Anglia Ruskin University
Faculty of Business and Law

Regulatory governance of ICT interoperability under EU law: Building up an appropriate policy framework

Mehmet Bilal Unver

A thesis in partial fulfilment of the requirements of Anglia Ruskin University for the degree of Doctor of Philosophy

Submitted: August 2019

Acknowledgements

Information and communication technologies (ICTs) and their legal and regulatory treatment have had a pioneering role in my academic life, along with several significant outputs up to date. This PhD thesis undoubtedly represents the most comprehensive and elaborate one among them, and I owe special thanks to many people for their support and assistance during this journey.

First and foremost, I would like to express my gratitude to my supervisor Prof. Rohan Kariyawasam for the spirit and support he has given me throughout this project. His insightful comments and feedback during my PhD kept me motivated and to revisit my former opinions and considerations towards more filtered findings. I am also grateful to Anglia Ruskin University for providing me with a full-fee waiver scholarship during the first three years of my PhD.

The support from my family, particularly my wife Saadet, helped me stand up to any hardship I faced during this four-year experience, especially at the times when I felt overwhelmed or exhausted. I am also indebted to my mother-in-law Saide Keles who deserves special thanks for the invaluable support she gave me and for her perseverance during this journey fraught with challenges.

On a personal note, I would also like to thank my PhD colleague Abderrezzaq Ghafsi who was more than a friend in his moral support and sharing his experiences with me during this process. Last but not least, I would like to share my gratefulness to Ahmet Darici for his allocating time regarding technical details and format, and Peter Gavigan for his proofreading, which extensively contributed to my writing and command of it.

Abstract

"Interoperability" means the ability for two different and independent ICT systems to exchange information and use that information. Having multi-dimensional aspects for the economy and society, the regulation of interoperability is the subject matter of various legal disciplines, i.e. intellectual property legislation, competition law and sector-specific rules e.g. the Electronic Communications Regulatory Framework (ECRF), under EU law. Lack of coherency among such disciplines is a compelling reason to find out the best possible rules to deal with the lack of interoperability and accompanying concerns, including vendor lock-in, switching costs, hindrance of innovation and information flows. On the other hand, each ICT industry has its own rules and standards, which also impacts interoperability. Against this background, drawing the boundaries for the regulation of ICT interoperability becomes more demanding.

This study aims to find out whether, or to what extent, ICT interoperability needs to be regulated under EU law, considering the abovementioned concerns. Starting with an investigation of the given legal disciplines with a focus on their measures dealing with lack of interoperability, this study primarily conducts blackletter (doctrinal) analysis based on multi-disciplinary research. After completing the blackletter analysis, the research continues with multiple case studies based on two emerging technologies 'cloud computing' and the 'Internet of Things' (IoT). These case studies relying on distinct industrial settings, have unravelled the real-life situation from the underlying architectural layers and their interdependencies. Cross analysis of the industrial settings, contributed to the doctrinal findings not only verifying but also advancing them with complementary results, pointing to meaningful and constructive outputs towards a holistic and layered regulatory treatment of ICT interoperability.

Overall, the research concludes with important findings regarding how to regulate ICT interoperability at the EU level. First and foremost, it has been established that the EU legal framework is of a limited nature, offering partial solutions and with shortcoming to the lack of interoperability. Secondly, it is found that interoperability is a concept not to be isolated from but to be elaborated with, other related concepts i.e. information flows, and problems i.e. gatekeeping, from a holistic and layered perspective. Thirdly, it has been ended up the ICT interdependencies, which have fully surfaced in the case study research, would be best addressed through a 'layered regulatory model' that can favourably respond to both ecosystem and non-ecosystem industrial settings. Fourthly, in dealing with the lack of interoperability and related concerns, the term 'gatekeeping' has been revitalised and embedded into this layered model, invigorating this holistic and ex-ante policy approach. Last but not least, the proposed 'layered regulatory model' would not only replace the core principles of the ECRF but also expand the EU regulatory vision with the necessary flexibility to cope with the ever fast changing ICT dynamics, going beyond interoperability-based problems.

Keywords: ICT, interoperability, competition, regulation, layering, gatekeeping.

Table of Contents

List of Abbreviations

3G	Third-Generation Wireless
4G	Fourth-Generation Wireless
5G	Fifth-Generation Wireless
ABS	Anti-Lock Braking Systems
AGCM	Autoria Grante della Concorrenza e del Mercato
AI	Artificial Intelligence
AMR	Automated Meter Reading
ANSI	American National Standards Institute
ANT	Adaptive Network Topology
APIs	Application Programming Interfaces
AVB/TSN	AVnu Alliance
AWS	Amazon Web Services
BEREC	Body of European Regulators of Electronic Communications
BSD	Berkeley Software Distribution
CAGR	Compound Annual Growth Rate
CAS	Conditional Access System
CD	Compact Disc
CDMI	Cloud Data Management Interface
CDN	Content Delivery Network
CDPA	UK Copyright, Designs and Patents Act
CMLR	Common Market Law Report
CoJ	Court of Justice of the European Union
Commission	European Commission
CP	Content Provider
CPU	Central Processing Unit
CREATE	UK Copyright and Creative Economy Centre
CRM	Customer Relationship Management
DMCA	Digital Millennium Copyright Act
DRM	Digital rights management
DSM	Digital Single Market
DT	Deutsche Telekom

