Intelligent Environments 2020
C.A. Iglesias et al. (Eds.)

doi:10.3233/AISE200029

Internet Protocol Standards for IoT Interoperability in the House. Open Issues in EU Competition Law

Francesca Gennari, PhD Candidate[a,1]
[a] *Mykolas Romeris University • University of Turin • University of Bologna*

Abstract. IoT for the house raises several concerns under the EU Competition and IP law. In order to create a better level of interoperability between the different smart home IoT objects, undertakings are willing to create new standards, in particular concerning the Internet Protocol. However, this problem seems to be over. In December 2019, Google, Amazon, Apple, Ikea, the ZigBee alliance and many other undertakings belonging to the electronics and innovation world joined together to form the project "connected home over IP" whose main goal is to create *"…a new, royalty free, connectivity standard*". This paper aims at giving a first analysis of this project under a competition law and IP law perspective. The main focus will be both on the interplay between Art.101(1),(3) TFEU and on Standard Essential Patents (SEPS) applied to this project. It will be argued that if this project is considered a collusive agreement, it could become a new case in the SEP litigation framework.

Keywords. IoT, interoperability, competition, IP

1. Introduction

The origin of the Internet of Things (IoT) and of some of its most lucrative applications [1] are connected to the house environment. The purpose of this paper is to outline the importance and main characteristics home IoT objects have, with a special focus on recent policies of the European Union (EU) designed to create a legal environment in which this technology can thrive (§1.1). Apart from the advantages, it is also important to know the main challenges that home IoT objects present not only from a technical but also from a legal point of view. The main challenge to optimize the capacity of the IoT is to allow the different smart appliances of the house to "communicate" not just with the inhabitant of the house but also with other appliances and smart objects. As a consequence, data-portability is a transversal EU IT law principle, established by Art. 20 of the General Data Protection Regulation [2]. Its technical equivalent, interoperability [3], is a target that IoT producers try to achieve as well. To draft a new standard for an internet protocol (IP) for the house is the core of the *"Connected over IP project"* (hereinafter Project IP) (§1.2) [4]. In the second section there will be a first analysis of this project in terms of the EU Competition and IP law on the basis of the information that has been made public so far by the undertakings of this project. This is a first

[1] Francesca Gennari, PhD candidate, LAST-JD-RIoE, https://last-jd-rioe.eu/francesca-gennari.html; E-mail: francesca.gennari8@unibo.it.

assessment and does not claim that Project IP is collusive, as there is not enough data available to, for instance, calculate the influence on the market of some of its partners. However, there are some doubts that arise, especially as far as the correlation between costs to sustain this project and the gratuity of this Project IP fee. The analysis of Competition and IP aspects, though deeply intertwined, will be developed into two separate parts (§2.1, §2.2). It will be argued that, if hypothetically judged anticompetitive by the European Commission, Project IP will set a new scenario not only in competition law, but also in the debate on Standard Essential Patents (SEPs). Its novelty will consist in the influence exercised by a plurality of undertakings in the home IoT connectivity standard market and in the home IoT production one.

1.1. IoT for the house: what it is and why it is important

There is not a unanimous consensus in defining the Internet of Things (IoT) despite this term being twenty-one years old [1]. In any case, there are some elements on which the academic community agrees on and these are the presence of "*[...]material hardware, electronic signals, and electromagnetic emissions that generates, stores, transmits and analyses data*" [5] and where "*ambient sensing occurs by remotely controllable and constantly connected physical objects"* [6].

As far as methodology, the legal analysis of this contribution will focus on the IoT devices that people buy and use in their homes, for the following reasons.

Firstly, because of the relevance of IoT objects in terms of EU policy. IoT is part of the new EU Commission's plan for the next five years in different documents. At the end of 2019, the European Green Deal set the framework in which environmental sustainability has to be considered the long-term objective even for the development of new technologies [7]. The importance of IoT technology and the infrastructure that is required to be competitive was stressed through the release of the 5g Toolkit [8] and the first report of the NIS group of EU Member States [9]. To have a sustainable and secure infrastructure for IoT is also part of the long-term objectives of the New Industrial Strategy for Europe [10]. Besides, the enactment of the Electronic Communications Code [11] together with the Cyber Security Act [12] and the upcoming Data Act [10] will lay out the core infrastructure rules for IoT in the EU.

