms come at a time when technology has come of age and is no longer seen as deserving of special protection. The eyes of the world are on the EU and the overall resolution achieved in the case of hosting platforms. Other jurisdictions are seeking to address the legal status of such online platforms.

217 Advocate General Szpunar, *Ziggo* EU:C:2017:456 [2017] Bus LR 1899 at [52].

218 AG Henrick Saugmandsgaard Øe in *YouTube/Cyando* EU:C:2020:586 at [115].

219 See for example, *YouTube* (29 U 2798/15) Higher Regional Court of München at [53].

220 *YouTube* (C-682/18) Summary of the request for a preliminary ruling at [21]-[23].

221 Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004).

222 Most recently see *Constantin Film Verleih GmbH v YouTube LLC and Google Inc.* (C-264/19) EU:C:2020:261 finding that the term "addresses" in Article 8(2) Directive 2004/48 should be given its usual meaning, i.e. postal address, but member states may have the option for fuller information if a fair balance is struck between the fundamental rights involved and is in line with the principle of proportionality.

Across the Atlantic, the US is contemplating such a review and the Copyright Office's Section 512 Digital Millennium Copyright Act study recommends that the US should wait and learn from developments in the EU.[223]

86 The ideas discussed in this paper may also be relevant for a future UK approach to hosting-platform liability for infringing content after Brexit, as the UK is moving away from the EU and will not implement the DSMD:

> *"We shall see how the copyright directive is implemented and how the various enforcement regimes within it will work, but of course it is not possible for us to remain part of it, because we will not accept the jurisdiction of the CJEU in these matters".*[224]

87 A void may appear in the regulation of hosting platforms in the UK, and it remains to be seen to what extent the UK may take inspiration from its (former) European brethren.

223 United States Copyright Office, Section 512 of Title 17: A Report on the Register of Copyrights. (May 2020) <https://www.copyright.gov/policy/section512/section-512-full-report.pdf> accessed 22 May 2020.

224 "Copyright directive and Brexit" (After Brexit, Tech policy throughout the Brexit process 08 July 2020) <https://afterbrexit.tech/digital-single-market/copyright-directive/> accessed 09 July 2020.

Navigating The Fragmented Online Music Licensing Landscape In Europe

A Legislative Compass In Sight?

by **Lucius Klobučník***

Abstract: Online exploitation of musical works allows consumers in the European Union (EU) to enjoy tens of millions of musical works from a place and at a time of their choice. While the Title III of the EU Collective Rights Management (CRM) Directive contributed to re-shaping the EU multi-territorial online music licensing market, it did not adequately facilitate licensing for online use of musical works on a multi-territorial level in the EU. This article seeks to answer the question as to which legislative measures should be introduced to facilitate licensing practices and to lower transaction costs in order to enable market entry of new online music services in Europe. In order to answer this question, this article analyses relevant provisions of the Title III of the CRM Directive and problematic aspects of their application to different licensors. Furthermore, legislative and soft law documents on the EU level as well as cooperation initiatives among CMOs are evaluated in order to assess whether past initiatives can be considered by the EU legislator. Finding answers to these questions seems relevant in the light of possible re-evaluation of multi-territorial licensing practices on the legislative level in April 2021, as foreseen by the CRM Directive.

Keywords: online music licensing entities; review of Collective Rights Management Directive; repertoire fragmentation; withdrawal right; online music services

Recommended citation: Lucius Klobučník, Navigating the Fragmented Online Music Licensing Landscape in Europe - A Legislative Compass in Sight?, 11 (2020) JIPITEC 340 para 1.

A. Introduction

1 Part B seeks to analyse the legislative and market-driven initiatives to facilitate online music licensing in the EU. It concludes that territorial rights fragmentation merely turned into repertoire-based fragmentation and did not sufficiently facilitate licensing process for online music services. Part C provides an overview of online music licensing entities in the EU and their licensing practices in order to identify regulatory gaps and to illustrate licensing complexities online music services face. Part D points out that several benefits of offline licensing for users were lost in the online licensing market. It criticises the CRM Directive for not providing sufficient measures for balancing stakeholder interests with regard to online licensing. Finally, the 'Conclusion' part provides recommendations for the EU legislator to facilitate the licensing process and to mitigate the impact of repertoire fragmentation on online music services. These measures should ultimately lead to the emergence of new online music services in the EU and thus a greater variety and more choice for European music consumers.

2 The focus of the article is limited to the EU and to the market of online music licensing of musical works. Neither EU Member States' national online music licensing practices nor multi-territorial licensing of other than musical works is addressed.

* Early Stage Researcher, PhD Candidate, Intellectual Property Law, EIPIN Innovation Society, Queen Mary University of London.

B. Transformed Online Music Licensing Market

I. New services demanding new licensing schemes

3 Technological developments coupled with changed consumer behaviour have sparked the need for new services providing online access to musical works. The end of the 20th and the first years of the 21st century have witnessed the rise of online sharing of musical works in the form of digital downloads. However, due to increased consumer demand and technological advances (particularly the availability of high-speed Internet), these services were in a few years succeeded by streaming services offering tens of millions of musical works[1] and operating on an EU-wide or worldwide level. These services have brought considerable benefits to consumers, who are able to enjoy tens of millions of musical works from a place and at a time of their choice. The existing music licensing schemes, applicable to offline exploitation of musical works and based on territorial limitations, proved unfit for these services which would have to obtain a licence in every single EU Member State in order to operate in Europe. These services started demanding a reform of the music licensing market, which would not be based on territorial restrictions and which would facilitate the licensing process and market access.

4 Although exploitation of musical works occurs in a borderless market, licensing has for a long time been confined to national borders. Efforts to reform the licensing process for multi-territorial use of musical works in the EU stemmed from both legislative and market-driven initiatives. However, online music services (particularly streaming services) offering access to musical works Europe-wide, still face a burdensome licensing process due to a fragmented online music licensing market (involving a necessity to obtain a licence from several licensors) connected with high transaction costs. These factors ultimately prevent new online music services from entering the market and from offering greater versatility of music services to consumers. Based on a study conducted before the CRM Directive entered into force[2], it can be inferred that transaction costs of music licensing are sufficiently high as to deter start-up online music services to enter the market.[3] It is noteworthy that five of the largest companies in the subscription-based online music services market (Spotify, Apple Music, Amazon, Tencent and YouTube) hold nearly 85% of the worldwide market share.[4] All these services can be considered as "all-in" or "over-the-top" mainstream providers, each offering roughly the same large catalogues and feature sets. Niche services, offering access to limited genres of works, are virtually non-existent[5]. This might be due to consumers' attitude – unlike with audio-visual content subscriptions, when it comes to music, most subscribers opt for just one service. However, another reason for a lack of niche online music services is that rights clearance and maintenance costs for such a service are disproportionately high for their income.[6] The CRM Directive aimed at facilitating the EU-wide licensing process for online music services and at reducing the number of licences a user needs to operate a multi-territory multi-repertoire service.[7] The CRM Directive leaves these tasks to the market, by giving preference to voluntary repertoire aggregation. The Impact Assessment, preceding the CRM Directive, implies that multi-territorial online music licensing solutions should be driven by market forces and build on the current level of market aggregation and market trends.[8] The CRM Directive further assumes that "[voluntary] aggregation of

1 'Apple Music vs. Spotify | Which Service Is the Streaming King? | Digital Trends' <https://www.digitaltrends.com/music/apple-music-vs-spotify/> accessed 25 September 2020.

2 Vrije Universiteit Brussel KEA European Affairs, 'Licensing Music Works and Transaction Costs in Europe', September 2012.

3 Towse, Ruth, Economics of Copyright Collecting Societies and Digital Rights: Is There a Case for a Centralised Digital Copyright Exchange? (December 12, 2012). Review of Economic Research on Copyright Issues, 2012, 9(2), 3-30, Available at SSRN: https://ssrn.com/abstract=2216165.

4 Statista, 'Share of Music Streaming Subscribers Worldwide, by Company' <https://www.statista.com/statistics/653926/music-streaming-service-subscriber-share/>.

5 DJ-oriented music service Beatport or classical-music focused Primephonic are some rare examples of niche services.

6 Camilla Kling, *Gebietsübergreifende Vergabe von Online-Rechten an Musikwerken: Probleme einer effizienten Lizenzierungspraxis unter Geltung des VGG* (Walter de Gruyter GmbH & Co KG 2017) 26.

7 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, OJ L 84/72 Recital 40.

8 European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the Document Proposal for a Directive 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' 162.

repertoires should facilitate the development of new online services and should result in a reduction of transaction costs being passed on to consumers".[9] However, the CRM Directive does not reflect on online music services' preferences. Neither do market developments sufficiently respond to their needs – they lead to the creation of new licensing entities, thus questioning the CRM Directive's goal of reducing the number of licences and lowering transaction costs. The upcoming review of the CRM Directive in Spring 2021 provides an opportunity to balance the interest of stakeholders in the multi-territorial online music licensing market.

II. From territorial to repertoire-based fragmentation

1. Soft-law measures to prevent territorial fragmentation and improve online licensing

5 Responses to these demands have comprised a form of top-down as well as bottom-up initiatives. When it comes to the former, the European Commission initially adopted a soft-law approach. Already in 1995, when online music services were still in inception, the EU Commission's Green Paper (referring to a Green Paper from 1988[10]) recognized that new technologies have entailed the *de facto* abolition of national frontiers and make territorial application of copyright law obsolete[11]. After the turn of the century, the EU Commission and the EU Parliament have published several soft law documents (recommendations, studies) emphasising the necessity to reform the collective rights management framework (especially regarding transparency of collective management organisations – CMOs) and issuance of multi-territorial licences[12]. These initiatives aimed at reforming licensing practices rather than substantive copyright law. The most impactful and the most controversial soft law document was the so-called Online Music Recommendation 2005[13] (Recommendation 2005), which emphasised the right of rightholders to withdraw their online rights[14] from CMOs and entrust a CMO in other EU Member States with administration and licensing of online rights, while at the same time being able to determine the territorial scope of licences. Despite its non-binding nature, the Recommendation 2005 led to sweeping changes in the online music licensing market, since major Anglo-American publishers withdrew their mechanical online rights from the system of reciprocal representation agreements (RRAs) and resorted to direct licensing or entrusted their online rights to other licensing entities. The Recommendation 2005 changed the traditional structure of international rights management forever. Prior to that, major Anglo-American publishers operated through a network of sub-publishers, who were members of national CMOs in Europe. However, the Recommendation 2005 effectively removed the need for a sub-publisher network, allowing major publishers to become direct members of any CMO in Europe and authorise that CMO to provide multi-territorial licences for their repertoire. It should be noted that the right to withdraw rights from CMOs had existed prior to the Recommendation 2005 in several EU Member States and had been confirmed by the European Commission *Daft Punk* case, where rightholders demanded withdrawal of online rights while keeping other (offline) rights under the CMO's control[15]. The Recommendation 2005 thus only confirmed the existing legal status quo regarding rights' withdrawals. However, it also led to the establishment of new licensing entities different

9 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, OJ L 84/72 Recital 44.

10 Commission of the European Communities, "Green Paper on Copyright and the Challenge of Technology – Copyright Issues Requiring Immediate Action", COM (88), 172.

11 Commission of the European Communities, 'Green Paper Copyright and Related Rights in the Information Society COM (95) 382 Final' Art 29.

12 European Parliament, European Parliament Resolution on a Community Framework for Collective Management Societies in the Field of Copyright and Neighbouring Rights (2002/2274(INI)); European Commission, Study on a Community Initiative on the Cross-Border Collective Management of Copyright.

13 European Commission, 'European Commission Recommendation of 18 October 2005 on Collective Cross-Border Management of Copyright and Related Rights for Legitimate Online Music Services (2005/737/EC), OJ L 276/54'.

14 Pursuant to Article 1 (f) of Recommendation 2005, online rights include the right of reproduction, right of communication to the public and right of making available. This understanding is in line with the Directive 2001/29/EU (InfoSoc) and Directive 2014/26/EU (CRM Directive).

15 *Commission Decision of 06. 08. 2002 in case COMP/C2/37219 Banghalter / Homem Christo (Daft Punk) v SACEM.*

from CMOs[16]. The European Parliament heavily criticised the Recommendation 2005 in its Report[17]. Although it did not dispute the right to withdraw online rights, it criticised the EU Commission for not consulting the EU Parliament and called for a legislative action which would *inter alia* harmonise rules governing activities of CMOs in the EU.

2. (Unintended) proliferation of individual licensing

6 The Recommendation 2005 had an objective to facilitate online music licensing. It has, however, made it even more complex by introducing an extra layer of intermediaries.[18] Recommendation 2005 resulted in the establishment of new licensing entities, through which rightholders license and administer their rights individually. It can be questioned whether the Recommendation 2005's goal was to promote individual licensing and to weaken collective licensing. The Recommendation 2005 contains only a brief reference to individual rights management, when it states that online rights may be managed by collective rights managers or by individual rightholders themselves[19]. Although the Recommendation 2005 aims at abolishing reciprocal representation agreements in online music licensing, it still seems to prefer collective licensing over individual licensing. This is clear particularly from Article 5 of the Recommendation 2005 which provides that "rightholders should be able to determine the online rights to be entrusted for collective management...to determine the territorial scope of the mandate of collective managers" and "to withdraw any of the online rights and transfer the multi-territorial management of those rights to *another* collective rights manager"[20]. The same can be observed in the stakeholder consultation, conducted shortly before the publication of the Recommendation 2005[21]. The consultation concluded that the so-called 'option 3' offers the most effective long-term model for cross-border licensing of copyright-protected content in the online environment. Option-3 was to 'give rightholders the choice to authorise one single CMO to license and monitor all the different uses made of their works across the entire EU'. The EU Commission also assumed that rightholders would conclude agreements directly with a CMO of their choice and transfer the mandate to license and administer their rights to a single rights' manager of their choice.[22] The Recommendation 2005 envisaged multi-territorial licensing by a single CMO rather than by an individual licensor[23]. As was confirmed 10 years after the Recommendation 2005's publication, major Anglo-American music publishers (referred to also as 'option-3-publishers') withdrew mechanical rights related to their repertoire from CMOs and license these rights directly to users. They only rely on CMOs for administrative services.[24] Proliferation of individual licensing might have been an unintended consequence of the Recommendation 2005.

16 As is shown in chapter 2 of this paper.

17 European Parliament and Rapporteur: Katarin Lévai, 'Report on the Commission Recommendation of 18 October 2005 on Collective Cross-Border Management of Copyright and Related Rights for Legitimate Online Music Services (2005/737/EC) (2006/2008(INI))' <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A6-2007-0053&language=EN#title2>.

18 Emilie Anthonis, 'Will the CRM-Directive Succeed in Re-Aggregating the Mechanical Reproduction Rights in the Anglo-American Music Repertoire?' (2014) International Journal of Intellectual Property Management 7 151, 151.

19 European Commission, 'European Commission Recommendation of 18 October 2005 on Collective Cross-Border Management of Copyright and Related Rights for Legitimate Online Music Services (2005/737/EC), OJ L 276/ 54' (n 14) Recital 6.

20 ibid Art. 5 a), b0, c).

21 European Commission, 'Frequently Asked Questions on Central Copyright Clearance for Online Use across the EU, MEMO/05/241, 7 July 2005' <https://ec.europa.eu/commission/presscorner/detail/de/MEMO_05_241>.

22 ibid 3.

23 Emanuela Arezzo, 'Competition and Intellectual Property Protection in the Market for the Provision of Multi-Territorial Licensing of Online Rights in Musical Works – Lights and Shadows of the New European Directive 2014/26/EU' [2015] Max Planck Institute for Innovation and Competition 534; Sebastian Felix Schwemer, *Licensing and Access to Content in the European Union: Regulation between Copyright and Competition Law* (Cambridge University Press 2019) 156; Anthonis (n 18); Bob Kohn, *Kohn on Music Licensing* (5th edn, Wolters Kluwer 2018) 202, 203.

24 European Commission, 'Press Release - Mergers: Commission Approves Joint Venture for Cross-Border Licensing of Online Music between PRSfM, STIM and GEMA, Subject to Commitments Brussels, 16 June 2015' 1.

3. Licensing passport as a facilitation of online music licensing in the CRM Directive

7 Title III the CRM Directive drew up a specific legal regime applicable only to multi-territorial licensing of online rights in musical works[25]. It determined that not every national CMO will be able to issue multi-territorial licences for the use of musical works, only those complying with several conditions set out in Title III – those having the ability to accurately identify musical works; to identify rightholders and rights to (shares of) musical works with respect to relevant territories; to use unique identifiers and to resolve inconsistencies in data[26]. This set of conditions is referred to as the 'European licensing passport', although the notion of 'passport' only appears in documents leading to the adoption of the CRM Directive, including the Proposal for the CRM Directive[27]; it is not present in the Directive itself. The CRM Directive foresees that not every single European CMO will be able to meet these criteria and introduces the so-called "tag-on regime" under which CMOs which do not grant or offer to grant multi-territorial licences for the online rights in musical works in its own repertoire can request another European CMO to represent these rights. The requested CMO is under a "must carry" obligation, i.e. it cannot refuse such a request, however, only if it is granting multi-territorial licences for the same category of rights for another CMO. It is clarified in Recital 46 of the CRM Directive that this representation agreement does not extend to CMOs that provide multi-territorial licences only for their own repertoire. All CMOs could theoretically comply with the provisions of Title III, just by offering their own repertoire on a multi-territorial basis.

25 Which means this regime does not apply to mono-repertoire licensing, offline licensing (whether multi- or mono-territorial) and licensing of works other than musical works.

26 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, OJ L 84/72 Art. 24 (2).

27 European Commission, 'Proposal for a Directive 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 COM/2012/0372 Final - 2012/0180 (COD)'.

4. CMO-driven efforts to prevent territorial fragmentation

8 Attempts to reform online music licensing in order to provide multi-territorial licences came also from CMOs. CMOs drafted 2 agreements which would establish a so-called "one-stop shop" for online music services seeking one licence covering multiple territories (multi-territorial multi-repertoire licence). The first agreement, Santiago Agreement, concerns the right to making available rights (public performance rights) in musical works. The second agreement, BIEM agreement concerns reproduction rights (mechanical rights)[28]. Both the Santiago and BIEM Agreements contained a clause providing that CMO with authority to grant a multi – territorial multi – repertoire licence is the CMO of the country where the service provider (user) has its actual and economic location[29] or where the user is incorporated or uses the URL (uniform resource locator) of that country[30]. Although this "economic residence" (or "customer – allocation") clause was received very well by European CMOs[31], the EU Commission's view was not favourable. The Commission argued that the economic residency clause restricts competition pursuant to article 101 (1) c) TFEU since each national CMO is given absolute exclusivity to grant a multi – territorial multi – repertoire licence in its territory[32]. Although the parties to the Santiago and BIEM Agreements were invited by the European Commission to exclude the economic residence clause, they were not willing to do so. Thus, neither of the agreements ever materialised. It has to be noted that a similar agreement – IFPI Simulcasting Agreement - was entered into among

28 As explained above, "online rights" include both public performance and mechanical rights;

29 European Commission, 'Notice Published Pursuant to Article 27(4) of Council Regulation (EC) No 1/2003 in Cases COMP/ C2/39152 — BUMA and COMP/C2/39151 SABAM (Santiago Agreement — COMP/C2/38126)' (n 19) (2004) para 6.

30 'Notification of Cooperation Agreements (Case COMP/C-2/38.377 — BIEM Barcelona Agreements) (2002/C 132/10).