DVD	Digital Versatile Disk
ECIS	European Committee for Interoperable Systems
ECMA	European Computer Manufacturers Association
ECRF	Electronic Communications Regulatory Framework
ECS	Electronic Communications Service
ECU	European Currency Unit
EDGE	Enhanced Data GSM Environment
EEA	European Economic Area
EEC	European Economic Community
EECC	European Electronic Communications Code
EIF	European Interoperability Framework
EPC	European Patent Convention
EPG	Electronic Programming Guide
EPO	European Patent Office
ERG	European Regulators Group
ETSI	European Telecommunications Standards Institute
EU	European Union
EUMR	European Union Merger Regulation
FAGMA	Facebook, Apple, Google, Microsoft and Amazon
FOSS	Free and Open Source Software
FRAND	Fair, Reasonable and Non-Discriminatory
FTC	Federal Trade Commission
GC	General Court
GDPR	General Data Protection Regulation
GPL	General Public License
GSM	Global System for Mobile Communications
GSR	Global Symposium for Regulators
GUI	Graphical User Interface
HTTP	Hyper Text Transfer Protocol
HVAC	Heating, Ventilation and Air Conditioning
IaaS	Infrastructure as a Service
IACC	International Advance Computing Conference
IAS	Internet Access Service
IATA	International Air Transport Association

Ibid	Ibidem
IBM	International Business Machines
ICS	Inter-personal Communications Service
ICT	Information and Communications Technology
IE	Internet Explorer
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
iOS	iPhone Operating System
IoT	Internet of Things
IP	Internet Protocol
IPR	Intellectual Property Right
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ISOC	Internet Society
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunications Union
JIPITEC	Journal of Intellectual Property, Information Technology and E-Commerce Law
LAN	Local Area Network
LLU	Local Loop Unbundling
LoRa	Long Range
LTE	Long-Term Evolution
M&A	Merger and Acquisition
M2M	Machine-to-Machine
MCR	Merger Control Regulation
MCU	Multi-Point Control Unit
MIT Press	Massachusetts Institute of Technology Press
MNC	Mobile Numbering Code
NES	Nintendo Entertainment System
NFC	Near Field Communication
NGN	Next Generation Network

NIST	National Institute for Standards and Technology
NRA	National Regulatory Authority
OCF	Open Connectivity Foundation
OCS	Online Communications Service
OECD	Organisation for Economic Co-operation and Development
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
ONP	Open Network Provision
OS	Operating System
OSI	Open Systems Interconnection
OSS	Open Source Software
OTA	Over-the-Air
OTT	Over-the-Top
OUP	Oxford University Press
OVF	Open Virtualization Format
P2P	Point-to-Point
PaaS	Platform as a Service
PC	Personal Computer
PSAP	Public Safety Answering Point
PSN	Professional Social Networking
PSTN	Public Switched Telephone Network
PTT	Postal Telegraph and Telephone
QoS	Quality of Service
QWERTY	Standard computer or typewriter keyboard
RAND	Reasonable and Non-Discriminatory
RAR	Roshal Archive
RFID	Radio Frequency Identification
RtDP	Right to Data Portability
SaaS	Software as a Service
SAP	Systems, Applications & Products
SDK	Software Development Kit
SDN	Software Defined Networking
SEP	Standard Essential Patent
SIEC	Significant Impediment to Effective Competition

SIM	Subscriber Identity Module
SME	Small and Medium-sized Enterprise
SMP	Significant Market Power
SSNIP	Small but Significant and Non-Transitory Increase in Price
SSO	Standard Setting Organisation
SSRN	Social Science Research Network
SSV	Software Security Vendor
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TEEC	Treaty Establishing the European Community
Telco	Telecommunications company
TFEU	Treaty on the Functioning of the European Union
TILEC	Tilburg Law and Economics Center
TIP	Telepresence Interoperability Protocol
TPM	Technology Protection Measure to control use of copyrighted work
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
TSM	Telecom Single Market
UMTS	Universal Mobile Telecommunications System
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
US	United States
USB	Universal Serial Bus
VCS	Video Communications Solution
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
W3C	World Wide Web Consortium
WCT	WIPO Copyright Treaty
Wi-Fi	Wireless Fidelity
Wi-Max	Worldwide Interoperability for Microwave Access
WIPO	World Intellectual Property Organization
WLAN	Wireless Local Area Network

WMP	Windows Media Player
WPL	World Programming Ltd
WTO	World Trade Organisation
WWW	World Wide Web
XML	Extensible Markup Language

Copyright declaration

I declare that my thesis consists of 81,902 words.

List of Figures

List of Tables

1. Introduction

1.1. Background and purpose of the research

"Interoperability" is defined as "the ability to exchange information and mutually use the information which has been exchanged".[1] It has a crucial meaning for the information and communication technologies (ICTs),[2] which is an umbrella term used to mean any technological platform, device or application by which the "information" is created and shared. Electronic file and mail exchanges, video streaming, music downloads are realised through *interfaces*[3] that enable interoperability between software/hardware components of non-homogenous ICT systems. Interoperability is generally considered to promote socially desirable goals such as fostering competition and innovation, enhancing consumer satisfaction, and promoting economic growth.[4] Lack of interoperability would have significant consequences for the society and economy, with potential restraints over competitive and innovative market forces. Closely related to this, 'interoperability' is governed by means of many rules and precedents concerning intellectual property rights (IPRs), competition law and sector-specific (electronic communications) regulations.

---

1 Directive (EC) 2009/24 of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs [2009] OJ L 111 ('Software Directive'), recital 10.

2 Although ICT might have various meanings peculiar to the context, this study uses this term to cover all kinds of (analog/digital) technologies used to create and share information depicting the underlying networks and services. For detailed information about the ICTs including nature and evolution of the underlying (ICT) networks/services, see the section '2. Interoperability in the field of ICTs' below.