Secondly, because the first IoT objects were indeed conceived for the house [1]. As a matter of fact, IoT objects for the house are becoming increasingly accessible for the average consumer and will probably play an important role in influencing consumers' habits [13] as they interact with the consumer/data subject by collecting, analysing and producing data [14] [15]. Compared with traditional home objects, IoT home objects have one characteristic that makes them truly special: they all contain embedded electronic material and software, some in a very rudimental form, others in a more advanced one.

1.2. Inter-operability: an underpinning principle in the home IoT and the new Connected home over IP project

In the next few years, the house will be increasingly more connected. IoT objects will not just be more performant and energy efficient on their own [16], but they will become also more connected between themselves, thus enabling the inhabitant to transform each smart object to a node in a network that can be easily controlled by the inhabitant [16]. However, in order to do this, it is indispensable that the different smart appliances can

communicate with each other. This dependence of the components of a future connected house on each other will be a main feature of the future smart house.

As a consequence, interoperability comes into play. Interoperability can be considered an overarching principle of EU IT law and the equivalent of the principle of data portability in the of EU Data Protection law [3]. Interoperability is functional also to the realisation of new technology and, in this specific case, to the construction of IoT objects that can be compliant with the principles of privacy by default and by design as requested by Art.25 GDPR [2] [17].

Nevertheless, interoperability is not just an abstract legal principle. Interoperability is also the technical capacity of different kinds of technologies to "speak" a common language, to execute tasks and to perform functions.

As far as the home IoT are concerned, one of the features that makes home interoperability possible lies in the Internet Protocol used by the different IoT objects in the house. The Internet Protocol is "*the principal set or (communications protocol) of digital message formats and rules for exchanging messages between computers across a single network or a series of interconnected networks… Messages are exchanged as datagrams, also known as data packets or just packets."* [18]. Its function is "*to deliver datagrams from the source computer to the destination host (receiving computer based on their addresses. To achieve this, IP includes methods and structures for putting tags (address information which is part of metadata) within datagrams*". [18].

Therefore, it is interesting to analyse the so-called, "*project connected home over IP*" [4]. In December 2019, Google, Amazon, Apple, Ikea, the ZigBee alliance, and many other subjects (belonging to electronics and innovation world) joined together to create *"[…]a new, royalty free, connectivity standard*" [4]. If the project must be translated in legal terms, it will be clear that some undertakings decided to agree on creating an essential interoperable connectivity standard to make home IoT better. This standard is going to be royalty free and the code will be open source [4]. How can this new project affect the market of home IoT in terms of competition and IP law? On the basis of the information publicly available we will draw a first analysis concerning these two fields of law.

2. Project IP over connected home. The entanglement of EU Competition and IP law

2.1. The possible interplay between Art. 101 (1) and (3) TFEU

This first attempt at giving a competitive assessment of the IP project will start from the basis of EU competition law Art.101 TFEU. Then it will follow a systematic interpretation involving other documents issued by the European Commission following the principle *lex specialis derogat generali*. The objective is to forecast, with the few data available, which kind of reasoning the Commission might follow to evaluate the competitiveness of Project IP.

One preliminary remark is that EU competition law adopts a pragmatic approach which is effects-based. In an analogue way to the American rule of reason, European antitrust uses the principle of proportionality [19] even in competition law to assess the anti-competitiveness of a behavior. In practice, this is done through the interplay of the first and third paragraphs of Art.101 TFEU if more than one undertaking is involved. Firstly, the behavior must be judged anticompetitive and, secondly, there is the

evaluation of reasons that might balance out the anti-competitive character of the behavior. This is called the two steps test [20]. To consider a behavior anticompetitive for two or more undertakings, the Court of Justice of the European Union (CJEU) has held that it is not even necessary to have a formal agreement between undertakings [20] [21]. Sometimes, just the exchange of information within the same network [21], or even the implicit coordinated behavior of two or more undertakings [20] can lead to collusion.