31 Giuseppe Mazziotti, 'New Licensing Models for Online Music Services in the European Union: From Collective To Customized Management' 34 Columbia Journal of Law & the Arts 757, 763.

32 European Commission, 'Notice Published Pursuant to Article 27(4) of Council Regulation (EC) No 1/2003 in Cases COMP/ C2/39152 — BUMA and COMP/C2/39151 SABAM (Santiago Agreement — COMP/C2/38126)' (n 30) para 6.

CMO members of the IFPI[33] with regard to record producers' rights (neighbouring rights). While this agreement had originally also included an economic residency clause[34], it was removed after the EU Commission's request. However, despite the IFPI Simulcasting Agreement receiving exemption from the EU Commission and entering into force in 2003, the participating CMOs did not extend its duration beyond the 31st December 2004. It can be speculated that CMOs did not wish to provide multi-territorial licences under the "reviewed" conditions by the EU Commission. The EU Commission did not oppose solutions aimed at improving licensing[35] *per se* but only particular provisions in these agreements.

III. Impact of the reformed licensing landscape on online music services

1. Voluntary aggregation of repertoire and a broad withdrawal right of the CRM Directive

9 In light of the withdrawn online mechanical rights to the Anglo-American repertoire of major publishers, the European legislator had to make a choice between introducing mandatory or voluntary re-aggregation of rights. A distinction must be made between the re-aggregation of mechanical rights that have been withdrawn from collective management after the Recommendation 2005 and aggregation of repertoire of different CMOs. The CRM Directive does not focus on compulsory repertoire aggregation but sets incentives for voluntary aggregation by way of the abovementioned European licensing passport model. The Commission considered that the passport model would encourage the aggregation of repertoire for online use of musical works at the EU level as well as licensing of rights through effective and responsive multi-territory infrastructure. In the EU Commission's view, the passport model would build upon the current level of aggregation and market trends[36]. Although the CRM Directive seems to seek the aggregation of repertoire from different CMOs in passport entities, the Commission seemed to have anticipated that the re-aggregation of the withdrawn mechanical rights would be an indirect consequence of better regulation on governance and transparency of CMOs.[37] The EU Commission seemed to believe that higher standards for passport entities might actually motivate major music publishers to bring back their mechanical rights to collective management.[38] The practice for granting mono-repertoire licences for multi-territorial use of music online is beneficial for publishers that can now set the prices for the licences by themselves and seem to be able to extract more value from their rights than under collective management.[39]

10 One of the main CRM Directive's measures to encourage aggregation of repertoire is by a broad withdrawal right of rightholders. Art. 5 (2) of the CRM Directive gives rightholders the right to authorise a CMO of their choice to manage the rights, categories of rights or types of works or other subject matter of their choice, for the territories of their choice, irrespective of the Member State of nationality, residence or establishment of either the CMO or the right holder.[40] This article reflects the principles from the Recommendation 2005 and makes them binding. However, the withdrawal right in the CRM Directive is even broader, because it does not only apply to online rights necessary to operate legitimate online music services but to rights and rightholders in the

33 International Federation of Phonograhpic Producers is a not-for-profit international trade association registered in Switzerland whose members comprise over 1300 music and video producers: <http://www.ifpi.org/about.php>, accessed 12. 02. 2020.

34 *Case No COMP/C2/38014 — IFPI 'Simulcasting* [2003] European Commission COMP/C2/38.014.

35 Intellectual Property Office of the United Kingdom, 'Music 2025: The Music Data Dilemma: Issues Facing the Music Industry in Improving Data Management' 164, 30.

36 Some CMOs entrusted their rights to other CMOs for the purpose of multi-territorial licensing of online services. For instance, the Irish CMO IMRO chose the British PRS and the Portuguese CMO SPA chose the Spanish CMO SGAE to license their rights on a multi-territory basis. Also, CMO hubs, such as Armonia and ICE started their collaboration before the CRM Directive's adoption (as shown below).

37 Anthonis (n 18) 158.

38 European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the Document Proposal for a Directive 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' (n 9) 28.

39 Anthonis (n 18) 160.

40 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, OJ L 84/72 Art. 5 (2).

broadest sense.[41] Art. 5 (6) provides that rigthholders should not be restricted to entrust withdrawn rights to another CMO.[42] Another initiative in support of voluntary aggregation is reflected in Article 31 of the CRM Directive. Rightholders can withdraw their online rights in musical works from a CMO, if this CMO does not itself offer multi-territorial licences or does not use the tag-on regime. Subsequently, rightholders can grant multi-territorial licences for their online rights in musical works themselves or through any other party or CMO complying with the Title III.[43] According to the withdrawal right in Article 5, rightholders would in any case have a right to authorise a CMO of their choice. Article 31 refers to a specific situation in which a rightholder is able to withdraw relevant online rights for the purpose of multi-territorial licensing, while keeping the same rights for mono-territorial licensing in the CMO. However, this seems to be confirmed in Art. 5 and in the *Daft Punk* case.[44] Perhaps the only novelty of Art. 31 is that it expressly refers to the possibility of individual rights' management - Art. 5 of the CRM Directive and the Recommendation 2005 only include an implicit reference to individual rights' management.[45] It is noteworthy though, that Recital 19 (2) of the CRM Directive does provide for individual management. Only when a Member State provides for mandatory collective management, rightholder's choice would be limited to other CMOs.[46] This provision might be important in countries with mandatory collective management for online music rights.[47] Another reading of Art. 31 could be that rightholders have a right to withdraw online rights or categories of online rights for multi-territorial licensing, even if such an online right is neither determined in a Member State's law nor recognised in a CMO's internal regulations.

41 Emanuela Arezzo (n 23) 540.

42 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, OJ L 84/72 Art. 5 (6).

43 ibid Art. 31.

44 *Commission Decision of 06.08.2002 in case COMP/C2/37.219 Banghalter / Homem Christo (Daft Punk) v SACEM* (n 16).

45 Emanuela Arezzo (n 23) 543.

46 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, OJ L 84/72 Recital 2 (2).

47 Schwemer (n 23) 156.

11 Individual rights' management might be beneficial for rightholders but might become more burdensome for users. From a user perspective, a fully individualised management is most likely to create prohibitive transaction costs.[48] The more rightholders withdraw their rights from CMOs and opt for individual licensing, the more licences online music services will have to clear.

2. Lowering the Number of Licensors?

12 It has been reported that the current European market for online music services lacks versatility[49] and services present in the market struggle to be profitable[50]. The CRM Directive pursues the goal of repertoire aggregation for the purpose of pan-European licensing by reducing the number of CMOs that online music services have to contact in order to clear authors' rights from 27 (equal to the number of Member States) to perhaps between three and ten[51]. However, in addition to CMOs, online music services will have to clear authors' rights for the Anglo-American repertoire of major publishers. Legislative and CMO-driven initiatives provided only very partial answers to problems of online music services seeking EU-wide rights clearance. Although the CRM Directive[52] as well as the Impact

48 Emanuela Arezzo (n 23) 545.

49 Mark Savage, 'Music Streaming Market "Needs More Choice"' *BBC News* (20 November 2019) <https://www.bbc.com/news/entertainment-arts-50472906> accessed 12 December 2019.

50 Johanna Nicholson, 'If Spotify Is so Huge, Why Is It Losing Money?' (*ABC News*, 6 September 2017) <http://www.abc.net.au/news/2017-09-06/digital-music-streaming-rising-but-spotify-losing-money/8875188> accessed 17 September 2020; Anna Nicolaou, 'Spotify Looks beyond Music in Search of a Profit' <https://www.ft.com/content/7f689608-4471-11ea-a43a-c4b328d9061c> accessed 12 September 2020; 'The French Music Streaming Service Taking on Spotify, Apple and Amazon' (*The Independent*, 20 September 2017) <http://www.independent.co.uk/news/business/analysis-and-features/deezer-music-streaming-spotify-amazon-apple-subscritpiton-hans-holger-albrecht-len-blavatnik-a7940896.html> accessed 12 September 2020.

51 Nikita Malevanny, *Online Music Distribution - How Much Exclusivity Is Needed?*, vol 12 (2019) 205.

52 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, OJ L 84/72 Recital 40.

Assessment[53] aim to 'substantially lower' the number of licences for multi-territorial online music services and simplify the licensing process, this goal has not been achieved. Developments in the licensing market show contrary results – the number of licences required has not been lowered and online music services are faced with a higher legal uncertainty[54]. The current developments run counter to the regulatory goal of a reasonable number of licensors.[55] Major publishers have not brought their mechanical rights back to collective management and it seems unlikely that it will happen as a result of the CRM Directive.[56]

13 The recent legislative and CMO-driven changes in the European online music licensing market turned territorial fragmentation into repertoire-based fragmentation. Recent legislative changes were prevalently rightholder-oriented and omitted interests of online music services. The most attractive features of collective management from the users' point of view – blanket licences and tariffs – providing legal security to users regarding the cost of the use of works belonging to the repertoire, were not addressed by the CRM Directive[57].

53 European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the Document Proposal for a Directive 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' (n 9) 162.

54 Jörn Radloff and others, 'Das Rechtsverhältnis Der GEMA Zu Den Nutzern - Lizenzierung' in Harald Heker and Karl Riesenhuber (eds), *Recht und Praxis der GEMA: Handbuch und Kommentar*, vol 3 (2018) 756; Bernd Justin Jütte, *Reconstructing European Copyright Law for the Digital Single Market*, vol 10 (Hart Publishing 2017) 482; R Kerremans, K Janssen and P Valcke, 'Collective Solutions for Cultural Collections Online: Search and Select!' (2011) 6 Journal of Intellectual Property Law & Practice 638, 643; Bob Kohn (n 24) 840; João Pedro Quintais, 'Empire Strikes Back: CISAC Beats Commission in General Court' (2013) 8 Journal of Intellectual Law and Practice 680, 682.

55 Schwemer (n 23) 157.

56 Anthonis (n 18) 160.

57 Sylvie Nérisson, 'Remaining Scope for Collective Management of Copyright in the Online World', *Remuneration of Copyright Owners - Regulatory Challenges of New Business Models*, vol 27 (Springer-Verlag GmbH 2017) 75; Romana Matanovac Vučković, 'The Role of Collective Management Organisations in New Business Models - Challenges for the Legislature and Courts', *Remuneration for the Use of Works, Exclusivity vs Other Approaches* (Walter de Gruyter GmbH 2015) 416.

C. Various Groups Of Licensing Entities

I. Classification of new online licensing models

14 The abovementioned changes in the music licensing market led to the clear separation of a multi-territorial online music licensing market from other music licensing markets, such as licensing for offline use or mono-territorial licensing for online use. These changes also caused a rise in the number of licensing entities in this market. Online music services have to interact not only with national CMOs (those complying with the passport conditions of the CRM Directive), but also with other licensing entities. Online licensing entities can be classified based on who takes the leading role – whether national CMOs or publishers[58]. After the CRM Directive adoption, a third category – independent management entities – can be added to the equation. Online licensing entities can also be grouped together based on other criteria, such as the level of institutionalisation[59] and whether they issue or merely facilitate licences. For clarity reasons, this article refers to the first division.

II. Licensing hubs run by CMOs

15 Licensing hubs resulted from cooperation between national CMOs. Although such cooperation was foreseen by the CRM Directive, the history of these hubs predates the CRM Directive and results from the market development. Provision and subsequent administration of multi-territorial licences are connected to substantial technological challenges. Online exploitation of musical works, particularly by way of streaming generates vast amounts of music metadata, which must be received, administered and connected to information on rightholders by CMOs. Even the largest and best equipped CMOs face difficulties in coping with this challenge[60]. The CRM

58 Johann Heyde, *Die grenzüberschreitende Lizenzierung von Online-Musikrechten in Europa*, vol 54 (Nomos Verlagsgesellschaft 2011) 135.

59 Kling (n 6) 143.

60 '"Collecting Societies Are Struggling to Keep up with the Influx of Millions of Lines of Data."' (Music Business Worldwide, 13 May 2018) <https://www.musicbusinessworldwide.com/the-future-of-digital-performance-rights-management/> accessed 25 September 2020; 'Streaming Generates Vast Amounts of Royalty Data, and Not All Collecting Societies Are Coping | Complete Music Update' <https://completemusicupdate.com/article/

Directive applies to CMO hubs if they are owned and controlled by CMOs and carry out an activity of a CMO[61]. Currently, there are several CMO hubs in Europe. This article focuses on the two largest ones – International Copyright Enterprise (ICE) and Armonia Online. Although both of these initiatives have a common goal – to provide a one-stop-shop for online music services – they also exhibit significant differences.

16 International Copyright Enterprise (ICE) is a joint venture of three European CMOs – British PRS for Music, Swedish STIM and German GEMA. The roots of ICE can be traced back to 2008, when PRS and STIM created a common database of rights. GEMA joined the initiative in 2012, and in 2015 ICE started offering multi-territorial licences for the repertoire of the three CMOs.[62] Before ICE started offering its services, it had to notify the merger to the European Commission, since a threat existed that ICE would hold a monopoly to offer multi-territorial licences. The merger was however declared compatible with the internal market[63]. Offering front, middle and back office services, ICE consists of two separate limited liability companies, ZETA and DELTA. Back office administers a database of copyright protected works. The task of middle office is mainly to issue invoices and resolve invoice claim disputes. Front office deals with the negotiation and the conclusion of licensing deals as well as monitoring online usage and detecting unauthorised use. Front office issues the so-called "Zeta Core Licence", which is a multi-territorial transactional licence[64] present only in the online rights' market[65]. Online music services purchasing the Zeta Core Licence will automatically have access to the entire repertoire within the Zeta Core Licence and will not be able to licence only parts of the repertoire covered by it[66]. When it comes to licence negotiations, two scenarios are possible. In the first one, a third party (typically a CMO from outside ICE) agrees to its repertoire being licenced by ICE as part of the Zeta Core Licence. In the second one, ICE only provides support in negotiation of a licensing deal with an online music service and the third party CMO licenses its repertoire separately from the Zeta Core Licence[67]. In the case of the latter, online music services will have to enter into separate licences with different licensors but can benefit from the fact that a licence is negotiated in one place. ICE disposes of its own negotiation team, which is separate from CMOs forming ICE.

17 Armonia Online is currently an alliance of 9 national CMOs[68], a single point of contact representing 13 million musical works[69]. Although Armonia offers technology as well as a licensing structure to other CMOs[70] (and other licensing entities) it is different from ICE in several aspects. Firstly, while ICE consists of 2 limited liability companies, Armonia is not a separate legal entity. Secondly, ICE provides one unique licence, ZETA Core Licence to DSPs, which means that ICE licenses all mechanical and performing rights of GEMA, PRSfM, STIM and publishers which are members of ICE under one licence in its own name. Armonia has not developed its own licence and although it provides for a "single

streaming-generates-vast-amounts-of-royalty-data-and-not-all-collecting-societies-are-coping/> accessed 8 September 2020.

61 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, OJ L 84/72 Art 2 (3).

62 <https://www.iceservices.com/company/about/> accessed 15 September 2020.

63 *CASE M6800-PRSfM/ STIM/ GEMA/ JV, Merger Procedure Regulation, C(2015) 4061 final* (European Commission).

64 Transactional licences can be understood as licences under which royalties (licence fees) are calculated at work-share level based on reported music usage data, i.e. according to the actual usage of copyright-protected works (based on actual number of downloads/ streams of individual works), whereas under "blanket licences", the royalties are typically (although not necessarily) charged as a lump sum calculated on the actual or potential audience reached by a certain service. Under "transactional licences", the usage report provided by a user will be the basis for the calculation of royalties owed by the user (and thus the invoicing to the user). Under lump sum blanket licences that are priced on a lump sum basis, usage reports are not relevant for the invoicing to the licensee, but only for the distribution of the collected royalties to members and rightholders.

65 If online music services operate only in one EU Member State, they acquire a licence from a national CMO.

66 *CASE M.6800-PRSfM/ STIM/ GEMA/ JV, Merger Procedure Regulation, C(2015) 4061 final* (n 64) Para 19.

67 ibid para 41-44.

68 French SACEM, Spanish SGAE, Italian SIAE, Hungarian Artisius, Belgian SABAM, Swiss SUISA, Portuguese SPA and Austrian AKM.

69 'Armonia Online - Licensing musical works for digital services' (*Armonia Online*) <https://www.armoniaonline.com/> accessed 19 August 2020.

70 'Benefits' (*Armonia Online*) <https://www.armoniaonline.com/benefits/> accessed 19 August 2020.

agreement"[71], this does not necessarily mean that online music services enter only into one licensing agreement. As opposed to ICE, Armonia does not have its own negotiation team and licence negotiations are typically taken up by one of the CMOs forming Armonia (in most cases SACEM). Unlike ICE, which has a mandate for licensing, Armonia serves as a licence facilitator and can be viewed as a "single contact point", rather than a one-stop-shop.

III. Independent management entities

18 Independent management entities (IMEs) are new licensing entities introduced by the CRM Directive[72]. Recital 15 of the CRM Directive emphasises that rightholders should be free to entrust the management of their rights to IMEs. The main difference compared to CMOs is that IMEs are not owned or controlled by rightholders (their members) and are organised on a for profit basis. IMEs are subject to information duties and excluded from several provisions of the CRM Directive. Other regulatory questions, such as registration, oversight and transparency are left to Member States[73]. IMEs can potentially offer easy access, higher tariffs and quick royalty distribution to rightholders. On the other hand, rightholders will not be able to take part in IMEs' decision-making. So far, IMEs have not been proliferating in the online music licensing market. One of the biggest European IMEs, Soundreef, is registered in Italy, the United Kingdom, Spain and Czechia[74] and represents 39000 rightholders[75]. One of the reasons for such a scarce presence of IMEs in Europe might be connected to the legal hurdles that IMEs have to overcome. The Italian CMO SIAE was preventing its members from withdrawing rights and mandating Soundreef with rights administration. Subsequently, the Italian competition authority ruled in favour of Soundreef and labelled SIAE's behaviour as anti-competitive[76]. Other obstacles for IMEs might include difficulties with withdrawals of rights in different EU Member States (since disputes on withdrawals are brought before courts of the state of CMO's seat) and unclarities concerning membership in international CMO groupings.

IV. Mono-repertoire multi - territorial licensors

19 Mono-repertoire multi- territorial licensors were created as a reaction to Recommendation 2005 when major publishers of Anglo-American repertoires (Sony/EMI, Warner/Chappel, Universal Music Publishing and BMG) decided to withdraw online mechanical rights from national CMOs in Europe. These publishers, also referred to as "option-3-publishers"[77], set up their own licensing entities, connected to varying extent to national CMOs. These entities license mono-repertoire on multi-territorial basis.

20 The legal position and functioning of these entities raises several questions. Can these entities be considered CMOs and be subject to similar rules? This question was dealt with in Germany with regard to one of these entities, SOLAR, which is registered as a limited liability company (Gesellschaft mit beschränkter Haftung – GmbH) and owned by German and British CMOs GEMA and PRS for Music[78]. According to German law, this entity can be considered a "dependent management entity" and should thus be subject to the same rules as CMOs (although it is not clear whether this applies to all rules). However, this interpretation is limited only to Germany and only to licensing entities having an ownership link with CMOs. The CRM Directive has entirely repealed Article 31 of the of the CRM Directive Proposal, under the heading "Multi-territorial licensing by subsidiaries of collecting societies", which expressly held that the provisions contained in Title III (regarding multi-territorial

71 ibid.