3 To achieve interoperability, interfaces must be accessed and/or be already opened to third parties in three forms: application programming interfaces (APIs), protocols, and data file formats (Malcolm Bain, 'Patents and FOSS' in Noam Shemtov and Ian Walden (eds), *Free and Open Source Software* (OUP 2013) 161; Robert S. Sutor, 'Software Standards, Openness, and Interoperability' in Laura DeNardis (eds), *Opening Standards: The Global Politics of Interoperability* (The MIT Press 2011) 215.

4 Pamela Samuelson, 'Are Patents on Interfaces Impeding Interoperability', [2009] 93 Minnesota Law Review 1943, 1943-1944.

Each body of the legal regulations have different objectives and means to accomplish such objectives, which have distinctive features. While IPR rules aim to encourage original creations, certain types of IPRs i.e. patents, copyrights, trademarks offer pre-defined tools and mechanisms to protect IPR holders against unauthorised uses by third parties. European Union (EU) competition law focuses on consumer welfare and protecting competition usually through punitive ex-post interventions, such as remedies addressing 'abuse of dominance'. As far as the electronic communications regulatory framework (ECRF)[5] is concerned, a more complicated body of rules is figured based on more specific objectives e.g. ensuring 'end-to-end connectivity', as well as ex-ante powers handed over to the regulators, revealing a more intrusive and straightforward nature, also reflected in dealing with the lack of interoperability.

Lack of interoperability causes some problems, often surrounding the concept of *lock-in,*[6] which is reflected in the consumers' inability to switch to one platform from another or a competitor being kept out of the market because of the network effects and/or path dependence.[7] Interoperability might have either positive or negative co-relation with the

---

5 Among the sector-specific regulations, the ECRF is the most relevant example regarding ICT interoperability as embodying ex ante tools and mechanisms to deal with the interoperability. Going beyond interoperability and entailing a great many issues (e.g. authorization, universal service, consumer rights, access and competition), the ECRF represents the mainstream regulatory framework with regards to regulation of the ICT networks/services. While it originates from the 2002 regulatory framework consisting of 5 main directives (as well as regulations, recommendations, etc.), 4 of these directives were consolidated recently (December 2018) under a single directive titled the 'European Electronic Communications Code' (EECC). For more details and distinctive aspects of the ECRF, see the section '6.1. Main elements of ECRF'.

6 Lock-in occurs in the case when users are confronted with a walled garden (i.e. proprietary platform) under which they are forced to use one company's products which might be incompatible with those of competitors. Lack of interoperability is one of the driving strategies for (vendor/technological) lock-in, particularly on the part of dominant players. For more information regarding vendor/technological lock-in, see the section '3.1.2. Main concerns surrounding lack of interoperability'.

7 Network effects mean an increase in a product's value when the number of the users of that product is multiplied, representing more connected consumers to the same network. High-technology markets well represent strong network effects. For detailed information about network effects and the accompanying path dependencies see the section '2.1.5. Network effects'. There is also an apparent link between the network effects and the vendor lock-in. For products with network effects (the purchase of a product increases its value to existing purchasers), greater sales volumes can increase the likelihood of consumers being locked into existing suppliers - especially if the

network effects. Dominant firms usually try to create their (firm-level) network effects and limit the interoperability to the extent that enables them to maximize brand loyalty and customer base. This strategy often contrasts to industry-level network effects and wider benefits to be reaped from broader interoperability. No legal system attempts to optimize the level of interoperability. Notwithstanding, diverse legal and non-legal rules and fragmented markets increasingly pose interoperability-based problems, which would have far-reaching implications e.g. not only economics based (mostly competition oriented) outcomes, but also further consequences related to hindered information flows. In conjunction with this, a set of concerns being drawn at the outset of this study shed a broader light on the interoperability discourse and demonstrate that ICT network/service providers tend to erect artificial gateways to control access and interoperability, resulting in gatekeeping roles and functionalities.[8]

While interoperability is by and large is attributed to lock-in and related problems e.g. switching costs, potential problems need to be extended to social production and democratic culture within and across the societies. In particular, with the advent of the digital technologies as well as internet connectivity, lack of interoperability would mean lack of communication and information channels across different platforms, apps and services. While the end-to-end connectivity is based on the global communication standards and an interoperable landscape, this is not the case when we mention about the media and information flows particularly when protected with the IPRs. The resultant picture would be better captured by the term 'gatekeeping' based on the lack of interoperability and surrounding problems. From this point of view, the

supplier uses non-standard interfaces and sells complementary services (Ian Brown, 'Regulations and the Internet of Thing (IoT)', (2015) GSR15 discussion paper, 23 <http://www.itu.int/en/ITU-D/Conferences/GSR/Pages/ GSR2015/GSR15-discussion-paper.aspx> accessed 9 October 2020).

[8] See the sections '3.1.3. Brief analysis of major concerns on the cumulative ground of 'gatekeeping''and '8.4.2. Revitalising gatekeeping and gatekeeping activities'.

thesis invokes this term to explain the interoperability related concerns and problems on a cumulative ground. Conversely, distinct bodies of law fragment such problems providing for crystallised tools and means. Most remarkably, the EU legal system offers distinctive solutions originating from different legal bodies, which mostly consider 'lack of interoperability' as a subordinate problem to other widely acknowledged matters of concern.