If we read the text of Art. 101 TFEU [22], the first paragraph describes the restrictions per object that are considered unlawful and hardcore competition restrictions in EU law [20][23]. These are not the only restrictions possible. Art 101(1) TFEU also establishes that restrictions can also be considered as such by their effects, making the previous list, *de facto*, an open list. The second paragraph establishes the consequence of nullity for these agreements. Finally, the third paragraph sets out four conditions according to which anticompetitive agreements can be considered compatible with the rules of the Single Market. The conditions are the following: the improvement of the production of a certain good or of technological development; the distribution of the results in a fair share to consumers; the indispensability of the restriction and the non-elimination of competition [22]. In conclusion, even anti-competitive agreements can be lawful if, though distorting competition, either they do that not in a significant way or they promote other interests that are considered beneficial to the market [20]. Other documents to consider are, (in chronological order): the guidelines on the application of (former) Art.81(3) (now Art. 101(3)) TFEU [24], the R&D agreements block exemption regulation [25]. Some might argue that the Regulation of the Commission on vertical restraints and the application of Art.101(3) TFEU to vertical restraints [26] is the relevant set of rules to apply given the diversity of the subjects that can join this project on the supply chain. As a matter of fact, in the 2010 Commission Regulation on vertical restraints (the so called Block Exemption Regulation), the definition of vertical restraint itself encompasses just *"[...]an agreement or concerted practice entered into between two or more undertakings each of which operates, for the purposes of the agreement or the concerted practice, at a different level of the production or distribution chain**, and relating to the conditions under which the parties may purchase, sell or resell certain goods or services.***"[2] This cannot be the case here. In fact, only a few things are clear from the description of Project IP but one is certain: the objective is the creation of a standard that is royalty free and it is not even specified if that applies only to the members of the agreement or also to third parties [4]. This makes inapplicable the guidelines on knowledge transfer agreements as they also involve the grant of a license against the payment of a price[3]. Moreover, in the corresponding Regulation, the only definition for transfer of technology agreement applicable to the IP project would be just the one concerning a *reciprocal agreement*, but it involves just two undertakings whereas here several are involved[4].

It is not claimed that Project IP is *prima facie* anti-competitive. On the contrary, many positive effects might be caused by that, for instance the passage from the Internet of Silos phase [29] to the Internet of Everything. However, the market influence and pervasiveness that Google, Amazon and Apple (which are part of the project) have in the relevant market of IoT for the home, makes it possible to think whether it is really pro-competitive that the three most important players work together. If we agree with

[2] Art. 1.1.a), emphasis added [26].
[3] Para 51 [27].
[4] Art. 1(d)[28].

Professor Petit's theory of Moligopolies[5], we might see that in the near future this market could be influenced thoroughly by a group of enterprises that are part of this project. Even if the IoT connectivity market is judged still very competitive and dynamic [31], the IP project has the objective to create an interoperable connectivity protocol. This is in substance a connectivity standard and it might be worthwhile to consider the smaller market of the IoT connectivity standards for the house, as it is the core of the mission of the IP project (e.g. connected home). There are few doubts that this standard will play a decisive role in the future in this market and exercise a decisive influence on the home IoT market.