72 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, OJ L 84/72 Art 3 (b).

73 Lucie Straková, 'Nové instituty kolektivní správy: nezávislý správce práv' (*Iurium*, 4 September 2020) <https://www.iurium.cz/2019/04/04/nove-instituty-kolektivni-spravy-nezavisly-spravce-prav/> accessed 10 September 2020.

74 Interestingly, there are 4 IMEs registered in Czechia: https://www.mkcr.cz/seznam-nezavislych-spravcu-prav-1640.html.

75 'About Us - Soundreef' <http://www.soundreef.com/en/about-us/> accessed 16 August 2020.

76 'Soundreef: Italian Antitrust Authority (AGCM) Rules in Favor of Songwriters' Rights.Pdf | Powered by Box' <https://soundreef.app.box.com/s/rnrrkca4f0rjcplqbwbb0rgkiy5n-7ljb> accessed 10 September 2020.

77 This name comes from a consultation issued by the European Commission, which included three options for improving online licensing. The third option included giving publishers a choice to appoint a single society to administer all the online uses of their musical works across the entire EU. The consultation is available at: https://europa.eu/rapid/press-release_MEMO-05-241_en.htm?locale=fr.

78 <http://www.celas.eu>.

licensing) applied to "entities owned, in whole or in part, by a collecting society and which offer or grant multi-territorial licences for online rights in musical works."[79] In favour of these entities being outside of the CRM Directive's application also speaks the fact that these entities represent only one rightholder. The CRM Directive clearly states that the CMO must represent more than one rightholder and that publishers cannot be considered CMOs[80]. They would thus not satisfy the condition of representing more than one rightholder to qualify as either a CMO or an IME.[81] The CRM Directive would apply to option-3 licensing entities, provided they are owned or controlled by a CMO and carry out an activity which, if carried out by a CMO, would be subject to the provisions of the CRM Directive.[82] These licensing entities (at least some of them) appear to be owned or controlled by CMOs and they seem to perform some of the central activities of CMOs. However, they perform only licensing activities and rely on CMOs for administrative services.[83] They do not offer the full bundle of services as CMOs do.[84] This at the same time means, that licensing and administration of the same rights is done by two different entities, which might compromise the CMO's ability to manage rights effectively.[85] It is odd that neither the CRM Directive nor preparatory documents mention option-3 licensing entities.[86] Calls from academia[87] as well as different stakeholders[88] to clarify in the CRM Directive whether option-3 licensing entities are subject to definition of CMOs fell on deaf ears. The EU Commission clearly did not envisage having every possible licensing entity fall under the CRM Directive. Instead, it assumed that the passport entities would be competing against other licensing entities, which fall outside the CRM Directive's application, for attracting repertoire with the passport entities.[89] This would, however, only be true if option-3 licensing entities would fall under the scope of the CRM Directive. Otherwise, rightholders would have no guarantee that option-3 licensing entities accept their rights for licensing and management. The legal status of these entities could hypothetically requalify if they accepted to represent the repertoire of another rightholder or CMO, thereby effectively becoming collective managers. However, if they are not subject to the CRM Directive, neither are they subject to an obligation to accept such a request[90]. Moreover, if the CRM Directive's rules do not apply to option-3 licensing entities, publishers might be incentivised to form licensing entities which are not subsidiaries of CMOs. Option-3 licensing entities, operating under a lower regulatory burden, might incentivise CMOs to create workarounds to escape the application of the CRM Directive (e. g. changing a relation from a CMO subsidiary to an agency agreement).[91] It appears that option-3 licensing entities are left

79 Emanuela Arezzo (n 23) 547.

80 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, OJ L 84/72 Art. 3 b) and recital 16.

81 An organisation can be understood as a CMO or IME even if it represents as few as two rightholders: Mihály Fiscor, 'Collective Management and Multi-Territorial Licensing: Key Aspects of the Transposition of Directive 2014/26/EU' in Irini Stamatoudi (ed), *New Developments in EU & International Copyright Law* (Wolters Kluwer 2016) 234.

82 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, OJ L 84/72 Art. 2 (3).

83 European Commission, 'Press Release - Mergers: Commission Approves Joint Venture for Cross-Border Licensing of Online Music between PRSfM, STIM and GEMA, Subject to Commitments Brussels, 16 June 2015' (n 25) 1.

84 Towse (n 3) 25.

85 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, OJ L 84/72 Recital 19 (2).

86 Schwemer (n 23) 142.

87 Josef Drexl and others, 'Comments of the Max Planck Institute for Intellectual Property and Competition Law on the Proposal for a Directive 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 COM (2012)372' 44(3) IIC (2013) 322, para 29.

88 European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the Document Proposal for a Directive 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' (n 9) 63.

89 ibid 162.

90 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, OJ L 84/72 Art 30.

91 Anthonis (n 18) 159.

outside of the scope of the CRM Directive. It is up to the discretion of national legislators to clarify the scope of the application (as was done in the German implementation), and the interpretation by the courts.[92] Mono-repertoire direct licensors not being subject to the same or similar rules as CMOs is one of the lost benefits of online music services and authors in the online music licensing market.

D. Lost Benefits

I. Imbalance of stakeholder interests

21 Some benefits which both users and rightholders enjoyed in the offline music licensing market (including cross-border use of works) were not reflected in the online licensing market. There are several reasons for this. European soft law instruments, the CRM Directive (but to a large extent also the CDSM Directive[93]) were strongly oriented towards rightholders, ultimately benefiting large publishers. A closer look at stakeholder interests in the Impact Assessment of the CRM Directive suggests that major music publishers were not in favour of bringing their rights back to collective management. They supported the emergence of various licensing entities, a broad withdrawal right, and 'bespoke' licences with online music services.[94] Music service providers advocated a limited number of licensing entities, creation of a Global Repertoire Database (to facilitate identification of repertoire and avoid 'double invoicing') and 'full-scope licencing' (where mechanical and public performance rights would not be licensed separately).[95] Some stakeholders[96] even asked for rules on CMOs to be extended to option-3 licensing entities[97], while others[98] asked to clarify whether the definition of CMOs also applies to option-3 licensing entities[99]. The final version of the CRM Directive thus corresponded to the demands of large publishers. When it comes to online music services, not only the CRM Directives largely ignored their needs, but also market-driven developments proved unfavourable to them – repertoire withdrawn due to Recommendation 2005 was not re-aggregated in the system of collective licensing and the Global Repertoire Database, originally initiated by CMOs, was abandoned.[100] The CRM Directive review in April 2021 provides another chance for the EU legislator to balance stakeholder interests and also to factor in market developments in the legislative solution.

22 Thus far, the EU legislator did very little to address a licensing framework of online music rights, especially information on rights' ownership, access to data, interoperability of data, and tariffs for online use. Moreover, phenomena such as split copyrights and metadata administration existed also in the online realm but did not cause any frictions. This is no longer true in the online environment, due to market developments and technical challenges connected to online rights administration.

23 Recent developments, particularly proliferation of licensing entities (as illustrated above) provided responses only to some issues faced by online music services. The need for a new approach is underlined by the fact that the CDSM Directive subjected a large group of online services – online content sharing service providers – to the need to obtain a licence.

92 Schwemer (n 23) 144.

93 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130/92 2019.

94 European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the Document Proposal for a Directive 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' (n 9) 60.

95 ibid 62.

96 Smaller publishers represented by IMPALA – Independent Music Companies Association.

97 European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the Document Proposal for a Directive 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' (n 9) 61.

98 Private broadcasters.

99 European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the Document Proposal for a Directive 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' (n 9) 63.

100 'PRS Confirms Global Repertoire Database "Cannot" Move Forward, Pledges to Find "Alternative Ways" | Complete Music Update' <http://www.completemusicupdate.com/article/prs-confirms-global-repertoire-database-cannot-move-forward-pledges-to-find-alternative-ways/> accessed 28 February 2018.

II. Lack of blanket licences for online use of music

24 A typical feature of the offline music licensing market was issuance of blanket licences covering the world-wide repertoire for users, albeit only for the territory of one Member State. Blanket licences bring several advantages for users - the certainty that all musical works they use are covered by the blanket licence[101], the security regarding the cost of use and reduced risk of conflict and litigation[102]. Blanket licences also benefit rightholders in facilitating proof of infringement. It sufficed to show the unauthorised use of a single work to presume infringement of all the others contained in the same repertoire and simultaneously licensed by a CMO[103]. Currently, rightholders have to demonstrate infringement analytically, i.e. by giving evidence one-by-one, of which works within the repertoire have been used without authorisation[104]. Despite the benefits for users, the CRM Directive failed to sufficiently address the lack of blanket licences in the online environment[105].

25 Blanket licences are weakened not only due to the withdrawn rights of option-3-publishers, rendering CMOs unable to represent the world repertoire, but also due to to the so-called "carve-outs". After the European Commission's decision in the *CISAC* case[106], CMOs started renegotiating their mutual reciprocal representation agreements and many CMOs have introduced "carve-out provisions" in relation to the licensing of repertoire for those online services which mandating CMOs have decided to license directly on a multi-territorial basis[107]. Once a CMO has decided to "carve-out" their rights, it will give notice to other CMOs. However, some local CMOs may not adhere to limitations of their mandate and purport to grant a license to the "carved-out rights". Currently, there is no legal mechanism compelling CMOs to update their databases in a timely manner and exclude the carved-out rights. Consequently, due to the lost benefit of blanket licences, online music services are not only unsure whether they have actually obtained all necessary licences, but might end up paying multiple times for the use of the same works due to CMOs' practices connected to carve-outs. Avoidance of double-invoicing was one of the main requests of online music services before the adoption of the CRM Directive.[108]

III. The problem of 'split copyright' transferred from licensors to users

26 Unlike other IP rights, copyright law allows for almost limitless divisibility of ownership, contributing thus significantly to increasing complexity in licensing and collective management[109]. Musical work (a song) is typically a result of a creative effort of a multitude of authors. An analysis of top 10 hit songs shows an increasing amount of rightholders being involved in one song over past decades[110], reaching the average

101 Mihály Ficsor, *Collective Management of Copyright and Related Rights* (WIPO 2002) 139.

102 Christian Handke, 'Collective Administration' in Richard Watt (ed), *Handbook on the Economics of Copyright: A Guide for Students and Teachers* (Edgar Elgar 2014) 184.

103 Ariel Katz, 'The Potential Demise of Another Natural Monopoly: Rethinking the Collective Admininstration of Performing Rights' (2005) 1 Journal of Competition Law & Economics 541, 556.

104 Emanuela Arezzo (n 23) 557.

105 Sylvie Nérisson (n 57) 75; Romana Matanovac Vučković (n 58) 415.

106 *Commission Decision of 16072008 relating to the proceeding under Article 81 of the EC Treaty and Article and Article 53 of the EEA Agreement (Case COMP/C2/38698 - CISAC)* [2008] European Commission C(2008), 3435 final.

107 Carve-out essentially means that a mandating CMO unilaterally limits the scope of the mandate granted to a mandated CMO in order to reserve an "exclusive customer group" for the purpose of directly licensing its repertoire.

108 European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the Document Proposal for a Directive 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' (n 9) 62.

109 Daniel Gervais, 'The Changing Role of Copyright Collectives' in Daniel Gervais (ed), *Collective Management of copyright and related rights* (Second Editions, Kluwer Law International 2012) 12. Daniel Gervais, 'The Changing Role of Copyright Collectives' in Daniel Gervais (ed), *Collective Management of copyright and related rights* (Second Editions, Kluwer Law International 2012) 12.

110 'Music Reports' Songdex® Analysis Shows Trend toward More Songwriters and Publishers for Top Hits since 1960s' (4 August 2017) <https://www.businesswire.com/news/home/20170804005339/en/Music-Reports%E2%80%99-Songdex%C2%AE-Analysis-Shows-Trend-Songwriters> accessed 21 August 2020. 'Music Reports' Songdex® Analysis Shows Trend toward More Songwriters and Publishers for Top Hits since 1960s' (4 August 2017) <https://www.

number of four writers and six publishers. The phenomenon of each rightholder owning a share in a work is known as "split copyright". Users must licence 100% of rights before offering their service. In many cases there will be more than one rightholder owning rights in one song. These rights might be transferred to different publishers and/or administered by different CMOs. Thus, clearing rights to a single song might require an involvement of several licensing entities. Rights might be registered within different CMOs and in different databases. An additional level of complexity might arise if rightholders cannot agree on the percentage of shares they own and on entities representing these shares[111]. Challenges connected to split copyright are not *per se* legal but relate to repertoire identification and are particularly pressing in the digital world[112]. Difficulties connected to split copyright were irrelevant in connection to licensing for offline use because the system of reciprocal representation agreements in connection to blanket licences covered the world repertoire[113], albeit only in one territory. Users had a certainty that they licenced 100% of rights in all songs in the repertoire offered by a CMO on a national basis (typically the world repertoire). However, in the online licensing world, users must make sure they licensed 100% of each work. Thus, the burden of split copyright is not borne by CMOs, which can benefit from databases and an established international network, but by online music services.

IV. Unclarities connected to tariff-setting for multi-territorial use of musical works

27 Another element providing legal certainty for users – tariff setting – remains obscure in connection to multi-territorial licences[114]. The problem is essentially twofold. Firstly, online music services have to obtain licences from a multitude of licensing entities, as illustrated in part B. It has to be noted that before the online music licensing transformation, licences had to be obtained from national CMOs, which are typically subject to statutory regulation, including pricing of licences[115]. Currently, online music services have to contact licensors which are subject to uneven regulation. These licensing entities include mono-repertoire direct licensors, CMO hubs, IMEs and national CMOs. Tariffs used by national CMOs are frequently regulated by national laws of EU Member States. However, tariff-setting of mono-repertoire direct licensors is far more dubious since the CRM Directive does not apply to them. Although some indication on their tariff-setting was available in the past, currently it is almost impossible to know how these licensing entities set their tariffs[116]. It has been observed that one of these entities, SOLAR (formerly CELAS), used up to 60 times higher tariffs than the German collective management organisation, GEMA[117]. Tariffs and licensing conditions are negotiated on a case-by-case basis between users and licensors. Moreover, since these entities are not subject to the obligation of non-discriminatory treatment of users, tariff rates and licensing conditions might vary substantially with regard to similar services. For users, negotiation on licence terms with CMOs is easier and more transparent than with mono-repertoire multi-territorial direct licensors[118].

28 According to the CRM Directive, both parties must negotiate licences in good faith and provide each other with necessary and relevant information. Tariffs must be reasonable to, *inter alia,* the economic value of the use of the rights in trade, taking into account the nature and scope of the use as well as in relation to the economic value

businesswire.com/news/home/20170804005339/en/Music-Reports%E2%80%99-Songdex%C2%AE-Analysis-Shows-Trend-Songwriters> accessed 21 August 2020.

111 Ben McEwan and Paul Dilorito, 'Interview with ICE Services & PRSfM - Integrated Licensing and Processing Hub' in Paul Kempton and Massimo Travostino (eds), *Finding the Value in the Gap* (FRUKT 2018) 309.

112 Johann Heyde (n 58) 296.

113 Users were thus certain that they obtained 100% of each work they use.

114 Sylvie Nérisson (n 57) 75; Romana Matanovac Vučković, 'Implementation of Directive 2014/26/EU on Collective Management and Multi-Territorial Licensing of Musical Rights in Regulating the Tariff – Setting Systems in Central and Eastern Europe' (2016) IIC Max Planck Institute for Innovation and Competition 45.

115 Christian Handke (n 51) 184; Daniel Gervais, 'Collective Management of Copyright: Theory and Practice in the Digital Age', in Daniel Gervais (ed), *Collective Management of Copyright and Related Rights* (3rd edn, Kluwer Law International 2016) 10.

116 Romana Matanovac Vučković (n 114) 46.

117 Nikita Malevanny (n 51) 218.

118 'CELAS Auch in Berufung Gegen MyVideo.de Gescheitert | Informiert Bleiben | K&L Gates' <http://www.klgates.com/de-DE/celas-auch-in-berufung-gegen-myvideode-gescheitert-06-02-2010/> accessed 2 September 2020.

of the service provided by the CMO.[119] Pursuant to the CRM Directive, there are no differences in criteria for tariff-setting for online and offline use, but the application of those criteria should lead to different results since the repertoires in online and offline use are completely different. While in online licensing the repertoire is strictly limited, in traditional licensing the monopolistic territorial CMOs represent the global repertoire. Thus, 'the economic value of the use of the rights in trade' and the 'economic value of the service provided by the CMO' are certainly different for the world-wide repertoire on the one side, and the limited repertoire on the other side.[120] Special provision concerning tariff-setting in online licensing is contained in Article 16 (2), which provides that in case of 'new type[s]' of online services, which have been available in the EU for less than three years, CMOs are allowed to use licensing terms without these terms becoming a precedent for other licences. Recital 32 clarifies what can be understood 'a new type of online service' by referring to 'totally new forms of exploitation and business models'. The CRM Directive, however, does not explain what should be understood as 'innovative services'. It seems to be up to a CMO to construe in individual cases whether a certain online music service is a 'new type'. If a 'totally new form of exploitation' is to be understood as a kind of service that has not been previously offered, only a very limited number of online music services could benefit from this provision. Moreover, the granting of an individual licence as a derogation from the non-discrimination principle is a mere possibility for a CMO, not an obligation. CMOs would thus have a substantial level of discretion in determining whether a specific online music service can benefit from an individualised licence.

29 Licensing hubs negotiate tariffs with online music services on a case-by-case basis and enjoy a substantial degree of pricing autonomy from CMOs participating in a CMO hub[121]. Although they are obliged to treat users in a non-discriminatory manner[122], sometimes it might not be clear under which category of users a specific online music service falls and online services might call for application of different rates than their competitors[123]. This decision would most likely be made solely by CMO hubs. Moreover, smaller online music services would lack the negotiating power of big services, such as YouTube and Spotify, to avail themselves of favourable licensing terms.

V. Metadata processing challenges and a multitude of databases

30 Online use of musical works via streaming platforms generates vast amounts of metadata. [124] Streaming platforms provide usage reports to licensors, which they have to process and connect to rightholder information for the purpose of royalty distribution. According to existing reports, the largest CMOs have to process billions of metadata[125]. This results in a substantial technological and financial strain on CMOs[126]. Metadata regarding information of ownership of rights and respective shares is recorded in databases operated by CMOs or other licensors. Every month, CMOs receive usage reports from online music services, but they struggle to process and pay revenues to authors in a timely manner. Consequently, more than 20% of performing rights'

119 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, OJ L 84/72 Art. 16 (2), Recital 31.

120 Romana Matanovac Vučković, 'Implementation of Directive 2014/26/EU on Collective Management and Multi-Territorial Licensing of Musical Rights in Regulating the Tariff-Setting Systems in Central and Eastern Europe' (2016) 47 IIC - International Review of Intellectual Property and Competition Law 28, 50.

121 *CASE M.6800-PRSfM/ STIM/ GEMA/ JV, Merger Procedure Regulation, C(2015) 4061 final* (n 64) para 61.

122 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, OJ L 84/72 Recital 31, Art. 16.

123 Christopher S. Reed, *The Unrealized Promise of the Next Great Copyright Act, U.S. Copyright Policy for the the 21st Century* (Edward Elgar Publishing 2019) 169.

124 Musical metadata can be described as information required to identify an audio file (such as name of author, title, other rightholders, money splits etc). Available at: Creative Europe AB music working group, *The AB Music Working Report.* (Office for official publications of the European communities 2016) 2, accessed 12 September 2020.