For instance, IPR rules mostly have an indirect and passive impact over interoperability i.e. limited to 'reverse engineering' under copyright regime, not securing a guaranteed access to the interfaces that ensure interoperability between the computer programs. Competition law measures, based on Articles 101-109 in the Treaty on the Functioning of the European Union (TFEU), are invoked to ensure and enhance interoperability in case of the anti-competitive effects, e.g. likelihood of market foreclosure. After fulfillment of certain thresholds and criteria, such practices could be addressed by the competition law remedies, including mandatory sharing (access/interoperability) and pricing obligations imposed on the dominant market players. This could be exemplified by the Commission's *Microsoft* decision whereby certain interface specifications are mandated to be disclosed to ensure viable competition in the server operating system (OS) market. Under the ECRF, the legal logic and framework differs in the sense that the consumers are put to the center, although competitive mindset is still kept and combined with the tools to protect consumer interests. Thereunder exist certain ex-ante obligations and measures, e.g. regarding 'interconnection' and 'conditional access', which constitute a consolidated framework along with partial solutions concerning 'interoperability'.

This dissertation attempts to revisit the EU legal framework and ultimately aims to refashion the applicable rules and regulations with a view to deal with the lack of

interoperability and accompanying problems. Thereby, it is aimed that major concerns are clarified, the existing loopholes are unravelled, and the appropriate tools are developed to cope with the interoperability-based problems. This study aims not to crystallise interoperability problems in technical terms, but to embrace them from a broader perspective of legal regulation on a sound and widely applicable basis. In this regard, a multi-disciplinary (doctrinal/traditional) legal research is done along with the multiple case studies based on Cloud Computing and Internet of Things (IoT), which represent the ever-faster growing technologies that have the potential to challenge the current ICT regulations, including interoperability rules and solutions. Having said that, and to be built on the findings of both the doctrinal analysis and case study research, it is intended that a policy approach be developed and ending up with a new regulatory model based on a normative perspective.

1.2. Context, perspective and research questions

At the core of this study lies the debate as to whether and to what extent interoperability information, basically application programming interfaces (APIs), would be the subject matter of regulatory concerns and interventions. To respond to this question, this study endeavours to search out the existing EU regulations based on the tripartite legal framework, incorporating IPR rules, competition law and sector-specific regulations. In this regard, Chapters 4, 5 and 6 are dedicated to multi-disciplinary legal research, starting with the IPRs and proceeding with competition law and the ECRF rules. In so doing, both the distinctive and overlapping aspects of the related EU legal regimes are investigated, ending up with a coherent and holistic perspective. Out of this research, the findings denote insufficient and partial interoperability solutions, which are summarised below.

Within the context of IPR rules, the abovementioned limitedness is noticeable under Software Directive 2009/24/EC, which regulates the conditions, scope and limits of the copyright regime for computer programs in the EU. For instance, decompilation (a type of reverse engineering)[9] is legally justified only for the purpose of achieving 'interoperability' under Software Directive.[10] However, this exceptional right is unique to copyright protection[11] and reveals a costly solution for the software developers, which does not match the benefits of the open standards or common protocols. These latter options could be realised through opening the APIs, which are however protected by the copyrights[12] alongside other potential IPRs e.g. patents. A practical result is the fact that a human-readable form of computer programs (source codes) could be identified just by reverse engineering; yet, this is not a sustainable and long-term business model.[13]

This discrepancy, between acknowledging interoperability as a reason for decompilation and the copyrightability of APIs, reinforces the idea that IPRs could be used as an effective shield over the APIs. Not only copyrights, but also patents and trade secrets are effectively used to prevent third parties (e.g. software developers) from having access to the key interfaces, which would otherwise allow competitive markets for derivative products. Firms may seek the protection of patents for interface

---

9 Regarding the definition, scope and purpose of 'reverse engineering' and of 'decompilation', see the section '4.1.2. Reverse engineering and ensuring interoperability under EU copyright law'.

10 See the Software Directive, recital 15 and art 6.

11 EU copyright rules for computer programs just allow interoperable solutions under the strict conditions of 'reverse engineering' which is translated as 'the right to decompilation' under the Software Directive. On the other hand, neither the EU patent regime, nor other IPRs, have such an unequivocal right enabling interoperability.

12 Under the EU legal system, whereas *ideas and principles* that underlie a software are excluded from copyright protection (enshrined by the Software Directive), APIs are not covered under this exemption. The ruling in *SAS Institute Inc v World Programming Ltd* affirmed neither the functionality of a computer program, nor the programming language and the format of data files used in a computer program constitute a form of expression and accordingly do not enjoy copyright protection under the EU Software Directive, while APIs are not contained within the same category of an un-copyrightable form of ideas (Case C-406/10 *SAS Institute Inc v World Programming Ltd* [2012] 3 CMLR 4).

13 See Sally Elizabeth Weston, 'The Legal Regulation of Interoperability in an Oligopolistic Market' (PhD thesis, Bournemouth University 2015), 35.

designs for anti-competitive purposes, that is, as a tool for blocking competitors from developing compatible platforms (e.g. game consoles) for controlling the market for complementary products (e.g. videogames).[14] However, this turns out to create an environment conducive to the gatekeeper positions for the protected software, and threatening consumer benefits to be derived from follow-on innovation. That being said, if the aftermarket(s) build on a proprietary platform, which is encumbered by IPR-protected APIs that deter third-party access/interoperability, the ultimate goals of IPRs, particularly the end of 'follow-on innovation', becomes compromised.