Analyzing this project, which is an agreement in EU competition terms, it is evident that creating a standard for an interconnectivity protocol involves the research and development resources of most if not all the undertakings involved. The R&D Block Exemption Regulation [6] could be easily used by the undertakings involved to benefit from an exemption from the application of Art.101(1)[25]. The Project IP agreement seems to fill the condition set out in the Art. 1(1)(a)(i) which is the "*i) joint research and development of contract products or contract technologies and joint exploitation of the results of that research and development"* [25]. It seems an educated guess that, in order for the exemption to apply (Art.2), also the condition of the agreement between the party will have to follow the rules of Art.3 which are *"full access to final result (2), pre-existing know-how (3), joint exploitation connected to IP rights that constitute know-how and are indispensable for the production of the product or the contract technology (4) and the obligation for parties in charge of the manufacture process to fill order for supplies except a joint distribution agreement is in place"* [25]. However, the undertakings involved compete against each other normally on different and on the same markets and it seems that Art.4(2)(i) will be applicable. According to this article, the application of the exemption applies only if *"[…] the case of research and development agreements referred to in point (a)(i), (ii) or (iii) of Article 1(1), the combined market share of the parties to a research and development agreement does not exceed 25 % on the relevant product and technology markets*" [25]. It seems likely that the combined share of all the parties could be higher than 25%. Therefore, it is probable that the R&D block exemption will not apply. However, given the lack of details, for now it is necessary to go back to the general rule, Art.101 TFEU, and check whether the justifications of its third paragraph could be applicable in the case this project is assessed as collusive. In the light of the interpretation offered by European Commission Guidelines on the application of former Art.81(3) TFEU [24] and by the CJEU, all the justifications set out by Art.101(3) are important and therefore cumulative (para 42.)[24]. In practice, the Commission also uses the idea of *workable competition*, indicated by the CJEU [32] as the *criterion* as whether to apply or not Art.101(3) TFEU. There have been a few exceptions to this trend so far[7], but there is still no case-law on the application of

[5] Moligopoly means that a corporation that is dominant on one digital market tries to expand and collaborate with dominant or influent firms from other markets to guarantee the pervasiveness of its action [30].

[6] It must be remembered however that the R&D exemption from the application of Art.101 TFEU is not granted for an unlimited amount of time. It is either seven years or for the duration of the agreement following the conditions detailed at Art. 7(1)(2)[25].

[7] Some of these exceptions concerned selected distribution of luxury goods or professional orders fixing prices for compensation (which are object restrictions), were considered as justified by the CJEU Among these cases, important are *Remia, Pronuptia*

Art.101(3) TFEU for the house IoT. It is still abstract to assess whether the efficiency gain concerning the technological development [22] can outweigh the other three causes of justification. Certainly, this agreement promotes technological development and the "fame" of the participants to this agreement might have a pass on effect on consumers (fair share), but how to calculate the inevitability of this agreement as a possible cause of distortion of competition in the home IoT connectivity market and in the home IoT products in the long run? It is likely that the standard created by Project IP will be the most widely-used one. Even if *prima facie* the positive effects of this project as presented by its promoters outweigh the negative ones, it must be kept in mind that the IoT connectivity market, despite being very competitive at the moment, might change swiftly and become very concentrated as far as IoT connectivity for the house is concerned. The network effects are one of the characteristics of digital markets that can have repercussions on connected markets as well [34]. In order to substantiate better these concerns, it is necessary to explain how IP rights are involved in this competitive assessment.

2.2. SEPs and collusive agreements. Is this the new phase in the SEPs saga?

The competition assessment of this project for interoperability standards is entwined with the analysis of IP rights. After a short explanation of what SEPs are, there will be a comparison of Project IP with the case-law of the CJEU and it will be argued that, if the agreement is ultimately found anticompetitive, Project IP could be the next step in the finding of a new part of the SEPs and FRAND litigation issues. It will not be as expanded as the part on competition as even less information is publicly available.

Building an IoT home object is not simple. Both its simpler material parts and the electronic material might need the application and use of standards possibly involving patents [35]. For instance, an innovator might need one of these patents as they are essential to the functioning of a new home IoT object. This allows an innovator to save the costs of R&D and of a patent procedure. For this reason, they are called standard essential patents (SEPs) [35]. A standard is created either through a process involving the patentee and a Standard Setting Organisation (SSO or Standard Developing Organisation, SDO) or it could be a *de facto* standard [35]. Even if not expressly mentioned, at least part of the protocol standard of Project IP, as in general all connectivity standards, might be subject to a process of patentability, most probably as a Computer Implementing Invention (CII) [29] or involving other intellectual property rights such as designs, know-how and software. Let us go back to the previous example of an innovator who wants to build a new IoT object and needs to use a standard, which is comprehensive of a patent which belongs to another patentee. To avoid infringing someone else's patent, the innovator has to ask the patentee permission to use the standard and is generally subject to the payment of a fee [36] whose value is quite complex to calculate in advance, before the patent is effective [37] [38]. International stakeholders and international organisations (included the OECD and the EU) promoted FRAND conditions on which a fair fee/royalty must be paid[8]. It follows that only

---

and *Wouters* [20]. More recently, agreements that were *prima facie* collusive have been justified by the Commission because of an effective demonstration of the out of market efficiencies, such as in the airlines market [33].