125 Leanne de Souza, 'Broken, Leaky Revenue Pipes — the Global Music Industry's Data Mess.' (*Medium*, 21 September 2019) <https://medium.com/@rebelbuzz/broken-leaky-revenue-pipes-the-global-music-industrys-data-mess-9b8a25528732> accessed 16 August 2020.

126 "Collecting Societies Are Struggling to Keep up with the Influx of Millions of Lines of Data."' (n 31); 'Streaming Generates Vast Amounts of Royalty Data, and Not All Collecting Societies Are Coping | Complete Music Update' (n 31).

royalties remains unmatched and unattributed[127]. Although unclaimed royalties are typically due to smaller writers and publishers, they are distributed on a market share basis, thus benefiting larger rightholders[128].

31 It has to be noted that while some databases result from cooperation among CMOs (such as ICE's database), other licensors might typically have their own databases. This results in multiple databases being present in the European online music licensing market. Although data discrepancies are solved within one database, they still persist between databases and there is currently no legal measure to solve inter-database inaccuracies. A multitude of databases only amounts to a higher possibility of conflicts among different databases[129]. Existence of multiple databases increases administrative and other transaction costs for rightholders.[130] A market-driven initiative to solve this problem has appeared. The Global Repertoire Database (GRD) aimed to be a single, authoritative source of multi-territory information about the ownership or control of the global repertoire of musical works. As mentioned above, it was a preferred option for users in the CRM Directive Impact Assessment. However, this initiative never materialised, most probably due to disputes between CMOs over control of the global database[131]. A similar legislative suggestion considering establishment of a centralised licensing portal was also discarded (mainly due to competition concerns)[132]. Time will tell whether there is still space for a unified EU-wide or worldwide database. It rather seems from the current developments, that a network of 'decentralised databases' is taking shape in Europe.[133]

VI. Declining role of CMOs in the European online music licensing

32 Metadata processing challenges coupled with legal changes favouring individual licensing[134] have questioned CMOs' role in online multi-territorial licensing. CMOs as intermediaries are not an essential part of the copyright infrastructure[135]. It has been argued that the importance of CMOs in online licensing will decline and their role will be limited merely to offline licensing[136]. On the other hand, it has been argued that CMOs will not be obsolete in the online music licensing market[137] and even calls to legislatively anchor their role in the online world to provide legal certainty to users have appeared[138]. It has been observed that although mechanical rights have been withdrawn from the CMOs' repertoire they are still managed in practice by large CMOs that were selected by publishers as their agents. This shows that CMOs might be indispensable in the online

127 'Where Are the Missing Song Royalties?' (*Music Business Worldwide*, 16 July 2019) <https://www.musicbusiness-worldwide.com/where-are-the-missing-song-royalties-2/> accessed 20 September 2019. 'Where Are the Missing Song Royalties?' (*Music Business Worldwide*, 16 July 2019) <https://www.musicbusinessworldwide.com/where-are-the-missing-song-royalties-2/> accessed 20 September 2020.

128 ibid.

129 <'Why Building More Rights Databases Won't Solve The Music Industry Metadata Problem' (*Hypebot*, 30 January 2018) <https://www.hypebot.com/hypebot/2018/01/why-building-more-rights-databases-wont-solve-the-music-industry-metadata-problem.html> accessed 12 August 2020.

130 Towse (n 4) 14.

131 'PRS Confirms Global Repertoire Database "Cannot" Move Forward, Pledges to Find "Alternative Ways" | Complete Music Update' (n 102).

132 European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the Document Proposal for a Directive 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' (n 9) para 6. 5.

133 Lex Keukens and Hans Bousie, '"Big Data" and Online Music Databases Roles in Digital Exploitation' in Paul Kempton and Massimo Travostino (eds), *Finding the Value in the Gap* (FRUKT) 279.

134 Raquel Xalabarder, '2. 1 Role of Collective Administration in Such Business Models? - Introduction', *Remuneration for the Use of Works, Exclusivity vs Other Approaches* (Walter de Gruyter GmbH 2015) 404.

135 Daniel Gervais, 'The Internet Taxi: Collective Management of Copyright and the Making Available Right, After the Pentalogy' in Michael Geist (ed), *The Copyright Pentalogy How the Supreme Court of Canada Shook the Foundations of Canadian Copyright Law* (University of Ottawa Press 2013) 394.

136 Yee Wah Chin, 'Copyright Collective Management in the Twenty-First Century from a Competition Law Perspective' in Susy Frankel and Daniel Gervais (eds), *The Evolution and Equilibrium of Copyright in the Digital Age* (2014) 283; Katz (n 105).

137 Emanuela Arezzo (n 23) 556.

138 Sylvie Nérisson (n 57) 82.

licensing.[139] Disappearance or substantial decrease of CMOs' role in the online world will have a negative impact on cultural diversity[140]. CMOs willing to cope with metadata processing challenges adopt different ways to do so. They either pool resources together with other CMOs and form a CMO hub (such as ICE) or outsource metadata administration and processing services to other CMOs based on the "tag-on" regime of the CRM Directive.

33 CMOs may issue multi-territorial licences themselves and outsource metadata processing services to technology companies. However, a careful consideration should be given to the fact that IT driven companies may in time become dominant players in the music industry. It has been pointed out that they do not only have capabilities to handle collections from online music services, but also an inclination to extend vertically and handle licence negotiations[141]. Subsequently, as they accumulate repertoire under their control, they will have a strong position in negotiations with users and at the same time find themselves outside of the application of rules on collective licensing. Furthermore, it has been reported that IT companies also develop their own standards for metadata, which might lead to further fragmentation and potential conflict between datasets[142].

E. Conclusion

34 Recent legislative and market-driven changes to the multi-territorial online music licensing market have clearly separated this market from offline as well as the mono-territorial online licensing market. However, these changes have neither facilitated market entry nor contributed to significantly lowering transaction costs for online music services, which face several challenges when navigating the fragmented online music licensing market. Rights clearance for multi-territorial online music services has become increasingly complex due to the rise of individual licencing and the presence of various groups of licensors subject to differing (and sometimes vague) levels of regulation. The role of CMOs has declined. Due to withdrawn rights, they are no longer able to offer the world repertoire. On the other hand, although withdrawn mechanical rights of major music publishers are licensed directly, these rights are still managed by large CMOs. This shows that not all licensors are able to meet challenges connected with online rights administration and that CMOs still have an important role regarding the logistics of management of mass repertoires.[143]

35 The CRM Directive did not provide for a proper balance of interests of stakeholders involved in online music exploitation. Developments of the European online music licensing market were rather unfavourable to online music services and their interests were neglected also by the CRM Directive. The next possibility to properly balance stakeholder interests presents itself in the potential review of the CRM Directive in April 2021. The EU legislator ought to take into account the current rights clearance complexities online music services face and provide a legislative 'compass' to navigate the European online music licensing market. The CRM Directive was not able to bring withdrawn rights back to the system of collective licensing and a prospective legislative amendment might neither be able to do so, unless it introduces substantial changes to substantive copyright law (e.g. redefinition of online rights) or limits the rightholder's withdrawal right. However, it can increase transparency of all licensors towards users. For instance, the prospective legislative amendment can still subject all licensors to the same rules as CMOs or at least clarify their legal status. It has to be noted that the CRM Directive introduced rules applying specifically to multi-territorial online music licensing, but it did not define licensors for the purposes of this market. In order to avoid regulatory grey areas, the potential CRM Directive revision can reconsider the definition of licensors (providing multi-territorial licences for online use), based not on how many rightholders they represent but rather on how many musical works they license.

36 Another potential measure can be a reformulation of Art. 16 (2) (1) of the CRM Directive. It has to be noted that pursuant to the CRM Directive Art. 16, CMOs can, but are not obliged to, provide lower licensing rates to new online music services[144]. Moreover, these provisions only apply to some licensing entities in

139 Anthonis (n 18) 154.

140 Christoph B Graber, 'Collective Rights Management, Competition Policy and Cultural Diversity: EU Lawmaking at a Crossroads' 4 The WIPO Journal 35, 12; Josef Drexl and others (n 87) 54.

141 'Collecting Societies Are Struggling to Keep up with the Influx of Millions of Lines of Data.' (*Music Business Worldwide*, 13 May 2018) <https://www.musicbusinessworldwide.com/the-future-of-digital-performance-rights-management/> accessed 15 August 2020.

142 Intellectual Property Office of the United Kingdom (n 35) 60.

143 Anthonis (n 18) 154.

144 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, OJ L 84/72 Art. 16 (2).

the online music licensing market (arguably only to national CMOs as opposed to other licensors) and present a mere appeal as opposed to an obligation. Only a 'new type' of online service can avail itself of this provision, while it is up to CMOs to evaluate if a service can be considered a 'new type'. Thus, the provision on individual licences in Art. 16 (2) (1) of the CRM Directive in its current form might not bring any benefits to multi-territorial online music services. The potential legislative amendment can give Art. 16 (2) (1) an obligatory character. One of the future potential examples for multi-territorial online licensing can be found in Germany, where the local CMO GEMA provides in its royalty rates a schedule for ad funded streaming services which are offered in Germany for the first time, the possibility to choose a flat-rate tariff (based on estimated number of streams) instead of a statutory minimum per-stream rate in the first and second year of its operation. The new online music services licence is thus not based on a per-stream rate but on a flat rate based on interactivity and projected amount of streams. In the second year of operation of a new music service, the flat rates are 50% higher compared to the first year[145]. Converted to the per-stream rate (and depending on the number of streams), the licence rate in the first year of a new service's operation can be up to four times lower compared to the tariff rate charged to online music services operating in the market for more than two years. New services are obliged to present to GEMA an estimated and expected number of streams, supported with documents such as business plans and market analysis. If the service already operates outside Germany, it also has to supply appropriate reference data and take into account distinctive features of the national market. Interestingly, this regime applies not only to a 'new type' of service, but to all new online music services. The presented option is available only to new online music services operating in a single EU Member State's territory (Germany). Online music services operating in multiple European countries are not able to avail themselves of this option. Moreover, national per-stream statutory tariff rates do not apply to online music services seeking a multi-territorial licence. Currently, there is no 'one-stop tariff' or a rate-setting regime for multi-territorial exploitation of musical works in Europe. The rate setting process should be open, fair and easy to implement.[146]

145 GEMA, 'GEMA Music & Video Streaming, GEMA Royalty Rates Schedule for the Use of Works from GEMA's Repertoire within the Scope of So-called Ad-Funded Streaming Offers, Tariff VR-OD 9', point 4, available at: https://www.gema.de/fileadmin/user_upload/Musiknutzer/Tarife/Tarife_VRA/tarif_vr_od9_e.pdf..

146 Bob Kohn (n 24) 215.

Abuse Of Patent Enforcement In Europe

How Can Start-ups And Growth Companies Fight Back?

by **Krista Rantasaari***

Abstract: The aim of this article is to examine whether smaller companies have any adequate measures to defend themselves against abusive claims. Patent holders can assert their patents inappropriately, thus going against the functions of patents, and going outside the claims and boundaries of what is protected. This is more damaging for smaller companies as they have fewer financial resources. As a corollary, start-ups and growth companies must be able to defend themselves against abusive claims. This article evaluates the abuse of patent enforcement and analyses the abuse of rights principle, the abuse of dominant position, the Enforcement Directive (IPRED) and unjustified threats. The article analyses whether these elements provide tools for start-ups and growth companies when acting as defendants in patent infringement cases that could be considered abusive. The abuse of patent enforcement is increasing for several reasons, such as, the increase in the number of patents, the fact that they are becoming more valuable, the emergence of a growing market for the sale of patents, and the introduction of new entities specialised in patent licensing and litigation. The article argues that the elements presented in this study mitigate, to a certain extent, the potential ill effects of abusive legal proceedings. However, there are limitations and uncertainties; for example, the case law often only applies to specific circumstances, and national practices vary. As a corollary, these legal tools are rather complicated for start-ups and growth companies to apply.

Keywords: patent enforcement; litigation; abuse of rights; NPE; non-practicing entity; start-up; growth companies

Recommended citation: Krista Rantasaari, Abuse of Patent Enforcement in Europe: How Can Start-ups and Growth Companies Fight Back?, 11 (2020) JIPITEC 358 para 1.

A. Introduction

1 Patent law must enable patent holders to assert their rights. However, patent holders can also assert their patents inappropriately, thus going against the functions of patents, and even deliberately going beyond the claims and boundaries of what is actually protected. This is more damaging for smaller companies as they have fewer financial resources. As a corollary, start-ups and growth companies must be able to defend themselves against abusive claims. The question therefore arises as to whether smaller companies have any adequate measures to defend themselves.

2 This article evaluates the abuse of patent enforcement and analyses the abuse of rights principle, the abuse of a dominant position, the Intellectual Property Enforcement Directive (IPRED), and unjustified threats.[1] The article analyses whether these elements provide tools for start-ups and growth companies when acting as defendants in patent infringement cases that could be considered abusive. Abuses of

* University of Turku, Faculty of Law; Email: krista.rantasaari@utu.fi.

1 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2014] OJ L 195/16 (Enforcement Directive, IPRED).

rights are strategies of illegitimate exploitation of an existing legal position.[2] Patent holders' use of patents may be abusive if the initial objectives of the patent system are not followed.[3] Thus, patent holders seek to enforce a patent that is probably invalid or stretch a valid patent right to cover activities outside the patent's proper scope.[4] Abusive claims are particularly damaging when targeted at small, less well-funded rivals such as start-ups and growth companies.[5] Abusive purposes decrease legal certainty and cause increasing transaction costs and, for example, deter or delay companies' entry into the markets.[6] Hence, it is essential to provide tools for start-ups and growth companies that are facing abusive claims or a threat of litigation.

3 One possibility to control such abusive practices is to use procedural law measures. Additionally, competition law can be used as a defence against exclusions of competitors or extractions of a wrongful settlement of payment.[7] Finally, the European Court of Justice (CJEU) has developed the abuse of rights doctrine as a general principle since the *Van Binsbergen* case, which was concerned with the freedom to provide services.[8] The term abuse appears in the context of a dominant position as part of EU competition law, and also applies to patent-related activities.[9] Examples of abusive litigation commenced with dominant undertakings include *ITT Promedia v Commission, AstraZeneca* and *Huawei Technologies*.[10] The IPRED generally applies to intellectual property infringements in EU Member States and requests EU Member States to provide safeguards against the abuse of measures, procedures and remedies.[11] A recent copyright case *Stowarzyszenie 'Olawska Telewizja Kablova'* concerned the calculation of damages.[12] Similar unjustified threats reflect the abuse of the process and refer to threats of groundless proceedings.[13] However, unjustified threats are not harmonised in Europe and therefore, the focus is on national legislation.

4 Abusive patent enforcement practices can be adopted by any patent holders.[14] However, non-practicing entities (NPEs), also called Patent Assertion Entities or patent trolls, are used here as an example as their core business is patent enforcement. NPEs referred to here are corporate entities that buy and develop patents with the intent of threatening or suing other companies in order to obtain financial compensation.[15] Also start-up and growth companies

2 A Saydé, *Abuse of EU Law and Regulation of the Internal Market* (Hart Publishing, 2014) 29-30. See also A Lenaerts, 'The General Principle of the Prohibition of Abuse of Rights: A Critical Position on Its Role in a Codified European Contract Law' (2010) 18 European Review of Private Law 1127, 1122; A Leónard, 'Abuse of Rights in Belgian and French Patent Law – A Case Law Analysis', (2016) 7 JIPITEC 2.

3 B Love, 'Bad Actors and the Evolution of Patent Law' (2015) 101 Va L. Rev. 1; A Strowel and A Léonard, 'Cutting Back Patent Over-Enforcement, How to Enforce Abusive Practices Within the EU Enforcement Framework (2020) 11 JIPITEC 1.

4 MJ Meurer, 'Controlling Opportunistic and Anti-Competitive Intellectual Property Litigation' (2003) 44 Boston College Law Review 510.

5 The term start-up and growth companies is used in this research as it focuses on companies that are relatively small, young and highly innovative.

6 For an analysis, see MJ Meurer, (n 4), 519 and 521.

7 MJ Meurer, (n 4), 508-509.

8 Case C-33/74 *Van Binsbergen v Bestuur van de Bedriftsvereniging voor de Metaalnijverheid*. ECLI:EU:C:1974:313.

9 Article 102 of the Consolidated Version of the Treaty on the Functioning of the European Union [2007] OJ C 306/1 (TFEU).

10 Case T-111/96 *ITT Promedia NV v Commission.* ECLI:EU:T:1998:183; Case C-457/10 *P AstraZeneca v Commission.* ECLI:EU:C:2012:770 ; Case C-170/13 *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH.* ECLI:EU:C:2015:477.

11 Article 3(2) of the IPRED.

12 Case C-367/15 *Stowarzyszenie 'Olawska Telewizja Kablova' v Stowarzyszenie Filmowców Polskich*. ECLI:EU:C:2017:36.

13 C Heath, 'Wrongful Patent Enforcement: Threats and Post-Infringement Invalidity in Comparative Perspective' (2008) 39 IIC 308.

14 C Chien, 'Of Trolls, Davids, Goliaths, and Kings: Narratives and Evidence in the Litigation of High-Tech Patents' (2009) 87 N.C. L. Rev 1571 < https://digitalcommons.law.scu.edu/facpubs/4 > accessed 17 November 2020; A Strowel and A Léonard, (n 3), 3.

15 For NPEs, see, inter alia, A Ohly, 'Patenttrolle oder: Der Patentrechtliche Unterlassungsanspruch unter Verhältnismälbigkeitsvorbehalt? Aktuelle Entwicklungen im US-Patentrecht und Ihre Bedeutung für das Deutsche und Europäische Patentsystem' (2008) 787 GRUR Int; T Ewing and R Feldman, 'Giants Among Us' (2012) 1 Stan. Tech. L. Rev; C Helmers and L McDonagh, 'Trolls at the High Court' (2012) Law, Society and Economy Working Papers < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2154958> accessed 27 November 2020; C Chien, 'Start-ups and Patent Trolls' (2012) Santa University Legal Studies Research Paper No.09-12, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2146251> accessed 27 November 2020; S Fusco, 'Markets and Patent Enforcement: A Comparative Investigation of Non-Practicing Entities in the United States and Europe' (2014) 20 Mich. Telecomm. & Tech. L. Rev.; D

are targets of NPE litigation.[16] NPEs are active in Europe, for example, in Germany, in the Netherlands and in the UK.[17] In Germany the Minister of Justice has demanded measures against patent trolls.[18]

5 The article argues that the studied elements of the abuse of rights principle, the abuse of a dominant position, the IPRED, and unjustified threats mitigate the potential ill effects of abusive legal proceedings to a certain extent. However, there are limitations, and, in addition, national practices vary. The studied elements are examined as institutions. When working effectively, institutions have a major role in reducing uncertainty and transaction costs by establishing a stable structure for the interaction.[19] All elements address the abuse of patent enforcement from their own perspective.

6 The article is structured as follows. Chapter B discusses the abuse of patent enforcement and presents NPEs as an example of abusive practices. Chapter C analyses the abuse of rights principle. Chapter D studies the abuse of a dominant position and abusive of litigation by a dominant undertaking. Chapter E focuses on the abuse of rights under the IPRED. Chapter F reflects on the unjustified threats. Finally, Chapter G presents a summary and considers whether institutions provide safeguards against abusive litigation for start-ups and growth companies.