Lack of interoperability would likewise pose a situation in contradiction with the competition law aims. This is more persuasive from the perspective of enabling aftermarket competition and enhancing consumer surplus. Particularly, exclusionary abusive conducts, e.g. the refusal to supply interoperability information, perpetuated by dominant players, would create lock-in that is hazardous to consumer welfare, thus creating a contradiction with the EU competition rules. This concern has so far led the EU Courts and the Commission to intervene into many cases by mandating access to interface specifications, such as in *Microsoft.*[15] Not only refusal to deal, or other abusive behaviours, but also collaborative and concentrative undertakings are comprehended by the EU competition law tools, when they affect competitive markets by degrading intra, or inter platform, interoperability. Clearly, while interoperability is not an aim of the EU competition law by itself, it emerges as an important means to break off lock-ins and to eliminate anti-competitive effects e.g. caused by the network effects.

---

14 See Samuelson (n 4) 1979.

15 Case COMP/C-3/37.792 - *Microsoft* [2004] OJ L 32/23 ('Commission's *Microsoft* decision'), upheld in Case T-201/04 *Microsoft v Commission* [2007] ECR II-3601 ('GC's *Microsoft* judgement').

While IPR rules aim at protection of original creations, technical inventions etc. by encouraging product differentiation and innovation, competition law rules underscore consumer welfare, often through effectively competitive markets. Out of the interactions between these two bodies of law, conflicting results would come up in the sense that IPR exceptions, including reverse engineering, would not permit incrementally created innovations, as opposed to the competition law interventions. Although no hierarchical relationship exists between the two, under certain circumstances the latter might have a superior effect by dictating mandatory sharing or interoperability, particularly where the former (IPR rules) is not responsive and/or capable enough. On the other hand, an obligation by competition law measures might be problematic in scope and effect, such as in the *Microsoft* case where the antitrust standards were unevenly changed and false positive debates inflamed.[16] Last but not least, accompanying lengthy processes have the potential to cause prohibitive costs for the market players should they rely on the interoperability information and seek a regulatory response.

After all, the question emerges as to whether the emergent gap would be filled by the ECRF rules. The ECRF rules and measures consist in far more crystallized rules that enable a number of end-goals and ensuing interoperability based remedies in several contexts. In this regard, ensuring adequate access and interconnection is of high importance, as this goal requires industry-wide interoperability e.g. enabling the end-users to communicate with each other. In the absence of such rules, end-to-end

[16] Inge Graef, 'Tailoring the Essential Facilities Doctrine to the IT Sector: Compulsory Licensing of Intellectual Property Rights after Microsoft' [2011] 7 Cambridge Student Law Review 1, 18; Alan Devlin, Michael Jacobs and Bruno Peixoto, 'Success, Dominance and Interoperability' [2009] 84 Indiana Law Journal 1157, 1177. See also Kathryn McMahon, 'Interoperability: "Indispensability" and "Special Responsibility" in High Technology Markets' [2007] 9 Tulane Journal of Technology and Intellectual Property 123, 161-6, where the author underlines that the approach followed in *Microsoft* focused on the "distortion of market structure" rather than foreclosure and anti-competitive effects with an implication of "imposition of special responsibility" (emphasis added).

connectivity would no longer exist, having far-reaching negative outcomes, which could be extended to the provision of EU-wide communications services and cross-network online transactions. While this end-goal goes beyond the competition law and IPR-oriented rules with a stricter agenda and safeguards, the reflections on interoperability regulations are limited under the ECRF. That is to say, interoperability remedies are envisaged to realise certain ends, including voice-based/conventional interconnection, conditional access to the set-top boxes, etc. and do not reach out to overall ICT services and networks e.g. interconnection of software governed platforms, being limited to electronic communications networks and services.

Under this light, an increasing need arises concerning more effective tools to ensure ICT interoperability under the EU legal system. Incorporating various concerns based on technological lock-in, switching costs, network effects, etc., this featured need has significant repercussions for a 'holistic' ex-ante approach against the shortcomings of competition law and IPR rules. This tentative conclusion reflects the general findings of the multi-disciplinary blackletter analysis done in Chapters 4, 5 and 6, which primarily seek to answer whether and to what extent interoperability-based problems are addressed under the *status quo*. In this context, not only the insufficiency of the existing solutions, either statutory or based on case law, against the major concerns surrounding ICT interoperability, but also the non-holistic character of the available rules and regulations is underscored as a deficiency of the EU legal system.

Whilst examination of the EU legal framework represents the first step, this (both 'descriptive' and 'exploratory') analysis poses a need for filtering through an additional analysis based on the real-life (industrial) practices. To have a more elaborate picture of the legal framework vis-à-vis the ICT industries, case study

research has been considered crucial against the plausible need for a holistic and ex ante regulation. That is to say, it is acknowledged that the tentative conclusion of Chapters 4, 5 and 6 needs to be verified and enriched by the case studies. To that effect, "cloud computing" and "IoT" have been selected for the purpose of case study which constitute the subject-matter of Chapter 7. The analytical lens used in the multiple case studies has been broadened in Chapter 8 (Conclusion) to take a further step towards finding out the appropriate policy approach and regulatory model.

Against this background and contextual analysis, several research questions emerge, including but not limited to: (i) Would the existing EU legal framework be sufficient to deal with the lack of interoperability and related concerns such as vendor lock-in, hindered innovation and information flows in the field of ICTs? (ii) What kind of a policy approach (ex-ante or ex-post; holistic or disaggregated; bottom-up or top-down) would be appropriate in dealing with the lack of interoperability and accompanying problems that characterise the emerging ICT landscape? (iii) What elements or responsive tools would need to be incorporated for the regulation of ICT networks/services and ultimately to be embedded in a regulatory model?