[8] FRAND is an acronym for Fair, Reasonable, And Non-Discriminatory.

undertakings with *a)* a series of useful patents and *b)* consistent economic resources can actively play a role in the IoT market, included the home one.

It is clear that SEPs on the one hand boost innovation, but, on the other hand, they often put the patentee in a position of power on the market, as his/her patent is indispensable to the creation of derived products [3][31]. That can be the origin of an abuse of dominance behaviour under Art.102 TFEU[22]. After a few EU and national cases dealing with patents and SEPs (such as *Volvo*, *Orange-Book-Standard [39]*) the CJEU gave important directives on how to assess the patentee and implementer's behaviour when SEPs and FRAND conditions are involved in the *Huawei* case [40]. This last case deals directly on how to demonstrate a connection between a SEP and the abuse of dominance of Art.102 TFEU[3][31]. In the *Huawei* case, the Court followed the opinion of Advocate General (AG) Wathelet. The AG suggested that there is not a direct correlation between owning a SEP and being dominant on a market[9]. At the same time, it gave some procedural rules on how the patentee and the implementer should behave in case the patentee had previously agreed to license its product according to FRAND terms[10]. As far as the meaning on FRAND, national courts, especially in Germany and in the UK, have been going further in determining substantially what a FRAND fee must contain [35].

As far as it can be understood from the site of the project, it seems that the standard would be a *de facto* one as no mention about any SSOs is done. This would mean saving time and resources from a long process in which a third institution is involved. However, this might contrast with the content of guidelines on how to proceed in dealing with SEPs published by the European Commission [3][41]. In this document we can find some recommendations to follow including transparency (which might not always be a good thing in Antitrust terms, especially in concentrated-oligopolist markets [3]). To achieve this goal, the Commission advised to preferably use FRAND terms for licensing and to guarantee an open source code. One of the actions that the Commission wanted to take is to use existing certifying bodies (maybe national patent offices?[3][41]) to assist the patentee and the SSO in the procedure of standardisation and the drafting of FRAND terms. This is a good idea as the SSOs generally have a private character. Nevertheless, nothing has been done yet in this field. If we try to compare these requirements with what we know of the connected over IP project it must be noted that the Project IP announced that it will use Github to leave the code open source and that must be acknowledged. As far as the FRAND terms, logically there is nothing more Fair, Reasonable and Non Discriminatory than leaving a potentially very useful protocol royalty free for everyone. What is not clear from the project page is whether this gratuity is limited to the parties of the agreement or whether it extends to other undertakings that might ask to use this protocol. In the first case, there would be no collusion and no infringement issues, and this project could really qualify as a charity project. If that is not the case and the royalty free clause concerns just the participants, it ought to be specified which kind of conditions for licensing would apply. In any case, it would be much more comforting to have the involvement of at least one SSO and possibly the opinion of specialised bodies such as national patent offices. In any case, having the involvement of a third party such as a SSO would already be a reassuring sign that the elaboration of the Internet Protocol is supervised by a third party and would appear more pro-competitive to competition enforcement authorities such as the European Commission.

[9] See para. 57 of the Opinion [39].
[10] See para. 103 n.1-2-3-4-5-6-7 of the Opinion [39].

If this last requirement is not followed there could be grounds to start considering the agreement anticompetitive in its effects, following the reasoning scheme exposed in §2.1). Moreover, if that were the case, Project IP would definitely become a new paradigm in the SEP saga. It would be much simpler under the FRAND paradigm as the royalty would be 0 and, in this case, a series of businesses would exercise a collective form of pervasive influence if not dominance on *a)* the access to the market of home IoT connectivity standards and home IoT production; *b)* the choice of Internet Protocols for implementers; *c)* the consumers who would be drawn to the already most known brands.