B. Abuse of patent enforcement

I. Increase of abusive patent enforcement strategies

7 Various changes in the market and legal environments have accelerated rent-seeking activities and abusive patent litigation. Abuse of patent enforcement typically relates to situations when an invalid patent is asserted or there is no patent infringed. In addition, right holders may attempt to extend the actual scope of protection and to weaken the competitor's market position. Furthermore, excessive remedies might lead to the abuse of enforcement.[20]

8 There are multiple reasons for accelerating abusive patent litigation. First, patents are becoming more valuable and the number of patents has increased, and this has accelerated the rate of patent litigation.[21] In Europe, the number of patent applications has increased steadily over the years from 160,004 in 2015 to 181,046 in 2019. The number of published patents has grown from 68,422 in 2015 to 137,787 in 2019.[22] Second, a growing market for the sale of patents has emerged and there are new entities such as patent funds specialised in patent litigation and licensing.[23] Third, an increasing number of products incorporate a combination of many different components, each of which may be subject to one or more patents,

Geradin, 'Patent Assertion Entities and EU Competition Law' (2019) 15 Journal of European Competition Law & Practise; L Cohen et al., 'Patent Trolls: Evidence from Targeted Firms' (2019) 65 Management Science; A Strowel and A Léonard, (n 12).

16 C E Tucker et al., 'The Effect of Patent Litigation and Patent Assertion Entities on Entrepreneurial Activity' (2016) 45 Research Policy 219; L Babin and A Jarrell, 'Patent Trolls' Threat to Small and Medium-Size Enterprises' (2018) 15 International Journal of Business and Public Administration 2-3. For start-ups litigation in Europe, see, inter alia, Darts-IP, 'NPE Litigation in the European Union. Facts and Figures' (2018) < https://www.darts-ip.com/npe-litigation-in-the-european-union-facts-and-figures-2/ > accessed 27 November 2020 10.

17 B Love, 'Bad Actors and the Evolution of Patent Law' (2015) 101 Va L. Rev.; C Helmers et al., 'Patent Assertion Entities in Europe' (2015) Santa Clara Law Digital Commons 2; Darts-IP, (n 14). See also, for example, T Ewing and R Feldman (n 13); C Helmers and L McDonagh (n 13); S Fusco, (n 13); D Geradin, (n 13), 3.

18 H Anger, 'Justizministerin Lambrecht erhöht den Druck auf Patenttrolle' (2020) Handelsblatt, <https://t1p.de/handelsblatt-Eckpunktepapier-Justizminister> accessed 27 November 2020.

19 DC North, *Institutions, Institutional Change and Economic Performance* (CUP 1990) 25; C Ménard and MM Shirley, 'Introduction', in C Ménard and MM Shirley (eds.), *Handbook of New Institutional Economics* (Springer-Verlag 2008) 1-2; EG Furubotn and R Richter, *Institutions & Economic Theory* (2nd edn, University of Michigan Press 2005) 7.

20 A Kesselheim, Intellectual Property Policy in the Pharmaceutical Sciences: The Effect of Inappropriate Patent and Market Exclusivity Extensions on the Health care System (2007) 9 AAPS Journal E307-E308; R M Hilty and K-C Lui, The Enforcement of Patents (Aspen Publisher, 2011) 25; R Hilty, Legal Remedies Against Abuse, Misuse, and other Forms of Inappropriate Conduct of IP Right Holders, in R M Hilty and (eds.), *Compulsory Licensing. Practical Experiences and Ways Forward* (Springer-Verlag, 2015) 381-382.

21 MJ Meurer, (n 4), 519.

22 See the EPO statistics <https://www.epo.org/about-us/annual-reports-statistics/annual-report/2019/at-a-glance.html > accessed 27 November 2020.

23 MJ Meurer, (n 4), 520.

which makes them constantly subject to patent disputes.[24] Thus, this allows a patent holder with comparatively insignificant patents to represent a disproportionate threat to a complex product if the invention in question is used as one of perhaps hundreds.[25]

9 Particularly in the IT sector numerous patents can overlap for only minor improvements.[26] In the life science industry, so-called evergreening patents dominate and the goal is to obtain narrow patent quickly while continuing to argue about the boarder one.[27] In practice, this hinders generic drugs from entering the market. Life science focused start-ups and growth companies are often not the originators of the innovations. Therefore, they are providing generic products for sale in their local market.[28] The generic company sells generics that have the same qualitative and quantitative composition in active substances and the same pharmaceutical form as the originator drug. The originator company may even create patent clusters around the patented drug. Patent clusters are multiple patent applications around the original base patent. This enables the originator company to bring numerous actions against a generic company in numerous countries, even when the originator company does not believe they have any likelihood of being successful. This kind of patent enforcement litigation financially overburdens smaller companies and creates obstacles for market entry.[29] The *ICA Pzifer* case that came before the Italian Courts concerned the delay to market of new generic products in glaucoma eye treatment. The delayed marketing created delayed market entry and a state of legal uncertainty.[30] Delayed market entry causes high-cost outlays and can be particularly harmful for smaller companies.

II. Patent holders adopting abusive strategies

10 The possibility for the abuse of patent enforcement provides new strategies for companies and have prompted the arrival of new strategic actors. Abusive patent enforcement strategies can be applied by any patent holders, such as companies or individuals.[31] The rise of companies on the enforcement scene such as NPEs has formed the focus of the debate.[32]

11 NPEs, in general, operate as patent funds. Patent funds are organisational arrangements that market actors create to facilitate transactions and contractual agreements.[33] For example, a patent fund may help innovators to obtain a return from their research and development activities by negotiating licenses with companies interested in exploiting their technology. In the case of an infringement, such a patent fund may assist innovators in enforcing their patents and receiving compensation for their investments. Patent funds might also cooperate with the operating company and target the rivals of the operating company on a downstream product

24 M Lemley and C Shapiro, Patent Holdup and Royalty Stacking (2007) 85 Texas Law Review 1992.

25 A Ohly, (n 13), 791.

26 A Ohly, (n 13), 791.

27 D Guellec and B van Pottelsberghe de la Potterie, *The Economics of the European Patent System. IP Policy for Innovation and Competition* (OUP, 2007) 98; R Feldman, *Rethinking Patent Law* (Harvard University Press, 2012) 170.

28 M Lemley and K Moore, Ending Abuse of Patent Continuations (2004) 84 Boston University Law Review 81; European Commission, Pharmaceutical Sector Inquiry Final Report, European Commission (2009) <https://ec.europa.eu/competition/sectors/pharmaceuticals/inquiry/staff_working_paper_part1.pdf > accessed 27 November 2020 35.

29 European Commission, Pharmaceutical Sector Inquiry Final Report, European Commission (2009) < https://ec.europa.eu/competition/sectors/pharmaceuticals/inquiry/staff_working_paper_part1.pdf > accessed 27 November 2020 199-200.

30 *Autoritá Garante della Concorrenza e del Mercata,* A431 – Ratiopharm/Pfizer (11 January 2012), Balletino n. 2/2012 5-56. For an analysis see S Vezzoso, 'Towards an EU Doctrine of Anticompetitive IP-Related Regulation' (2012) 6 Journal of European Competition Law and Practice 529-530.

31 C Chien, (n 12) 1574; A Strowel and A Léonard, (n 12) 3.

32 J McDonough III, 'The Mynth of Patent Troll: An Alternative View of the Function of Patent Dealers in an Idea Economy' 56 Emory L. J. 189 (2006-2007); A Hagiu and D Yoffie, 'The New Patent Intermediaries: Platforms, Defensive Aggregators and Super-Aggregators' (2013) 27 J. Econ. Persp. 45; C Law, D Schwatz and J Kesan, 'Analyzing the role of non-practicing entities in the patent system' (2014) 99 Cornell L. Rev. 425; M Lemley and R Feldman, 'Is Patent Enforcement Efficient?' (2018) 98 B. U. L. Rev. 649 < https://repository.uchastings.edu/faculty_scholarship/1679/ > accessed 27 November 2020; R Feldman and M Lemley, 'The Sound and Fury Patent Activity', Olin Stanford Working Paper Series No. 521 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195988 > accessed 27 November 2020.

33 A Ohly, 'Three Principles of European IP Enforcement Law: Effectiveness, Proportionality, Dissuasiveness', in J Drexl, L Boy, C Godt and B Remiche (eds.), *Technology and Competition. Contributions in Honour of Hanns Ullrich* (Larcier 2009) 4; C Ménard and MM Shirley, (n 17), 1.

market.[34]

12 However, NPEs threat to sue other companies in order to obtain financial compensation and incur costs. NPEs also quickly settle for a lower price than the estimated cost of litigation, and do not necessarily bring cases before the courts. As a consequence, un-litigated assertions now form the majority in all patent enforcements. Licensing negotiations and license deals that do not result in litigation are almost invariably kept secret. Thus, patent litigation data provides only partial information on the activities of NPEs.[35] NPEs place the targeted companies under significant pressure, particularly if the company is a start-up or growth company with limited resources. There is a strong incentive for small companies to settle due to the length and cost of litigation.

13 NPEs use excessive power in the pre-litigation phase and force the opponent into a deal. In practice, NPEs contact with a start-up and growth company typically begins with a cease and desist letter accusing the company of infringing one or more of its patents. Subsequently, the NPE then sends a request to the targeted company with, for example, three options: to stop using the technology which is claimed to infringe the patent and to change to an alternative technology, to pay royalties to the NPE, or to face litigation. The high costs and uncertainty of patent litigation, as well as the costs of changing to alternative technology, in most cases force the targeted company to pay royalties to the NPE.[36] Occasionally, an NPE attack results in patent litigation.[37]

In Europe, a litigation threat might apply to a number of countries simultaneously.[38]

14 In the research literature, the increasing litigation and abusive strategies by NPEs have been one of the key concerns as regards the EU's upcoming unitary patent system.[39] The unitary patent system will provide broad patent protection covering most EU countries with a single application and with a common enforcement mechanism.[40] However, the future of the unitary patent system remains unclear. The UK's exit from the EU ("Brexit") also led to its withdrawal from the unitary patent system. In addition, Germany has had constitutional problems with the ratification process.[41] Furthermore, the uncertainty typical to any new court system will also attract NPEs.[42]

34 D Geradin, (n 13), 207-208.

35 M Lemley et al. 'The Patent Enforcement Iceberg' (2019) 97 Texas Law Review 101-102; A Strowel and A Léonard, (n 12), 3.

36 J Mello, 'Technology Licensing and Patent Trolls' (2006) 12 Boston University Journal of Science & Technology Law 388 and 397; A Ohly, (n 13), 790-791; S Fusco, (n 13), 444; C Chien has made a study of the costs and impacts of NPE demands on small companies. See C Chien, (n 13), 10-11.

37 AJ Davis and K Jesien, 'The Balance of Power in Patent Law: Moving towards Effectiveness in Addressing Patent Trolls Concerns' (2012) 22 Fordham Intellectual Property Law & Entertainment Law Journal 836. Patent demands are expensive, and therefore induces settlement. For this matter see C Chien, (n 13).

38 S Scotchmer, *Innovation and Incentives* (The MIT Press 2004) 200.

39 D Harhoff, 'Economic Cost-Benefit Analysis of a Unified and Integrated European Patent Litigation System', *Final Report in Ludwig Maximilian University München* (2009), Tender No. MARKT/2008/06/D, 29-50; D Xenos, 'The European Unified Patent Court: Assessment and Implications of the Federalisation of the Patent System in Europe', 10 Scripted (2013) 252; S Fusco, 'Markets and Patent Enforcement: A Comparative Investigation of Non-Practicing Entities in the United States and Europe', 20 Michigan Telecommunications and Technology Review (2014) 463.

40 The unitary patent system consist of the Regulation (EU) No. 1257/2012 of the EP and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection, [2012] OJ L361/1, Regulation (EU) No. 1260/2012 of 17 December 2012 implementing enhanced cooperation in the area of creation unitary patent protection with regard to the applicable translation arrangements, OJ L361/89 [2012] and the Agreement on a Unified Patent Court, OJ C175/1 [2013].

41 For the analysis of the post-Brexit situation in the UK, see for example T Jaeger, 'Reset and Go: The Unitary Patent System Post-Brexit, SSRN Discussion Paper' (2016); M Lamping and H Ullrich, 'The Impact of Brexit on Unitary Patent Protection and its Court', Max Planck Institute for Innovation & Competition Research Paper No. 18-20 (2018); L McDonagh and M Mimler, 'Intellectual Property Law and Brexit: A Retreat or a Reaffirmation of Jurisdiction?' in M. Dougan (ed.) *The UK After Brexit* (CUP, 2017). For Germany, see A complaint (2 BvR 739/17) was decided by the Second Senate of the Federal Court in 13 February 2020.

See <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-020.html > accessed 27 November 2020. The German Bundestag approved ratification bill on the Unified Patent Court Agreement on 27 November 2020 see < https://www.epo.org/news-events/news/2020/20201126b.html>, <http://patentblog.kluweriplaw.com/2020/11/26/german-bundestag-approves-legislation-to-ratify-the-unified-patent-court-agreement/>, <https://dip21.bundestag.de/dip21/btd/19/228/1922847.pdf >, accessed 27 November 2020.

42 L McDonagh, *European Patent Litigation in the Shadow of the*

C. Prohibition of abuse of rights as a general principle of EU law

15 The abuse of rights principle in the CJEU case law and in the EU Member States' national practices forms an appropriate starting point and has an interpretative function. Union law seeks to prevent the rights it confers from being abused. In Europe, the abuse of rights principle is not a field-specific doctrine, such as the intellectual property specific doctrine of misuse in the US.[43]

16 The CJEU has referred to the prohibition on the abuse of law since the *Van Binsbergen* case.[44] In *Kofoed*, the CJEU argued that there is a general Community law principle prohibiting abuse of rights.[45] The sole purpose of normal commercial operations cannot be wrongfully obtaining advantages from legislation provided for by Community law.[46] The idea of restraining abusive practices emerged in the context of the free movement of services and, thereafter, has been subsequently invoked in many other areas of EU law.[47]

17 The doctrine of abuse has been adopted or even codified in legislation in a number of countries, for example in Germany and in the Netherlands. In those countries, the prohibition of abuse is founded on the restrictive function of good faith or reasonableness and fairness.[48] It may be assumed that such provisions have common practice; however, such approaches vary widely in detail.[49]

18 In Germany, the exercise of a right is not permitted if the only possible purpose is to cause damage to another. In addition, an obligor has a duty to perform according to the requirements of good faith. This general provision provides guidelines to courts and there is need for interpretation in the light of the different circumstances of each case in order to determine if the exercise of a right is contrary to the principle of good faith.[50] Abusive behaviour can also be in conflict with the purpose of the legal provision.[51] In Germany, the condition for an abuse requires that the harmful effect of a particular abuse can be proved.[52] In the Netherlands, a right may be abused when it is exercised with no other purpose than to damage another person or with another purpose than that for which it is granted, given the

Unified Patent Court (Edward Elgar, 2016) 142.

43 R Feldman, 'Intellectual Property Wrongs' (2013) 18 Stanford Journal of Law, Business & Finance 298; See also V Chiappetta, 'Living with Patents: Insight from Patents Misuse' (2011) 15 Marquette Intellectual Property Law Review; DG Competition Discussion paper on the application of article 82 of the Treaty to exclusionary abuses, European Commission (2005) <https://ec.europa.eu/competition/antitrust/art82/discpaper2005.pdf > accessed 27 November 2020.

44 Case C-33/74 *Van Binsbergen v Bestuur van de Bedrijfsvereniging voor de Metaalnijverheid.* ECLI:EU:C:1974:313, para 13. This case is generally considered as the starting point even though the term abuse is not directly used in the decision of the Court.

45 In this article, references to EC law will be replaced by the term EU law to provide consistency. Case C-321/05 *Hans Markus Kofoed v Skatteministeriet.* ECLI:EU:C:2007:408, para 38.

46 Case C-321/05 *Hans Markus Kofoed v Skatteministeriet.* ECLI:EU:C:2007:408, para 38.

47 EU law areas include such areas as agricultural policy, fundamental freedoms, corporate law and tax law. S Vogenauer, The Prohibition of Abuse Law: An Emerging General Principle of EU Law, in R de la Feria and S Vogenauer (eds.), *Prohibition of Abuse of Law. A New General Principle of EU Law* (Hart Publishing 2011) 521. Within the European Treaties, the term abuse appears in the following contexts: in competition law, which prohibits abuses of dominant position (Articles 102 and 104 of the TFEU), and in the Charter of Fundamental Rights, which prohibits abuses of rights and freedoms recognized in the Charter (Article 54 of the Charter of Fundamental rights). See, the Charter of the Fundamental Rights of the European Union (the Charter of Fundamental Rights) [2000] OJ C 364/3. European Treaties form the primary law of the European Union. In addition, the term abuse also appears in the context of the protection of public health, in relation to the abuse of alcohol (Article 168 of the TFEU). Use of the term abuse in other official European Union documents has grown steadily over the years. The research conducted by A Saydé proves that the use of the term abuse and its derivatives is nowadays common in the legal vocabulary of the European Union. See A Saydé, (n 2), 11-12.

48 For Germany, see § 242 of the German Civil Code (*Bürgerliches Gesetzbuch*) (BGB). For the Netherlands, see § 6:2(2) and 6:248(2) of the Dutch Civil Code (*Burgerlijk Wetboek*) (BW). See also A Lenaerts, (n 2), 1127; A Strowel and A Léonard, (n 12), 4.

49 RM Hilty, (n 18), 386.

50 See § 226 and § 242 of the German Civil Code (*Bürgerliches Gesetzbuch*) (BGB). § 242 of the BGB translates Leistung nach Treu und Glauben ("*reasonableness and fairness*") into performance in good faith. See also A Lenaerts (n 2) 1127; A Strowel and A Léonard, (n 12), 4.

51 S Kamanabrou, 'Abuse of Law in the Context of EU Law' (2018) 43 European Law Review 536. See also C Schubert, *Münchener Kommentar zum BGB* (Beck 2016) 212.