While some more questions would be added on top, these research questions represent the major/pioneering ones. Among these, while the first one is addressed under the blackletter/doctrinal analysis, appropriate responses to the other two questions are mostly found out during and subsequent to the case study research. Thus, these two research components of blackletter analysis and case studies have 'complementary' aspects within this study. For instance, significant inputs are drawn from the initial (blackletter) analysis towards the holistic 'policy approach' in the sense that very nature and would-be characteristics of this approach have started to emerge. Along the

same lines, completion of the case studies has brought out a significant contribution to the construction of the 'regulatory model' based on the 'layering' approach. Drawing a set of progressive steps, all the components of the research could be found in Figure 1 below.

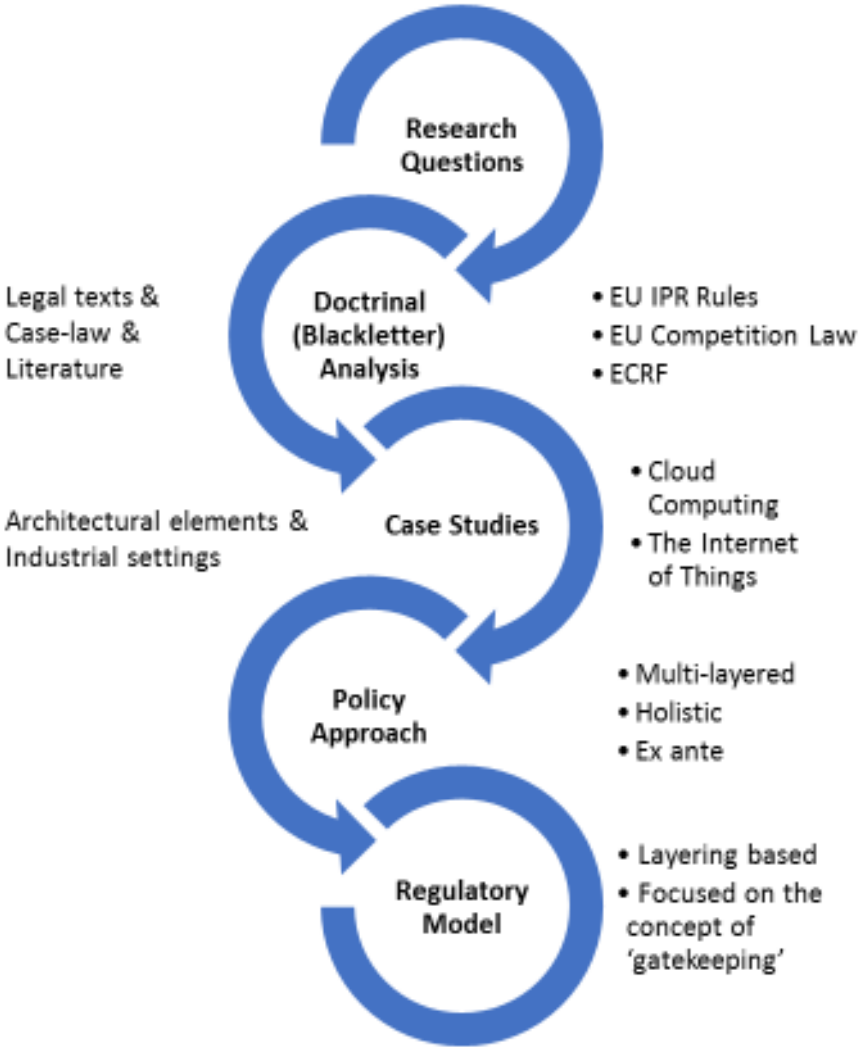

Figure 1: Progressive steps of the research

Source: Constructed by the author

1.3. Research methodology

The research methodology pursued in this study is built upon the combination of 'doctrinal (blackletter) analysis' with 'case study' research. The former (doctrinal) analysis aims to examine the relevant legal texts and case law, as well as secondary sources like books, journal articles, working papers, reports and newsletters, in seeking to discuss and clarify the scope and boundaries of the EU legal framework concerning ICT interoperability. On the other hand, the latter (case study) research has been employed in order to expand and enrich the findings of the former analysis towards the designation of the policy approach and development of the regulatory model in the end. It is envisaged that on the 'positive' ground of the doctrinal analysis, the multiple case studies would bring out new 'normative' elements along with new inputs as to the intended regulatory design.

Based on the combinative approach explained above, this study aims to find out whether current rules and precedents under EU law are sufficient to cope with the highlighted concerns given the real-life situations, with a view to build up an appropriate regulatory model. To that effect, the multiple cases worked out in Chapter 7 lay the groundwork to reach out to new outputs concerning a pertinent regulatory approach, as well as to validate the former findings.[17] Given this fact, this study could arguably be said to employ both 'deductive' and 'inductive' logic in its endeavour to

[17] These two components are important in the sense that case study researchers are supposed not just to make an in-depth analysis of real-life situations, but also to reach out to tested and generalisable theoretical propositions based on rigorously selected cases and well-structured design. While the theoretical propositions need to be incorporated into the case study research, construction of a new generalisable theory or normative framework is also expected to come up following the case studies. This approach results in placing more emphasis on inductive exploration, discovery, and in holistic analysis presented in thick descriptions of the cases (Helena Harrison, Melanie Birks, Richard Franklin and Jane Mills, 'Case Study Research: Foundations and Methodological Orientations', (2017) 18 Forum: Qualitative Social Research <http://dx.doi.org/10.17169/fqs-18.1.2655> accessed 9 October 2020).

filtering out the appropriate policy approach, based on both the doctrinal findings and case study research. Notwithstanding, the 'inductive' aspects come to the fore as the consecutive steps followed in the study draw up a progressive research ending up with a new regulatory model.