Conclusions

In conclusion, there are important questions that are not answered by what is made public about the IP project. It is not clear which kind of EU competition legislation to apply as the call is still open and other actors on the supply chain might adhere to different conditions. Either the Block Exemption Regulation on the transfer of knowledge or the R&D block exemption Regulation could be applicable. However, because of precise elements of their wording, it is safer to draft the analysis following the interplay between the first and third paragraph of Art.101 TFEU. A first assessment revealed *prima facie* a non-collusive agreement as a new interoperability protocol would play a major role in paving the way to the Internet of Everything. Furthermore, the market of connectivity standards for IoT is still considered dynamic and competitive. Nevertheless, perhaps it is useful not to consider the IoT connectivity standard market at large but to restrict the analysis to the smart home IoT connectivity market. The popularity of some of the participants of the project might be a cause of problems in terms of access to this market of competitors and it is not sure that the efficiency gains, consumer share and the necessity exceptions can outbalance the impossibility to have access to competition on this market. To make a complete and thorough analysis at this moment seems difficult, as the CJEU has no case-law on connectivity standards concerning IoT and the application of Art.101(3) TFEU. Furthermore, doubts arise from the absence of any mention about how the free royalty fee would be possible if not on planning to share an indirect collective influent position on the home IoT products market, given the essentiality of this standard (probably involving SEP) for the production of home IoT objects. Despite the open source code, the absence of an SSO from the process makes it quite clear that this would become a *de facto* standard that has a chance to become the most used and it might give more substance to the competition concerns expressed before. Moreover, if declared anticompetitive, this project could be a new episode in the SEP saga, where the SEP patentee is not just one but a series of subjects that exercise a collective form of influence originated by a collusive agreement as far as its effects in the long run.

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD grant agreement No 814177.

References

[1] Lexinnova. Internet of Things: patent landscape analysis. Geneva: WIPO; 2014. P.1- 21

[2] 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). OJ L 119, 4.5.2016, p. 1-88.

[3] Podszun R. Standard Essential Patents and Antitrust Law in the Age of Standardisation and the Internet of Things: Shifting Paradigms. IIC International Review of Intellectual Property and Competition Law. 2019; 50(6):720-45.

[4] Project Connected Home over IP, https://www.connectedhomeip.com/ [25/03/2020]

[5] Perry S, Roda C. Chapter 5: The Internet of things. In: Perry S, Roda C, 1st, editors. Human rights and digital technology: digital tightrope. London: Palgrave MacMillan; 2016. p.131-62.

[6] Urquhart L, McAuley D, Avoiding the internet of insecure industrial things. Computer Law and Security Review. 2018; 34(3):450-66.

[7] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Green Deal. COM/2019/640 final, p.1-24.

[8] Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions, Secure 5G deployment in the EU, Implementing the EU toolbox. COM/2020/50 final, p. 1-14.

[9] NIS Cooperation Group. Cybersecurity of 5G networks and EU toolbox of risk mitigating measures. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures [25/03/2020].

[10] Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions, A new Industrial Strategy for Europe. COM/2020/102 final, p.1-13.

[11] Directive (EU) 2018/1972 of the European Parliament and the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast). OJ L 321/36, p.36- 214.

[12] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), PE/86/2018/REV/1. OJ L 151, 7.6.2019, p. 15-69.

[13] Gal M, Elikin-Koren N. Algorithmic Consumers. Harvard Journal of Law and Technology. 2017; 30(2): 309-52.

[14] De Conca S. From the glass house to the hive: the private sphere in the era of intelligent home assistant robots. IFIP. 2018;126: 282-98.

[15] Ali A, Awad A. Cyber and physical security vulnerability assessment for IoT based smart homes. Sensors, 2018; 18(3): 1-18.

[16] Serrenho T, Bertoldi P. Smart home appliances: state of the art. Energy, communications, protocols, standards. Brussels: JRC technical reports. 2019. p. 2-36.

[17] Chaudhuri A, Cavoukian A. The proactive and preventive privacy (3P) framework for IoT privacy by design. Edpacs. 2018; 57(1):1-16.

[18] Technopedia. What does Internet Protocol (IP) mean? https://www.techopedia.com/definition/5366/internet-protocol-ip [25/03/2020].