52 A Lenaerts, (n 2), 1125.

disparity between the interests that are served by its effectuation and the interests that are damaged as a result.[53] In the Netherlands, an abuse of rights exists when a right is exercised with the intention of causing harm, but also if the right is exercised in a careless and unreasonable manner. [54]

19 In Common law systems, there is no general recognition of the principle of the prohibition of the abuse of rights and no general doctrine limiting deliberately harmful behaviour, unless it corresponds with an existing tort. Furthermore, if a right has been developed in case law, it is considered as a *ratio decidendi* of the judgement, and is hedged with various qualifiers, such as reasonableness.[55] In the Nordic countries, the principle of the prohibition of the abuse of rights is not codified. In Finland, for example, the abuse of rights is seen as a part of the general doctrines of civil law.[56] This principle applies to situations where a right is exercised in way that the intention and motives cannot be thought of as acceptable.[57]

20 The general doctrine of abuse of rights in national laws could apply to IP and patent cases. However, there are only a few known IP related cases. In a copyright case, the Jena Court of Appeal in Germany denied injunctive relief because of the dysfunctional conduct of the right holder based on the § 242 German Civil Code.[58] Defendants in patent litigation have arguably engaged in litigation that has violated the general prohibition of the abuse of rights or the principle of good faith. In the courts, these claims have rarely been successful due to the lack of proof of a specific intention to harm, a malicious intent, or the bad faith of the right holders.[59] The question that arises is whether such national laws would apply either if an IP right as such is used abusively or if there are abusive prosecution procedures or similar occurrences.[60]

21 The formal doctrine of the abuse of rights was developed by the CJEU in *Emsland-Stärke.* Subsequent decisions such as *Halifax* and *Cadbury Schweppes* further defined the test.[61] The CJEU established an abuse of law test that may be useful as a yardstick for other areas of law if detached from their agricultural and tax law setting. The CJEU's elaborate test comprises of two parts in order to find the abuse of rights in a case. The first objective test focuses on the purpose of the right, and the second subjective test focuses on the intention of the party.[62] The objective part resembles the teleological method of interpretation and requires the Court to pronounce on the purpose of a given rule.[63] Respectively, in *Emsland-Stärke* an abuse required a combination of objective circumstances in which, despite the formal observance of the conditions laid down by the Union rules, the purpose of those rules had not

53 See § 3.13 of Dutch Civil Code (*Burgerlijk Weboek*) (BW).

54 A Lenaerts, (n 2), 1125.

55 M Byers, 'An abuse of Rights: An Old Principle, A New Age' (2002) 47 McGill Law Journal 396; A Lenaerts, (n 2), 1125; J Snell, The Notion of and a General Test for Abuse of Rights, in R. de la Feria and S. Vogenaur (eds.), *Prohibition of Abuse of Law. A New General Principle of EU Law* (Hart Publishing 2011) 220; A Saydé, (n 2), 35-37. In an old UK case, the House of Lords unanimously held that the defendant´s motives were irrelevant. For the UK, see *Bradford Corporation v Pickles* [1895] AC 587 (HL). However, in two subsequent cases of nuisance, the House Lords relied on the presence of harmful intent to qualify a behavior as unlawful. See *Christie v Davey* [1893] 1 Ch 316 (HL); *Hollywood Silver Fox Farm v Emmett* [1936] 2 KB 468 (HL).

56 J Pöyhönen, *Uusi varallisuusoikeus* (Talentum 2003) 97-109. In Finnish the abuse of rights is "*oikeuden väärinkäytön kielto*".

57 See for example E Tammi-Salminen, *Sopimus, kompetenssi ja kolmas*, (Suomalainen lakimiesyhdistys 2001) 247-251; M Hemmo, *Sopimusoikeuden oppikirja* (Talentum 2016) 56; S Kulmala, Oikeuden väärinkäytön kielto ja oikeudekäyntikulusanktiosäännökset (2018) 6 Defensor Legis 895. In Finland, the Abuse of Rights have been applied in the Supreme Court cases KKO 1992:145 and KKO 2011:6 and the Supreme Court has referred to it in a number of cases see for example KKO 2015:49, KKO 2009:93 and KKO 2007:99.

58 A Ohly, (n 13); RM Hilty, (n 18), 386. For the case see, OLG Jena (Court of Appeal), MMR 2008 408 and 413.

59 A Strowel and A Léonard, (n 12), 4. For cases, see for the UK, see *Nokia Corporation v. Interdigital Technology Corp.* [2004] EWHC 2920 (Pat); for the Germany, see BGH, 10 May 2016, XZR 114/13 and LG Dusseldorf 4b O 157/14 (19.01.16).

60 RM Hilty, (n 18), 386-387.

61 Case C-255/02 Halifax plc, Leeds Permanent Development Services Ltd., County Wide Property Investments Ltd v Commissioners of Customs & Excise. ECLI:EU:C:2006:121; Case C-196/04 Cadbury Schweppes and Cadbury Schweppes Oversea., ECLI:EU:C:2006:544.

62 Case 110/99 *Emsland-Stärke v Hauptzollmt Hamburg-Jonas*, EU:C:2000:695, para. 52-53; Joined Cases C-116/16 and C-117/16 *T Denmark and Y-Denmark Aps*, ECLI:EU:C:2019:135, para 74. This concept of objectivity was introduced by L Josserand in modern French theory and has been influential in France and other continental countries. See A Metzger, Abuse of Law in EU private Law: A (Re)Construction from Fragments. In de la Feria R. and S Vogenaur (eds.), *Prohibition of Abuse of Law. A New General Principle of EU Law* (Hart Publishing 2011) 239.

63 J Snell, (n 53), 220; A Saydé, (n 2), 93.

been achieved.[64] The subjective part consists of the intention to obtain an advantage and seeks to determine whether the legal norms of the conditions of application have been fulfilled artificially, and whether such an act is compatible with the purpose of the affected legal regime.[65]

22 The artificiality test enquires into the economic reality of the transaction: if the transaction had some genuine economic explanation other than the regulatory benefit claimed, it would not be considered as artificial.[66] In *Emsland-Stärke*, the legal issue was whether the conditions of application of the applicable rule could be considered as fulfilled when they were accomplished through artificial means.[67] In *Vonk Dairy Products* the existence of the subjective element was established by evidence of collusion between the exporter receiving the refunds and the importer of the goods in a non-member country other than the country of importation.[68] The doctrine of abuse of rights may also refer to the harmful intent or general criteria of proportionality or reasonableness. For instance, the Greek authorities did not dispute the existence of the shareholders' rights to decide on an increase in the capital of the company, but rather sought to assess whether this right was being exercised abusively.[69] Hence, the CJEU evoked the eventuality that shareholders exert the right conferred by Article 25(1) of the Second Directive for the purpose of deriving, to the detriment of the company, an improper advantage, manifestly contrary to the objective of that provision.[70]

23 The prohibition of abuse, if allowed to develop too strongly, also causes concern as it could undermine the foundation of the internal market.[71] This concern is also reflected in the CJEU case law in the context of the freedom of movement and the freedom of establishment. The freedom of movement of students or the freedom to establish a company in a Member State and to set up branches in other EU Member States cannot by themselves constitute an abuse of rights.[72] In a reflection on the freedom of establishment, the restrained use of the notion of abuse by the CJEU was applauded by Advocate General (AG) Maduro.[73] However, there is also criticism against an abuse of law test. AG Geelhoed claimed that the subjective element served no purpose in a case concerning the freedom of workers. According to Geelhoed, considerable reluctance to attach weight to such criteria is discernible in the case law. One example is *Levin,* where the workers' motives were not taken into consideration.[74] One reason for this reluctance is that the aim of those concerned may readily be subject to manipulation.[75]

24 Even though in certain contexts there is hesitation as regards the application of the prohibition of abuse, the principle has a prominent role. This criticism also indicates the wide spectrum of the abuse of rights cases. These cases cover various fields of law, for

64 Case 110/99 *Emsland-Stärke v Hauptzollmt Hamburg-Jonas*. ECLI:EU:C:2000:695, para 52. In addition, see for example Case C-206/94 *Brennet AG v Victoria Paletta*. ECLI:EU:C:1996:182, para 25; Case C-212/97 *Centros Ltd v Erhvervs- og Selskabsstyrelse.* ECLI:EU:C:1999:126, para 25.

65 According to the CJEU, the subjective element can be established, inter alia, by the evidence of collusion between the Community exporter receiving the refunds and the importer of the goods in the non-member country. Case 110/99 *Emsland-Stärke v Hauptzollmt Hamburg-Jonas.* ECLI:EU:C:2000:695, para 53. Furthermore, this pragmatic approach to the subjective element has been underlined by the CJEU in Case C-255/02 *Halifax plc, Leeds Permanent Development Services Ltd., County Wide Property Investments Ltd v Commissioners of Customs & Excise*. ECLI:EU:C:2006:121, para 81 and 82.

66 A Saydé, (n 2), 89.

67 Case 110/99 *Emsland-Stärke v Hauptzollmt Hamburg-Jonas*. ECLI:EU:C:2000:695, para 56.

68 Case C-279/05 *Vong Dairy Products Bv v Productschap Zuivel*. ECLI:EU:C:2007:18, para 33.

69 A Saydé, (n 2), 30-31; Case C-441/93 *Panagis Pafitis and others v Trapeza Kentrikis Ellados A.E. and others.* ECLI: EU:C:2000:150, para 32-43; Case 367/96 *Alexandros Kefalas and Others v Elliniko Dimosio (Greek State) and Organismos Oikonomikis Anasygkrotisis Epicheiriseon AE (OAE)*. ECLI:EU:C:1998:222, para 22-29.

70 Case C-373/97 *Dionysios Diamantis v Elliniko Dimosio (Greek State) and Organismos Ikonomikis Anasygkrotisis Epicheiriseon AE (OAE)*. ECLI:EU:C:2000:150, para 33 and 38; Case 367/96 *Alexandros Kefalas and Others v Elliniko Dimosio (Greek State) and Organismos Oikonomikis Anasygkrotisis Epicheiriseon AE (OAE)*. ECLI:EU:C:1998:222, para 28.

71 See AG Geelhoed in Case C-109/01 *Secretary of State for the Home Department v Hacene Akrich.* ECLI:EU:C:2003:112, para 173, 178 and 179.

72 Case C-147/03 *Commission of the European Communities v Republic of Austria*. ECLI:EU:C:2005:427, para 70; Case C-212/97 *Centros Ltd v Erhvervs- og Selskabsstyrelsen.* ECLI:EU:C:1999:126, para 27.

73 AG Maduro in Case C-210/06 *Cartesio Oktató és Szolgáltató Bt.* ECLI:EU:C:2008:294, para 29.

74 Case C-53/81 *D.M. Levin v Staatssecretaris van Justitie*. ECLI:EU:C:1982:105, para 22.

75 Advocate General Geelhoed in Case C-109/01 *Secretary of State for the Home Department v Hacene Akrich*. ECLI:EU:C:2003:491, para 173 and 174.

example, the free movement of goods, the freedom to provide services, the freedom of establishment, company law and tax law.[76] In addition, the abuse of rights principle can be applied to various situations. Abuse of rights is formally exercised in conformity with the conditions laid down in the rule granting the right, whilst the legal outcome may be opposed to the objective of that rule. It is for the national court, in the light of the ruling of the CJEU, to establish the existence of the objective and subjective elements, whether the application of the rule would serve its purpose and whether reliance on the rule would be abusive in certain circumstances.[77] Hence, an examination of the facts is needed to establish whether the constituent elements of an abusive practice are present.[78]

25 The principle of the prohibition of the abuse of rights functions as a corrective mechanism to a strict application of a rule of law by reducing the abusive exercise of the rights granted by that rule. Often a doctrine of abuse is associated with situations where there is no visible infringement of a formal legal requirement. Thus, it has also an interpretative function that ensures the underlying objectives or purposes for the rules are being respected.[79] The general prohibition of the abuse of rights means that the issue of the abuse of rights is addressed through the general legislation. However, it seems rather impracticable that a court would apply such general provisions in the case of an abusive exertion of an IP right. For example, those Civil Law countries that lack balancing instruments of equity might face difficulties making use of such unspecified legislation.[80]

76 The CJEU mentions an example of various fields where the principle of the abuse of rights has been applied. For this see joined Cases C-116/16 and C-117/16 *T-Denmark and Y-Denmark Aps*. ECLI:EU:C:2019:135, para 74.

77 S Vogenauer (n 45) 543. See also Case C-8/92 *General Milk Products GmbH v Hauptzollamt Hamburg-Jonas*, EU:C:1993:82, para 21; Case 110/99 *Emsland-Stärke v Hauptzollmt Hamburg-Jonas*. ECLI:EU:C:2000:695, para 54.

78 C-116/16 and C-117/16 *T-Denmark and Y-Denmark Aps*, EU:C:2019:135, para 98.

79 J Drexl, 'Is There a More Economic Approach to Intellectual Property and Competition Law?, in J Drexl (ed.) *Research Handbook on Intellectual Property and Competition Law* (Edward Elgar Publishing Limited 2008); A Lenaerts, (n 2), 1122; A Strowel and A Léonard, (n 12), 14

80 RM Hilty, (n 18), 391.

D. Competition law limiting abuse

I. Dominant position and its abuse

26 Primarily, courts have relied on competition law to limit abusive practices by patent holders.[81] This is mostly the case in the context of litigation involving standard essential patents (SEPs). The CJEU case of Huawei v. ZTE has offered the most elaborate set of guiding principles for courts.[82]

27 Intellectual property rights do not automatically confer a dominant position. However, they might put the undertaking in the position of abuser.[83] Thus, exercising the exclusive rights conferred by an intellectual property right can be an abuse of a dominant position when used as an instrument for the abuse.[84] In *AstraZeneca*, the CJEU stated that although the mere possession of an intellectual property right does not indicate a dominant position, such possession is still capable in certain circumstances of creating a dominant position, in particular by enabling an undertaking to prevent effective competition on the market.[85]

81 A Strowel and A Léonard, (n 12), 11. For cases see in Germany: LG Dusseldorf 4b o 274/10 (24.04.12), LG Dusseldorf 4a O 54/12 (11.12.12); in the UK *Unwired Planet International Ltd. v Huawei & Samsung* [2017] EWHC 711 (Pat); *SanDisk Corp. v. Philips et al. (including SISVEL)* [2007] EWHC 322 (Ch.); *Vringo Infrastructure Inc V. ZTE (UK) Ltd.* [2014] EWHC 3924 (Pat.).

82 D Geradin, (n 13), 212; A Strowel and A Léonard, (n 12), 11. See Case C-170/13 *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH,* EU:C:2015:477. See also Case AT.39985, Motorola-Enforcement of GPRS Standard Essential Patents, 29 April 2014, C(2014) 2892 final; Case AT.39939, Samsung-Enforcement of UMTS Standard Essential Patents, 29 April 2014, C(2014) 2891 final.

83 M Lamping, 'Refusal to License as an Abuse of Market Dominance: From Commercial Solvents to Microsoft', in RM Hilty and K-C Liu (eds.), *Compulsory Licensing. Practical Experiences and Ways Forward* (Springer 2015) 127; D Geradin (n 13), 212; See Joined Cases C-241/91 P and C-242/*91 P Radio Telefis Eireann (RTE) and Independent Televisions Publications Ltd (ITP) v Commission of the European Communities (Magill)*. ECLI:EU:C:1995:98; Case C-418/01 *IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG*. ECLI:EU:C:2004:257; Case T-201/04 *Microsoft Corp. v. Commission*. ECLI:EU:T:2007:289; Case C-170/13 *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH.* ECLI:EU:C:2015:477.

84 Case C-102/77 *Hoffman-La Roche v. Centrafarm*. ECLI:EU:C:1978:108, para. 16.

85 Case C-457/10 P *AstraZeneca v Commission*. ECLI:EU:C:2012:770, para 186. The CJEU also referred to an earlier case *Magill*.

28 In practice the abuse of a dominant position relates to a position of economic strength from the plaintiff and of acting independently of its competitors, customers and ultimately consumers.[86] An abuse of a dominant position can be verified under Article 102 of the TFEU when the abuse happens within the internal market or in a substantial part of it. For an abuse of a dominant position to apply, it is necessary that three conditions are present together: the existence of a dominant position on the relevant market, the abuse of that position and the possibility that trade between Member States has been affected.[87] Thus, it has to be analysed whether the NPE in question is dominant on a specific market. In the case of a holder of an SEP, there is a stronger likelihood that it confers a dominant position, as it is essential to a standard and there are no alternatives.[88]

29 The concept of relevant market implies that there can be effective competition between products or services that form part of it. Products may involve a combination of many different components, each of which may be the subject of one or more patents.[89] The relevant market presupposes that products and services are regarded as interchangeable or substitutable by the consumer, because of the products, services, price or the intended use.[90] The definition of the relevant market for example can be so narrow that the market is defined as a one-product market. For example, in *AstraZeneca*, the company's patented product was characterised in a narrow market, not in a general market, which led to the conclusion that there were no competitors. Hence, the patent stood as a barrier to entry to the product market.[91]

30 Dominance refers to the ability to have an appreciable influence on the degree of competition on the market.[92] Irrespective of the reasons for which an undertaking holds a dominant position it has a special responsibility not to allow its conduct to impair genuine undistorted competition.[93] Hence, a dominant undertaking must refrain from any behaviour that may unduly prevent other undertakings from entering the market and competing on their own merits.[94]

31 In practice a dominant undertaking will not enjoy the same freedoms operating on the market and interacting with competitors as other undertakings. Thus, the behaviour of the dominant undertaking may be illegitimate, even though the very same behaviour would be perfectly legitimate for any other company.[95] This, however, does not prevent dominant undertakings from competing, even with small competitors. However, there are limitations

In Magill, there was only one source of information for the channel information. Hence, the effective competition was prevented. See joined cases C-241/91 P and C 242/91 *P Radio Television Eireann (RTE) and Independent Television Publications Ltd (IPT) v Commission* (Magill). ECLI:EU:C:1995:98, para 47.

86 See Case 27/76 United Brands Company and United Brands Continentaal BV v EC Commission. ECLI:EU:C:1978:22**,** para 65; Case 85/76 Hoffman- La Roche & Co AG v Commission. ECLI:EU:C:1979:36, para 38-39.

87 Article 102 of the TFEU. See also M Lamping, (n 81), 122.

88 D Geradin, (n 13), 217. See Case AT.39985, Motorola-Enforcement of GPRS Standard Essential Patents, 29 April 2014, C(2014) 2892 final, para. 223.

89 M Lemley and M Shapiro, 'Potent holdup and Royalty Stacking (2007) 85 Texas Law Review 1992.

90 Commission Notice on the definition of the relevant market for the purpose of Community competition law, OJ 1997, C 372/5, para. 7; M Lamping, (n 81), 124; Case 85/76 *Hoffman-La Roche & Co AG v Commission*. ECLI:EU:C:1979:36, para. 28; C-322/81 *Michelin v Commission*. ECLI:EU:C:1983:313, para. 48.

91 The starting for the analysis was the Anatomical Therapeutic Chemical (ATC) Classification System. The narrower market definition was based on the fourth ATC level that is the product's mode of action. For a detailed analysis see J Westin, ´Defining relevant market in the pharmaceutical sector in the light of the Losec case – just how different is the pharmaceutical market?´ (2011) 32 European Competition Law Review 58-59; S Anderman, ´Competition Law Perspective II´ in J. Pila and C. Wadlow (eds.), *The Unitary EU Patent System* (Hart Publishing, 2015) 135.

92 Case 27/76 *United Brands Co v EC Commission*. ECLI:EU:C:1978:22, para. 65; Case 85/76 Case 85/76 *Hoffman- La Roche & Co AG v Commission*. ECLI:EU:C:1979:36, para 38-39. See also European Commission, ´Guidance on the Commission Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings `, OJ 2009, C 45/02, para. 9-13.

93 T Eilmansberger, 'How to distinguish a good from bad competition under article 82: In search of clearer and more coherent standards for anti-competitive abuses' (2005) Common Market Law Review 42; M Lamping, (n 81), 122. See also Case C-322/81 *Michelin v Commission*. ECLI:EU:C:1983:313, para 57.

94 T Eilmansberger, (n 85), 133; European Commission, DG Competition Discussion paper on the application of article 82 of the Treaty to exclusionary abuses (2005) < https://ec.europa.eu/competition/antitrust/art82/discpaper2005.pdf > accessed 27 November 2020, para. 54; M Lamping, (n 81), 122.