From this viewpoint, the constituent elements of this research effectively complement each other. The initial aim followed in Chapters 4 - 6 has been to elaborate the EU rules and precedents concerning ICT interoperability. In this regard, existing rules, remedies and mechanisms prevailing under IPR rules, competition law and sector-specific regulations are investigated with the aim to identify the loopholes existing in the EU framework. This multi-disciplinary (doctrinal) analysis, although having the potential for elaborate outputs,[18] might be limited and insufficient on its own to build up a new regulatory model intended to apply to a very broad context like ICTs, given the descriptive nature of this research. In fact, identification of causal mechanisms would be more clarified through case studies, which generally seek to take account of as much as possible about a given phenomenon and, thus, are likely to capture the processes that link various factors to one another in time.[19]

This study thus attempts to surmount any potential limitedness of blackletter analysis with the aid of case studies,[20] filtering out the real-life scenarios, in combination and

---

18 Regarding the details of doctrinal analysis and its interplay with non-doctrinal research methodologies, see Terry Hutchinson 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law' 3 [2015] Erasmus Law Review, 130-138.

19 Lisa L. Miller, 'The Use of Case Studies in law and Social Science Research', [2018] 14 Annual Review of Law and Social Science 381, 385.

20 It is acknowledged that when information is plentiful and concepts abstract, it is important to utilize processes that help interpret, sort, and manage information and that adapt findings to convey clarity and applicability to the results (Harrison et al (n 17)). Likewise, Yin asserts that, "a case study is an empirical method that

- investigates a contemporary phenomenon (the "case") in depth and within its real-world context, especially when
- the boundaries between phenomenon and context may not be clearly evident" (Robert K. Yin, *Case Study Research and Applications: Design and Methods* (6th edn, Sage 2018), 15.

interplay with the former analysis. Thereby, not only is the integrity of the research components, but also the anticipation of progressive research outputs, maintained. Notwithstanding, it is worth underlining that the doctrinal analysis in this study has gone further than the pure description of the law, in the particular sense that it unravels the narrow mindset and fragility of the EU legal framework against the ICTs and their interoperability and upholding a holistic viewpoint for the layered technologies. This tentative conclusion towards holistic and multi-layered policy approach has served as the stepping-stone for the following case study research. Case study research, delving into the real-life scenarios and interactions between the ICT layers and players, has laid the ground for the development of a regulatory model in the end. Given the structure, scope and purpose of the overall research, below it is explained what particular meaning and characteristics the selected cases have within the meaning of methodological approach.

1.4. Case selection

Primarily exploratory and explanatory in nature, case study is used to gain an understanding of the issue(s) in real life settings and is recommended to answer 'How' and 'Why', or less frequently 'What', research questions.[21] Following this spirit, case study research in this thesis has been conducted to exemplify, search and shape out the interoperability-based problems, along with the possible solutions for the real-life situations. By looking at the most representative cases of the multi-layered ICT interoperability, this study aimed to combine the positive findings of the doctrinal analysis with real-life constructivism. This 'constructivist' approach reminds one of,

[21] Helena Harrison et al (n 17). See also Yin (n 20) 13; Gary Thomas, *How to do your case study* (2nd edn, Sage 2016), 36-37; Malcolm Tight, *Understanding Case Study Research: Small-scale Research with Meaning* (Sage 2017) 45-49.

and resembles the approach of, Merriam, who acknowledges that case study research can use both quantitative and qualitative methods and that when working on qualitative case studies, methods aim at generating inductive reasoning and interpretation, rather than testing hypothesis.[22]

From this viewpoint, this study attempts to use the case studies primarily to take a further step towards the investigating and filtering of the industrial settings and practices, in order to find out whether interoperability is a stand-alone concept and could be achieved by self-regulatory mechanisms or it does need coercive means to cope with the surrounding problems access seekers face. That being said, case studies have been conducted for two main reasons; namely, to search out (i) to what extent the plausible need for a holistic policy approach has a matching response from the industrial settings (more *relativist*), and (ii) what regulatory repercussions ICT interoperability would have in the selected industrial settings (more *interpretivist and constructivist*).

In particular the latter question involves an 'inductive' logic and endeavour, in the sense that details of the intended holistic regulatory model are aimed to be built upon the revelatory aspects of the case studies. Within this context and rationale, 'Cloud Computing' and the 'Internet of Things' have been selected as to constitute the backdrop for the case study research. Below, brief information about these two technological phenomena (cases) are given.

---

[22] Harrison et al (n 17), referring to Sharan B. Merriam, Qualitative research: A guide to design and implementation (2nd edn, Jossey-Bass 2009). Remarkably, Yin, a pioneering figure in this field, advocates a structured process concerning case study research and focused on the formal propositions and theoretical foundations, his realist and sometimes deterministic approach is contrasted with other scholars' constructivist, pragmatic and/or interpretivist methodological approaches. For more details regarding the philosophical variations of case study approach incorporating realist - postpositivist / pragmatic - constructivist / relativist - constructivist/interpretivist approaches, see Harrison et al (n 17).