[19] Tridimas T. Fundamental rights, general principles of EU law and the Charter. In: Cambridge: Cambridge Yearbook of European Legal Studies. 2014; 16. p. 361-92.

[20] Jones A, Sufrin B, EU competition law. Texts, cases and materials. Oxford: Oxford University Press; 2016(3).p.114-256.

[21] Estevan de Quesada C. Collusive practices inside a business network: the case of information exchange. European Business Law Review, 2013; 24(6): 829-47.

[22] Consolidated version of the Treaty on the Functioning of the European Union. OJ C 326, 26.10.2012, p. 47-390.

[23] Toffoletto A, Stabilini A, De Giorgi et al. Part II. The application of the prohibitions-Italy. IEL Competition Law. 2019. p.123-234.

[24] Communication from the Commission - Notice - Guidelines on the application of Article 81(3) of the Treaty, OJ C 101, 27.4.2004, p. 97-118.

[25] Commission Regulation (EU) No 1217/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of research and development agreements. OJ L 335, 18.12.2010, p. 36-42.

[26] Commission Regulation (EU) No 330/2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices. OJ 23.4.2010, p.1-7.
[27] Communication from the Commission - Guidelines on the Application of Article 101 of the Treaty on the Functioning of the European Union to technology transfer agreements, OJ C 89,28.3.2015, p.3-50.
[28] Commission Regulation (EU) No 316/2014 of 21 March 2014 on the application of the Treaty on the Functioning of the European Union to categories of technology transfer agreements. OJ L 93,28.3.2014, p.17-23.
[29] Noto La Diega G. Internet of Things and Patents Towards the IoT Patent Wars? Journal of Commercial and Intellectual Property Law. 2017; 3(2):47-66.
[30] Petit N. Technology Giants, the Moligopoly Hypothesis and Holistic Competition: A Primer (October 20, 2016). SSRN: https://ssrn.com/abstract=2856502 or http://dx.doi.org/10.2139/ssrn.2856502 [25/03/2020].
[31] Conde Gallego B, Drexl J. IoT Connectivity Standards: How Adaptive is the Current SEP Regulatory Framework? IIC International Review of Intellectual Property and Competition Law. 2019; 50(1):135-56.
[32] Brook O. Struggling with Article 101(3) TFEU: Diverging approaches of the Commission, EU Courts, and five competition authorities. CMLR. 2019; 59(1):121-56.
[33] Mohan M. Ray of Hope for Airline Alliances: Consideration of Out of Market Efficiencies by the European Commission. Air and Space Law. 2014; 39(2):155-62.
[34] Crémer J, De Montjoye Y-A, Schweitzer H. Competition policy for the digital era, Brussels: European Commission; 2019. 2p.
[35] Kurgonaitė E, Treacy P, Bond E. Looking Back to the Future- Selective SEP Licensing Through a Competition Law Lens? Journal of European Competition Law and Practice. 2020; DOI: 10.1093/jeclap/lpaa003,1-14.
[36] Kasdan M. Chapter: Intellectual Property Licensing. In: Dreyfuss R, Pila J 1 editors. The Oxford Handbook of Intellectual Property Law. Oxford: Oxford University Press. 2018. p.653-63. DOI: 10.1093/oxfordhb/9780198758457.013.41
[37] Neurhor B. Dynamically Efficient Royalties for Standard Essential Patents. Journal of Competition Law & Economics. 2020;0(0):1-17, DOI: 10.1093/joclec/nhaa010.
[38] Pentheroudakis C, Baron J. Licensing Terms of Standard Essential Patents. A Comprehensive Analysis of Cases. Brussels: JRC. 2018. p. 84-110.
[39] Opinion of Advocate General Wathelet, *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH*, C-170/13, ECLI:EU:C:2014:2391.
[40] Judgment of the Court (Fifth Chamber) of 16 July 2015 *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH*, C-170/13, ECLI:EU:C:2015:477.
[41] Communication from the Commission to the European Parliament, the Council and the European Social and Economic Committee, Setting out the EU approach to Standard Essential Patents. COM/2017/712 final, p. 1-14.