95 M Lamping, (n 81), 122.

to such behaviour, for example, a below-cost price can burden an undertaking with smaller financial resources.[96] NPEs as a dominant undertaking may also impose undue costs on downstream manufacturers by charging more in licensing fees than their patented technology justifies.[97]

II. Abusive litigation by dominant undertaking

32 The high level of protection for intellectual property rights means that the proprietor may not be deprived of the right to have recourse to legal proceedings to ensure the effective enforcement of patent rights. From this it follows that in general a dominant undertaking should have the ability to seek legal redress similar to any other undertakings unless the patent system is misused.[98] Generally, abuses of the process occur when a judicial action is unreasonable or vexatious.[99]

33 The CJEU case law on abusive litigation in EU competition law is limited. The earliest cases were *BBI/Boosey & Hawkes* and *Decca Navigator System*.[100] In the first case, there was no abusive conduct and in the second case, other elements of Decca's behaviour, other than the abusive litigation, offered enough legal grounds for the infringement.[101] The more recent cases are *ITT Promedia v Commission* followed by *AstraZeneca* and *Huawei Technologies v ZTE*.[102] In the US's antitrust laws, the improper enforcement of patents is divided into the enforcement of a patent obtained by fraud (Walker process claims) and the enforcement of IPR rights, which, while not obtained by fraud, are considered invalid, unenforceable, or not infringed (sham litigation).[103]

34 *ITT Promedia v Commission* concerned litigation between the telecommunications operator Belgacom and the publisher of the business directory ITT Promedia. Promedia published telephone directories based on the data provided by Belgacom's predecessor RTT. Negotiations to renew the agreement did not succeed and gave rise to numerous legal proceedings between Belgacom and ITT Promedia. ITT Promedia submitted a complaint to the Commission claiming among other things that Belgacom had committed an abuse of a dominant position by initiating vexatious litigation.[104] In *AstraZeneca* the Commission imposed a fine on AstraZeneca for abuse of its dominant position in the proton pump inhibitors' market. The commission focused on two aspects: a pattern of misleading representations presented to the national patent offices and courts with regard to the authorisation applications for the granting of Supplementary Protection Certificates and a misuse of applicable regulatory procedures.[105] In the *AstraZeneca* case the patent litigation tactic was discussed as part of a well-structured abusive strategy.[106] In *Huawei Technologies v ZTE,* Huawei the owner of the SEP had provided a fair, reasonable and non-discriminatory (FRAND) licensing commitment to the standardisation body, and the issue was the right to seek injunctive relief. The injunctive relief

96 Case C-62/86 *AKZO Chemie BV v Commission.* ECLI:EU:C:1991:286, para 72.

97 C Shapiro, 'Injunctions, Hold-Up and Patent Royalties' (2006) 12 American Law and Economics Review; D. Geradin et al., 'Elves or Trolls? The Role of Non-practicing Patent Owners in the Innovation Economy' (2008) TILEC Discussion Paper DP18-2008 2.

98 Case C-170/13 *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH.* ECLI:EU:C:2015:477, para 58.

99 See Article 139 of the Rules of Procedure of the Court of Justice [2010] OJ C177/1. Article 139 enables the CJEU to order a party to pay costs in a case of an unreasonable or vexatious procedure; applied in Case C-338/82 *Carlo Albertini and Mario Montagnini v Commission.* ECLI:EU:C:1984:181, para 51-52; Case T-302/00 R II Order of the President of the Court of First Instance of 29 March 2001, *Anthony Goldstein v Commission.* ECLI:EU:T:2001:108, para. 40-41.

100 BBI/Boosey & Hawkes [1987] OJ L286/36; Decca Navigator System [1989] OJ L43/27.

101 *BBI/Boosey & Hawkes* [1987] OJ L286/36, para. 11; *Decca Navigator System* [1989] OJ L43/27, para 50.

102 Case T-111/96 *ITT Promedia NV v Commission.* ECLI:EU:T:1998:183; Case C-457/10 P *AstraZeneca v Commission.* ECLI:EU:C:2012:770; Case C-170/13 *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH.* ECLI:EU:C:2015:477.

103 For example, S Vezzoso has compared the ITT Promedia and US antitrust law. See S Vezzoso, (n 28), 529-534. See also F Murphy, 'Abuse of Regulatory Procedures – the AstraZeneca Case: Part 2' (2009) 30 European Competition Law Review 300; T Käseberg, *Intellectual Property, Antitrust and Cumulative Innovation in the EU and the US* (Hart Publishing 2012) 24.

104 Case T-111/96 *ITT Promedia NV v Commission.* ECLI:EU:T:1998:183.

105 Case C-457/10 P *AstraZeneca v Commission.* ECLI:EU:C:2012:770. See also J Drexl, 'Astrazeneca and the EU Sector Inquiry: When do Patent Filings Violate Competition Law?' (2012) Max Planck Institute for Intellectual Property and Competition Law Research Paper no. 12-02.

106 Case C-457/10 P *AstraZeneca v Commission.* ECLI:EU:C:2012:770, para 18.

was sought against ZTE, who were allegedly using Huawei's SEPs, but were unwilling to license the disputed patents on the terms offered by Huawei.[107]

35 The CJEU ruled in the *ITT Promedia v Commission* that access to the Court is a fundamental right and a general principle ensuring the rule of law.[108] Rent-seeking activities that lead to the abuse of enforcement should be restricted. At the same time, however, the law cannot aim to deprive the right to seek legal redress. Access to justice is a universally recognised right.[109] Access to justice is one of the pillars of the European Union and mentioned in the TFEU, and also in Article 47 in the Charter of Fundamental Rights of the European Union (EU Charter).[110] The CJEU has referred to Article 47 of the EU Charter in relation to intellectual property cases; however the CJEU also affirms that Article 52(1) of the Charter of Fundamental Rights permits a limitation on the exercise of the rights guaranteed by Article 47.[111] In the ZZ, the CJEU stated that any limitation must necessary and genuinely meet the objectives of general interest recognised by the European Union.[112]

36 Further, the CJEU noted in *Huawei Technologies v ZTE* the need for a high level of protection for intellectual-property rights means that patent owners may not be deprived of the right to have recourse to legal proceedings to ensure the effective enforcement of their exclusive rights.[113] Hence, only in wholly exceptional circumstances are the legal proceedings capable of constituting an abuse of a dominant position within the meaning of Article 102 of the TFEU.[114] The Commission established the presence of wholly exceptional circumstances with the help of two cumulative criteria that have been confirmed by the General Court. These two cumulative criteria must be applied strictly and applied together due to the fact that they constitute an exception to the general principle of access to courts, which ensures the rule of law.[115]

37 According to the first cumulative criterion, the action cannot reasonably be considered an attempt to assert the rights of the undertaking concerned by legal proceeding which only serve to harass the opposing party.[116] According to the second cumulative criterion, the aim of the action must be to eliminate competition.[117] The first cumulative criterion means that the action must be from an objective point of view manifestly unfounded.[118] Thus, if the action is well founded and has no aim to eliminate competition, the patentee is not committing an abuse by taking the competitor to court. Furthermore, purely internal acts within the company or merely preparatory acts of potential abuse, even though manifested externally, cannot constitute abusive practices.[119] The second criterion means that litigation must be planned to have as its goal the elimination of the competition. Therefore, a dominant undertaking has special responsibility not to further hinder the entry of competitors to a market and to weaken the competition. However, this criterion appears to take into consideration the subjective intention of the dominant undertaking. [120]

107 Case C-170/13 *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH.* ECLI:EU:C:2015:477.

108 Case T-111/96 *ITT Promedia NV v Commission.* ECLI:EU:T:1998:183, para 60.

109 Article 8 of the Universal Declaration on Human Rights, UN general Assembly, Resolution 217 A(III), UN Document A/810 (1948) 73.

110 Article 67(4) of the TFEU and Article 47 of the Charter of Fundamental Rights.

111 C300/11 *ZZ v Secretary of the State for Home Department* ECLI:EU:C:2013:363, para 51; Case C-170/13 *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH* ECLI:EU:C:2015:477, para 58. See also Advocate General Wathalet in Case C-170/13 *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH* ECLI:EU:C:2015:477, para 67.

112 C300/11 *ZZ v Secretary of the State for Home Department* ECLI:EU:C:2013:363, para 51.

113 Case C-170/13 Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH. ECLI:EU:C:2015:477, para 58. See also case T-701/14 Niche Generics Ltd v. European Commission. ECLI:EU:T:2018:921, para 248.

114 Case T-111/96 *ITT Promedia NV v Commission.* ECLI:EU:T:1998:183, para 60. Case also further states the ability to assert one´s rights through the courts constitute the expression of a general principle of law which underlies the constitutional traditions commons to the Member States and refers to the Articles 6 and 13 of the European Convention for Human Rights and Fundamental Freedoms. See also more recent case T-701/14 *Niche Generics Ltd v. European Commission.* ECLI:EU:T:2018:921, para 248.

115 Case T-111/96 *ITT Promedia NV v Commission.* ECLI:EU:T: 1998:183, para 56 and 61.

116 ibid., para 55.

117 ibid., para 55 and 56.

118 ibid., para 56.

119 This is described in a great detail in F Murphy, (n 101).

120 See for example Case C-457/10 P *AstraZeneca v Commission.* ECLI:EU:C:2012:770, para 134; Case T-111/96 *ITT Promedia NV v Commission.* ECLI:EU:T:1998:183, para 138; Case 85/76 *Hoffman- La Roche & Co AG v Commission.* ECLI:EU:C:1979:36,

38 The two cumulative criteria include broad concepts such as "manifestly unfounded", which leave much room for interpretation.[121] If the manifestly unfounded, for example, is not based on fraud, there is a fear that inadvertent error or negligence in the patent application might lead to a claim of abuse of enforcement.[122] However, patent rights granted by a public authority are normally assumed to be valid. In practice, third parties seldom know when a patent right is unlawfully granted. In *AstraZeneca,* the defence made a central argument that an abuse of a dominant position exists where a fraudulently obtained patent is enforced.[123] One indicator to the infringement of Article 102 of the TFEU seems to be when the legal proceeding harasses the opponent, for example, in a situation where the dominant undertaking has wilfully enforced a patent knowing that the patent is invalid, or the patent is extended to cover activities outside the granted scope. However, the Commission, later confirmed by the General Court, stated that the need for the actual enforcement of the unduly obtained exclusive right is not a necessary requirement to be able to categorise conduct as an abuse.[124]

39 It is difficult to distinguish between abusive and non-abusive litigation by a dominant undertaking without resorting to subjective concepts such as the intention. Relying on subjective concepts arises where a dominant undertaking makes use of regulatory procedures to the detriment of a smaller rival, for example a start-up or growth company. In the *AstraZeneca* case, a pharmaceutical company had withdrawn a registration for a product in a specific form and at the same time obtained registration for the same product in a slightly different form. This strategy was aimed at delaying the entry of generic producers and parallel traders.[125] In this case, it would have been difficult to establish that the dominant undertaking abused its dominant position without considering the subjective intentions, such as withdrawing and obtaining regulatory approvals without any false statement or other misrepresentation towards the regulatory body.[126]

40 Injunctions play an important role as they expose infringers to the risks that their patented technology will have to be removed from the market at a great cost. The CJEU has focused on the extent to which an SEP holder could seek an injunction to enforce its SEPs without committing an abuse. In the *Huawei Technologies v ZTE*, the CJEU ruled that prior to the infringement proceedings the owner of the SEP has to notify or consult the alleged infringer. First, the owner has to notify the infringer when the infringer was identified as making an unauthorised use of their patents.[127] Second, the alleged infringer has to show willingness to conclude a licensing agreement and the proprietor of the SEP has to present a specific licence on FRAND terms.[128]

41 It has been claimed that the seeking of an injunction leads to exclusion rather than exploitation. However, NPEs are not interested in excluding target companies from the licensing market. As a corollary, restrictions imposed by the CJEU apply to operating companies instead of NPEs.[129] However, the applicability of the *Huawei Technologies v. ZTE* case to NPEs has now been resolved positively by national courts. For instance, the High Court and the Court of Appeal of England & Wales applied the Huawei v. ZTE licensing framework to a patent dispute between an NPE (Unwired Planet) and an operating company (Huawei). Furthermore, German courts have applied this framework to infringement lawsuits filed by an NPE (Saint Lawrence) against two operating companies (Deutsche Telekom and Vodafone). [130]

42 NPEs can use abusive litigation to seek unreasonable

para 91

121 L Moritz, An introduction to EU competition law (CUP 2013) 239.

122 F Murphy, (n 101), 296.

123 Case C-457/10 P *AstraZeneca v Commission*. ECLI:EU:C:2012:770, para 71

124 ibid., para 99. See also S Vezzoso, (n 21), 529-530.

125 M Negorinotti, 'Abuse of Regulatory Procedures in the AstraZeneca Case' (2008) 29 European Competition Law Review 296.

126 L Moritz, (n 119), 239.

127 Case C-170/13 Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH. ECLI:EU:C:2015:477, para 60-61.

128 ibid., para 63.

129 N Petit, 'Huawei v. ZTE: Judicial Conservatism at the Patent-Antitrust Intersection', 2015 CPI AntiTrust Chronicle; Case C-170/13 *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH*.ECLI:EU:C:2015:477, para 52.

130 D Geradin, (n 13), 224. See cases *Unwired Planet v. Huawei* [2017] EWHC 1304 (Pat) (High Court) and [2018] EWCA Civ 2344 (Court of Appeal), *Saint Lawrence Communications GmbH v. Telekom Deutschland GmbH*, District Court Mannheim 2nd Civil Division, 10 March 2015, 2 O 103/14; *Saint Lawrence Communications GmbH v. Telekom Deutschland GmbH*, the Regional Court of Düsseldorf, 31 March 2016, 4a O 73/14.

royalties. As NPEs are not exposed to countersuits and do not face the same reputational constraints as operating companies, it is likely that they will more aggressively assert their patents to maximise their royalty revenues.[131] The first criteria, if manifestly unfounded, can be met by a lawsuit brought by the NPE. The second criteria's aim to eliminate competition is harder to meet due to the fact it is not in the interest of an NPE to exclude the target company from the market, as in that case it will not obtain license fees. Therefore, these cumulative criteria can also be criticised as the abuse can be used for both exploitative and exclusionary purposes.[132] It seems that applying both criteria in an NPE related litigation is hard to implement.

43 In conclusion, it can be seen that the case law addressing abusive litigation by a dominant undertaking is limited and applies partly to specific circumstances such as SEP disputes. Although two cumulative criteria provide a good starting point for an analysis of the abuse process by dominant undertaking, several questions remain open, and the applicability of two cumulative criteria simultaneously to NPEs is problematic. Litigation relating to an SEP holder and injunctions address abuse more frequently. However, in this context the national courts have played a role. The abuse of rights principle creates opportunities for alleging an abuse of a dominant position in national courts; thus, making national doctrines of abuse more relevant.

E. Abuse of rights under the Enforcement Directive

44 In 2004, the European legislators added the application of the abuse of law principle to intellectual property rights through the Directive on the Enforcement of IPR (IPRED).[133] Prior to this, the abuse of rights principle had appeared in trademark law under the concept of bad faith. The concept of bad faith has similarities to the abuse of rights principle. The concept of bad faith is codified in Article 59(1)(b) as an absolute ground for invalidity.[134] In the *Chocladefabriken Lindt* case the CJEU argued that bad faith requires that an intention is shown, and that the intention must be demonstrated on the basis of objective elements.[135]

45 According to Article 2(1), IPRED applies to any infringement of intellectual property rights as provided by Union law and/or by the national laws of the Member State concerned. Hence, it applies to patents. IPRED provides remedies for the infringement, especially as regards damages and injunctions. Article 3(2) of IPRED demands that states take appropriate measures, procedures and remedies against the abuse of enforcement procedures that are effective, proportionate and dissuasive. They should be applied in such manner as to avoid the creation of barriers to legitimate trade and to provide safeguards against their abuse.

46 Due to the broad application of the Directive, the codified abuse of law principle is applicable to almost all remedies and procedural measures in EU intellectual property law.[136] In addition, recital 17 of IPRED demands that the measures, procedures and remedies provided should be determined in each case and take into account the specific characteristics of that case, such as the intentional or unintentional character of the infringement.[137] IPRED has similarities to Article 41(1) of the TRIPS Agreement that argues for ensuring enforcement procedures to permit effective action against any act of infringement of intellectual property rights covered by the TRIPS Agreement, including expeditious remedies to prevent infringements, and remedies which constitute a deterrent to further infringements.

These procedures must be applied in order to avoid

131 D Geradin, (n 13), 217.

132 D Geradin, (n 13), 229.

133 Article 3 of IPRED. IPRED provides harmonisation of civil redress rules and measures and contains the minimum harmonisation rules. 6

134 In addition, Article 61's limitation in consequence of acquiescence and Article 138 prior rights is applicable to particular localities of the Trademark Law. See Articles 59(1)(b), 61 and 138 of the Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union Trademark. The first reference to bad faith was in Article 3(2)(d) of Directive 2008/95/EC of the European Parliament and the Council of 22 October 2008 to approximate the laws of the Member States relating to trademarks, OJ L 299/25.

135 Case-529/07 *Chocoladefabriken Lindt & Sprüngli AG v Franz Hauswirth GmbH*. ECLI:EU:C:2009:361, para 42; Advocate General Sharpston in Case-529/07 *Chocoladefabriken Lindt & Sprüngli AG v Franz Hauswirth GmbH*. ECLI:EU:C:2009:148, para 58. See Articles 59 and 61 of the Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union Trademark. The first reference was in Article 3(2)(d) of Directive 2008/95/EC of the European Parliament and the Council of 22 October 2008 to approximate the laws of the Member States relating to trademarks, OJ L 299/25.

136 A Metzger, (n 60), 243.

137 Recital 17 of the IPRED.

the creation of barriers to legitimate trade and to provide safeguards against their abuse.[138]

47 In 2017, the Commission clarified the provisions of IPRED where there have been different interpretations in EU countries. The guidance is based on rulings by the CJEU and the best practices identified in EU countries. This guidance also focuses on the means, which are particularly important to SMEs, such as the rule on calculating damages, awarding legal costs, and the means to prevent abuse.[139] Hence, abuse has a significant meaning in the guidance. Article 3(2) of IPRED is a general obligation and other articles should be interpreted and applied in the light of the general requirements of this article. As a result, in order to ensure the balanced use of the civil IPR system, the competent judicial authorities should generally conduct a case-by-case assessment when considering the granting of measures, procedures and remedies provided for by IPRED.[140] The balanced use of the civil IPR system is essential as NPEs might also take advantage of the enforcement system if the remedies and enforcement costs are high enough.

48 The abuse under IPRED concerns the proportionality of procedures and remedies, and the proper balance between the parties to the suit.[141] Compensation for example should be based on an objective criterion while taking account of the expenses incurred by the right holder.[142] Since IPRED is an instrument of EU law, its provisions are subject to the interpretation of the CJEU. Therefore, hypothetically, guidance on the interpretation of article 3(2), and the meaning of the abuse in the adjudication context, may be found in the case law of the CJEU.[143] However, the case law is limited in this matter. Most decision referring to article 3(2) concentrate on the effectiveness and dissuasiveness of measures, procedures and remedies.[144] In a recent copyright case *Bastei Lübbe* the litigation was between Bastei Lübbe, a German phonogram producer, and Michael Strotzer, the owner of an internet connection through which an infringement was committed. The CJEU ruled that the Member States should provide effective and dissuasive measures, procedures and remedies in respect of infringements of copyright and related rights.[145]

49 Thus far, case law regarding the measures, procedures and remedies to be applied in such a manner as to provide for safeguards against their abuse has been rare. In a copyright case *Stowarzyszenie 'Olawska Telewizja Kablova'* the ligation was between an organisation collectively managing the copyright of Stowarzyszenie Filmowców Polskich and Stowarzyszenie Oławska Telewizja Kablowa that broadcast television programmes through a cable network. According to the CJEU, in this exceptional case, payment for a loss calculated on the basis of twice the amount of the hypothetical royalty clearly exceeds the loss actually suffered. As a corollary, a claim to that effect could constitute an abuse of rights.[146] In the *Huawei Technologies v ZTE*, AG Wathelet introduced one possible meaning of abuse under article 3(2) of IPRED. In his opinion he noted that the concept of abuse is not defined in IPRED. However, from his point of view the concept necessarily, though not exclusively, encompasses infringements of articles 101 and 102 TFEU.[147]

50 IPRED has been applied to cases evaluating remedies. In a competition law context, the abuse litigation relates to exclusionary and exploitative purposes. However, abusive claims solely based on their exclusionary purposes are not applicable to the NPEs. When evaluating IPRED, the CJEU could also follow the application of the formal doctrine of the abuse of rights by taking also into consideration the subjective part and the intention to obtain

138 Agreement on Trade-Related Aspects of intellectual Property Rights (TRIPS), Marraskesh Agreement Establishing the World Trade Organization, Annex 1 C, Legal Instruments-Results of the Uruguay Round, vol. 31 (15 April 1994) 33 ILM 81, Article 41(4).

139 Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the Enforcement of Intellectual Property Rights, COM(2017) 708 Final, p. 1-2.

140 Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the Enforcement of Intellectual Property Rights, COM(2017) 708 Final, p. 9-10.

141 C Heath, (n 11), 307.

142 Recital 26 of the IPRED.

143 A Strowel and A Léonard, (n 12), 6.

144 For example, most recent cases C-149/17 *Bastei Lübbe GmbH & Co. KG v Michael Strotzer.* ECLI:EU:C:2018:841; C-494/15 T*ommy Hilfiger Licensing LLC et al. v Delta Center a.s.* ECLI:EU:C:2016:528; Case C-57/15 United Video Properties Inc. v Telenet NV, EU:C:2015:471; C-681/13 Diageo Brands BV v Simiramida-04 EOOD. ECLI:EU:C:2015:471.

145 See C-149/17 *Bastei Lübbe GmbH & Co. KG v Michael Strotzer*. ECLI:EU:C:2018:841, para 37.

146 See Case C-367/15 S*towarzyszenie ´Olawska Telewizja Kablova´ v Stowarzyszenie Filmowców Polskich.* ECLI:EU:C:2017:36, para 31.

147 Opinion of Advocate General Wathelet, Case C-170/13, *Huawei Technologies Co. Ltd. v. ZTE Corp. and ZTE Deutschland GmbH*. ECLI:EU:C:2014:2391, para. 63 and footnote 36. See also A Strowel and A Léonard, (n 12), 6.

an advantage. This kind of a balancing exercise acknowledges the intentional and unintentional character mentioned in the Recital 17 of the IPRED

F. Approach of national laws to unjustified threats

51 Unjustified threats refer to a situation where the alleged infringing act, for example, falls outside of the scope of the claim or because the patent is invalid, meaning that enforcement proceedings have been abused. Here the interest is in an affirmative defence called unjustified threats or warning letters. In practice, the patent holder sends warning letters to the manufactures or commercial distributors of allegedly infringing goods, and then later it transpires there was no infringement, or the patent was invalid. The idea behind the letters of infringement is to threaten with infringement action unless the allegedly infringing behaviour stops.

52 Unjustified threats have a background in the Paris Convention that prohibits false allegations in the course of trade.[148] The Guide to the Application of the Paris Convention gives further guidance on the scope of the requirement providing that distinguishing a competitor by undue allegations does not need injurious intention. In addition, the Guide to the Application of the Paris Convention leaves/allows some freedom for the domestic legislation or case law of each country to decide whether and under what circumstances, discrediting and untrue allegations, may also constitute acts of unfair competition.[149]

53 The Paris Convention therefore requires protection against the use of unjustified threats in infringement proceedings. In Europe, the law in this area is not harmonised. A threat allows the addressee to join a pending opposition or appeal proceedings before the European Patent Office (EPO).[150] IPRED does not address unjustified threats or warning letters. In some jurisdictions, unjustified threats or warning letters are implemented through domestic law and used as a basis for the action.[151] The UK has a specific threat provision dealing with unjustified threats to patents. In Germany and the Netherlands groundless threats are dealt with as an aspect of the general tort law or through unfair competition law.

54 The justification for a remedy against groundless threats can be the protection of suppliers, retailers, and consumers from a patentee seeking to damage the business of competitors. For instance, a pharmaceutical company, which knows that its case on patent validity and infringement is weak, can threaten a retailer that stocks the competing product of a rival company with infringement proceedings.[152] Start-ups and growth companies can even be targeted for their use or adoption of existing technology.[153] In practice, NPEs use a warning letter to contact start-up and growth companies accusing the company of infringing one or more of its patents.[154] Unjustified threats can be particularly damaging to smaller companies that may not have the resources to respond or take advice as to whether there has been an infringement.[155] From the perspective of harm to business, threats may be harmful in the way they propose the denial of an activity that may not eventually prove to be unlawful. In addition, threats may cause harm to a company's reputation and lead to a significant loss in sales.[156]

55 In the UK, the threat provision was modified in 2017. According to the Intellectual Property Act, communication contains a threat if a reasonable person receiving the communication understands from it that a patent exists and that a person intends to bring proceedings in the UK for the infringement of that right in the UK.[157] This is a formal definition containing judicial flexibility. A threat can be written

148 Article 10bis 3 ii of the Paris Convention for the Protection of Industrial Property (20 March 1883) 1160 UNTS 231 (as revised)

149 GHC Bodenhausen, *Guide to the Application of the Paris Convention* (United International Bureaux for the Protection of Intellectual Property 1967) 145(g)

150 Article 105 of the European Patent Convention

151 H-P Brack, 'Patent Infringement Warnings in a Common Law vrsus a Civil Law Jurisdiction – An Actionable Threat?'(2006) 37 IIC 31; C Heath, (n 11), 310; Law Commission, *Patents, Trade Marks and Design Rights: Groundless Threats, Consultation Paper no. 212* (2014) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2015/03/cp212_patents_groundless_threats.pdf 7> accessed 27 November 2020 8.

152 Simmons & Simmons International Life Science Group, 'Threatening patent infringement proceedings – an international perspective', Pharmaceutical Law Insight (2016) <https://www.fisal.nl/pdf/publicatie-4.pdf > accessed 27 November 2020

153 C Chien, (n 12), 16.

154 J Mello, (n 34), 388; S Fusco, (n 13), 444.

155 H MacQueen et al., Contemporary Intellectual Property. Law and Policy (OUP 2011) 956.

156 C Heath, (n 11), 308-309; Law Commission, (n 149), 42.

157 §70 of the Intellectual Property (Unjustified Threats) Act 2017.

or unwritten, it does not need to be directed at any particular person.[158] A threat can even be a letter sent in response to an inquiry made by the infringer himself.[159] The test whether a threat is actionable seems to be quite subjective. According to Justice Aldous, the Court must look at the warning through the eyes of a reasonable and normal recipient and thereafter decide whether there is a reasonable argument that it would be understood as a threat of patent proceedings.[160]

56 In the UK, there are two types of infringements: primary and secondary. Primary infringement refers to making or importing goods. Hence, primary infringers are often the manufacturers and importers. By contrast, secondary infringement refers to other acts such as the selling or advertising of goods. Hence, secondary infringers are often the distributors or retailers.[161] In the UK, threats concerning primary infringements cannot be used as the basis for a groundless threat claim, while threats concerning secondary infringement do form the basis of such claims. In patent cases, threats relating to the acts of making or importing products for disposal or using a process are not actionable. The threat provision aims to prevent a right holder shutting down the network of supply without the risk and cost of proceedings to justify their claim. The fear of litigation costs and the availability of an alternative supplier, including the rights holder, act as powerful incentives for a retailer to abandon a product.[162] The infringing actions of the trade source are likely to cause the most damage to a right holder. Hence, they are classified as being primary acts and are excluded from the protection of the threat's provisions. A right holder can therefore threaten a primary infringer without the fear of being sued for making a groundless threat claim. However, these parties can also bring an action for a negative declaration – for example that they do not infringe – in the cases here – the patentee fails to follow up threats with a claim form.[163]

57 In Germany, much of the law governing whether a warning is actionable has developed as a matter of case law rather than a statute.[164] The German Act against Unfair Competition (UWG) has a general clause that prohibits unfair competition practices such as tangible impairment of the interests of competitors, consumers or other market participants.[165] The case law in this context is highly developed, but also rather more casuistic than principled.[166] The UWG contains examples of unfair acts; these include cases where a person discredits or denigrates the distinguishing marks, goods, services, activities, personal or business circumstances of a competitor.[167] In addition, there are cases where facts have been asserted or disseminated about the goods, services, or business of a competitor; these facts have to harm the operation of a business or the credit of the entrepreneur to an extent that shows the facts are not demonstrably true.[168] Here the conduct of the defendant is important and the manner of misappropriation.[169]

58 The UWG applies to acts performed in the course of commerce, therefore wider protection is provided by the general tort law.[170] In practice, the warning must have a clear demand for a specific person to

158 T Sherliker, 'Don´t Threat the Small Stuff – Reform Coming for Unjustified Threats' (2016) 11 Journal of Intellectual Property Law & Practice 330.

159 Cerosa Ltd v. Poseidon Industrie A.B. and Another, High Court of Justice Chancery Division [1973] FSR 223.

160 *Bowden Controls Ltd. v. Acco Cable Controls Ltd. and Another* [1990] RPC 427. The Case concerned a patent dispute in Germany resulting in a finding of infringement, which was subject to appeal. A letter was sent in England referring to the German decision, stating that the company intended to enforce its rights. The Court considered whether it was arguable that the letter constituted a threat.

161 C Heath, (n 11), 308-309; Law Commission, (n 149), 42.

162 Law Commission, (n 149), 3, 6, 42.

163 J Pila and P Torremans, *European Intellectual Property Law* (OUP 2016) 602.

164 H-P Brack, (n 149), 15.

165 Section 3 of the German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*) (UWG); Law Commission, (n 149), 81-82; JP Heidenreich, 'The New German Act Against Unfair Competition', *German Law Archive* (2015), <https://www.harmsen.utescher.com/rechtsanwaelte-patentanwaelte/dr-jan-peter-heidenreich/ > accessed 27 November 2020

166 H Ullrich, 'Anti Unfair-Competition Law and Anti-Trust Law: A Continental Conundrum?', *EUI Working Paper Law No. 2005/01*, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=837086 > accessed 27 November 2020 30.

167 Section 4(7) of the the German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*) (UWG); JP Heidenreich, (n 163).

168 Section 4(8) of the German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*) (UWG); JP Heidenreich, (n 163).

169 H Ullrich, (n 164), 30.

170 §823 of the German Civil Code (*Bürgerliches Gesetzbuch*) (BGB); Law Commission (n 149), 82.

stop a specific activity and warn the infringer that the right holder will file an action if the warning goes unheeded. A warning is unjustified if there is a deficiency in a substantive right and/or in a formal justification for the warning. [171]A substantive right might be lacking if the patent is invalid or has been revoked in full or in part, or if there was no infringement. There would be a lack of a formal justification for example if the warning was misleading.[172] In order for a warning to be actionable for damages there must be culpability on the part of the warning party in the form of either intent or negligence.[173]

59 However, the German Supreme Court has stated that sending a warning letter to the customers of the competition is highly problematic for these competitors. By warning off a competing manufacturer's customers with exaggerated claims, the right can enlarge its exclusive rights beyond the true scope of the IP right in question.[174] In *Spritzgiesmachine* a warning party believed that his/her patent was valid based on the successful maintenance of the patent after an opposition. Hence, he/she was not aware of other relevant prior art, nor did he/she attempt to avoid disclosure of any such prior art.[175] In addition, for an unjustified warning to be actionable for damages under tort there must be a violation of the right of a plaintiff and a causal link between the defendant's conduct and the harm suffered by the plaintiff.[176]

60 In the Netherlands, there is a general duty not to commit wrongful acts and when a wrongful act is committed, the damage has to be repaired.[177] The Dutch Courts have developed these provisions in order to provide protection against the threat of infringement proceedings. The mere fact that a patent is ultimately revoked does not necessarily mean that the threat is unlawful.[178] A threat may be considered unlawful where it is known, or ought reasonably to be known, that at the time of issuing the threat its patent was not valid and/or not infringed.[179] The Courts have also considered a threat unlawful where it is unnecessarily offensive or unnecessarily public. In addition, if the person making the threats is not the owner of the IP rights asserted, the threat will generally be unlawful.[180] There is no formal distinction between primary and secondary infringers. However, this might be a relevant factor when deciding the lawfulness of the threat; for instance, when the primary infringers are already known and no action is directed towards a primary infringer.[181]

61 A defendant should be able to bring an action for the inappropriate use of IP rights, rather than having to wait to be sued for infringement as a defence.[182] There are differences between the examined EU member States regarding addressing unjustified threats in legislation, cases, and approaches. These national differences make the threshold for a reaction to unjustified threats by start-ups and growth companies very high. A company that asserts its patent rights at a European level must consider the unjustified threat element on a case-by-case basis in each jurisdiction. This increases the costs of the transactions. Even though there is no harmonisation addressing unjustified threats in Europe, the essential aim of benefiting from an improper advantage lies behind the unjustified threats and warning letters.

171 M Brandi-Dohrn, 'Die Abnehmerverwarnung in Rechtsprechung und Praxis' (1981) 83 Gewerblicher Rechtsschutz und Urheberrecht 680; H-P Brack, (n 149), 16.

172 H-P Brack, (n 149), 16. For example, a misleading warning could give a false impression that the warning is based on a valid infringement decision. See Bürgerliches- und Verfahrensrecht (BGH), Urteil vom 23.02.1995, I ZR 15/93, 97 *GRUR* (1995) 424-427 (*Abnehmerverwarnung*).

173 H-P Brack, (n 149), 16; B Markesinis and H Unberath, *The German law of Torts* (OUP 2002) 83.

174 Simmons & Simmons, Threatening Patent Infringement Proceedings – an International Perspective (Pharmaceutical Law Insight 2006), < https://fisal.nl/pdf/publicatie-4.pdf > accessed 27 November 2020; Bundesgerichtshof, BGH, Urteil vom. 15 Juli 2005, GSZ 1/04, para 16.

175 Bürgerliches- und Verfahrensrecht, BGH, Urteil vom. 22 Juni 1976, X ZR 44/74, 78 *GRUR* (1976) 715-719 (*Spritzgießmaschine*).

176 H-P Brack, (n 149), 18.

177 Article 162 of the Book 6 of the Dutch Civil Code (*Burgerlijk Wetboek*) (BW).

178 Court of Appeal 20 September 2011, IER 2001/57 (*Kopperts/Boekstein*)

179 Law Commission, (n 149), 83; Supreme Court 27 January 1989, NJ 1989, 506 (*Mejn/Stork*); Supreme Court 29 Maart 2002, LJN AD8184 (*Van Bentum/Kool*); Hoge Raad 29 September 2006, LJN AU6098 (*CFS Bakel/Stork Titan*).

180 See for example District Court Amsterdam, 13 April 2011 (*Steffex*), regarding a claim of copyright infringement.

181 Law Commission, (n 149), 83.

182 R Feldman, (n 25), 310.

This resembles the CJEU case law under the abuse of rights doctrine. In the CJEU case law, the essential aim of benefiting from an improper advantage indicates an abuse.[183]

G. Conclusion

62 Start-ups and growth companies must be able to have safeguards against abusive claims. Institutions set a structure for interaction between different parties and frame these safeguards. This article has evaluated the abuse of patent enforcement and analysed the abuse of rights principle, the abuse of a dominant position, the Enforcement Directive (IPRED), and unjustified threats. The article has provided an analysis of whether these elements provide tools for start-ups and growth companies when acting as defendants in patent infringement cases that could be considered abusive.

63 The article argues that the studied elements mitigate the potential ill effects of abusive legal proceedings to a certain extent. All the elements address the abuse of patent enforcement from their own perspective.

64 The abuse of rights doctrine has not been applied to patent litigation cases by the CJEU. For the abuse of rights principle to apply it is not sufficient that the patent has not been used. In this context, compulsory licensing would provide a solution if the public interest is involved. It would, however, be more meaningful to cover under the abuse of rights doctrine claims that are raised by means of harassing, threatening, weakening the position, or preventing the entry into the market of the defendant. The abuse of rights principle seems to be too general to be used in the IP context.

65 The abuse of a dominant position under Article 102 of the TFEU applies only to a situation where the plaintiff is a dominant undertaking and has sufficient market power. The CJEU case law related to abusive litigation in EU competition law is limited and to a certain extent only applies to specific situations such as the misuse of enforcement procedure and SEP disputes. Two cumulative criteria set a good starting point. However, several questions remain open, such as the definition of "manifestly unfounded". The applicability of the two cumulative criteria simultaneously makes the applicability of NPEs problematic. The aim to eliminate competition indicates exclusionary purposes. In relation to the SEPs and injunctions, NPEs have been addressed in national case law following the CJEU's steps set out in *Huawei Technologies v. ZTE*. Thus, in the UK and Germany, restrictions set by the CJEU apply also to NPEs. In addition, NPEs evidently bring new practices that should be addressed such as the separation between exclusionary and exploitative practices.

66 The IPRED has institutional support at the European Union level. Hence, measures, procedures and remedies can be abused under IPRED. However, the case law is limited and the abuse under IPRED has been applied in the context of remedies. The abuse is not defined in the IPRED. When evaluating the IPRED, the CJEU could follow the doctrine of abuse of rights and take into consideration the essential aim of benefiting an improper advantage.

67 Unjustified threats were studied in the UK, Germany and the Netherlands with the result that National practices were seen to vary. Unjustified threats seem to be complex matter for start-ups and growth companies due to the lack of harmonisation at the EU level. In relation to unjustified threats, the studied countries have different practices. In the UK, there is a specific threat provision addressing unjustified threats to patents. In Germany and the Netherlands, groundless threats are addressed as an aspect of the general tort law or through unfair competition law. These national differences mean that a company asserting its patent rights at a European level must consider the unjustified threat element on a case-by-case basis in each jurisdiction. However, a defendant should be able to have a means of defence earlier than having to wait to be sued for infringement without any real infringement having taken place.

Unjustified threats as an affirmative claim lowers transaction costs and therefore, is particularly beneficial for start-ups and growth companies.

68 In the CJEU case law, in relation to the abuse of rights doctrine, the subjective intention is a precondition for the application of the abuse of rights principle. The subjective intention and the essential aim of benefiting from an improper advantage could also be justified as an unjustified threat. This approach to subjective intention could be taken into consideration when a set of facts establishing unjustified threats are evaluated by national courts. Subjective intention could harmonise national practices to a certain extent. Further study of this harmonisation aspect would offer an interesting research area in the future.

69 The abuse of rights principle, the abuse of a dominant position, the Enforcement Directive (IPRED), and unjustified threats, potentially increase legal certainty and improve efficiency by lowering transaction costs. However, they are not sufficient, and adjustments and clarifications are needed. The

183 Case C-147/03 *Commission of the European Communities v Republic of Austria*. ECLI:EU:C:2005:427, para 55; C-116/16 and C-117/16 *T-Denmark and Y-Denmark Aps*. ECLI:EU:C:2019:135, para 9

generality of the abuse of rights principle, the minor case law, national practices varying significantly, and the lack of harmonisation make the studied legal tools rather complicated for start-ups and growth companies when defending their rights in patent enforcement proceedings.

JIPITEC

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

www.jipitec.eu