1.4.1. Cloud Computing

Cloud computing, broadly speaking, is the storage of data and processing in a location which is not the user's own computer, or the provision of computer resources on-demand over the internet.[23] Cloud facilities offer many advantages to users, such as remote storage, easy and ubiquitous accessibility, the storage or processing of (very) large amounts of data which would not be possible on a user's device, the opportunity to collaborate with other users privately and remotely etc.[24] The central feature of cloud computing is that existing and novel computing applications are increasingly being performed in a "cloud' online, e.g. not on users' own hardware.[25] Cloud computing is thus considered as a new wave of technological development combining different services in a manner that arguably revolutionizes computer and internet usage.[26]

In providing cloud services e.g. storage, security, messaging, reporting, cloud providers rely on the physical link and broadband connectivity provided by the internet service providers (ISPs).[27] They also use and rely on additional software and hardware elements taken from the software developers, virtualisation providers, vendors e.g. original equipment manufacturers (OEMs) and security (anti-virus) companies. All these latter services could be classified as the internal elements within the cloud architecture, constituting the major cloud layers of applications, platform and

23 Angela Daly, *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart Publishing 2016) 120.
24 Ibid.
25 Jasper P. Sluijs, Pierre Larouche and Wolf Sauter, 'Cloud Computing in the EU Policy Sphere: Interoperability, Vertical Integration and the Internal Market' [2012] 3 JIPITEC 12, 13.
26 Ibid.
27 Mehmet Bilal Unver, 'What cloud interoperability connotates for EU policy making: Recurrence of old problems or new ones looming on the horizon?' [2019] 43 *Telecommunications Policy* 154, 155.

infrastructure. Whereas, the broadband connectivity between the cloud facilities and the users, as well as the internet hubs, is referred to as the external access/network layer underlying these cloud layers.[28]

Against this background, cloud interoperability represents a common thread across the internal/external layers that constitute the cloud architecture. To mention a fully-fledged cloud interoperability, cloud users should be able to exchange, port and use their data, applications and software tools across different clouds. This could be enabled by means of cross-layer interoperability within and across the cloud systems. Hence, achievement of cloud interoperability needs to be secured across all the layers, e.g. application, platform, infrastructure. However, proprietary protocols and the absence of common standards in the cloud industry would prevent this and preclude the interoperability across the distinct cloud systems. As a matter of fact, there is only one standard, that of Open Virtualization Format (OVF), adopted by the industry stakeholders, which is commonly used by the cloud providers and truly fitting into the meaning of 'common standard'.

All the facts mentioned above, point to a need to make research of this subject matter, namely 'cloud computing' in relation to interoperability. This selection would enable a fulfilling analysis, concerning not only the possible scenarios based on (non-)interoperability and the accompanying legal and non-legal solutions, but also of the potential causal mechanisms that would pave the way for construction of a regulatory model. Related to this, cloud-based interdependencies are also note-worthy from the holistic perspective featured in this study. That is to say, cloud computing offers a

[28] For detailed information regarding internal/external elements, or layers of the cloud architectures, see the section '7.1.2. Technical and economic underpinnings'.

fertile environment for the examination of the cross-layer interactions and accompanying interoperability gaps and problems, allowing a generalisable picture for the regulatory design. Given this fact, cloud computing has been selected as one of the cases to be examined on top of the doctrinal analysis.

1.4.2. The Internet of Things

The Internet of Things (IoT) represents another fertile and dynamic environment for the analysis of interoperability related problems. A world of networked smart objects, including cars, refrigerators, health care services, wearable devices are depicted by the term the 'IoT', which builds and thrives on diverse industrial settings e.g. home appliances, smart city, transport, logistics, agriculture, traffic management, monitoring of production cycles and telemedicine. In such a landscape, the IoT devices and the governing software are distinguished through data sensors e.g. RFID chips, that communicate constantly and seamlessly with each other. On top of this, Internet Protocol (IP) connectivity makes the IoT platforms more effective, responsive and data-driven e.g. coupled with big data management. Global figures show that connected products and devices have already exceeded the global population and are expected to reach 50 billion by 2020, up from 25 billion in 2015.[29] Given this fact, the IoT seems to mark a distinctive revolution along with cloud computing, which supplies the necessary platforms, software tools and applications that are necessary for processing the data gathered from the smart/connected things.

[29] KPMG, *Securing the benefits of industry digitisation* (A Report for Vodafone, 2015) 5 <https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2017/02/vodafonewebaccess.pdf> accessed 9 October 2020.

Against this background, cloud services underlie the IoT platform and applications in general. The IoT also relies on other supportive or underlying networks and services e.g. broadband connectivity and local area networks, which represent access and perception layers. On top of these, applications are run, revealing another layer that needs to speak to the lower layers. Interoperability across these layers of perception, access and cloud and application is inherent in the concept of the IoT. Meaning, for an IoT system, all these layers need to operate in a systemic and organised manner, based on the agreed standards.

From a broader perspective, absent or hindered interoperability could discourage IoT users, including manufacturers, from purchasing new products and, at the extreme, fully stop them using the IoT devices.[30] Notwithstanding, the IoT industry is currently driven more by proprietary standards than by open standards.[31] Google (Brillo and Weave), Samsung (SmartThings), Apple (HomeKit) and Amazon (Alexa) run their unilateral programs to bring out new IoT solutions,[32] which seem to dominate the IoT landscape,[33] as these market players have a great many leverages to attract user groups into their ecosystems. Moreover, the solutions developed by many IoT alliances e.g. IETF and OneM2M, often appear incompatible with each other, and this is considered able to create switching barriers commonly referred to as the "lock-in" problem.[34]

---

30 Mehmet Bilal Unver, 'Turning the crossroad for a connected world: reshaping the European prospect for the Internet of Things' [2018] 26(2) International Journal of Law and Information Technology 93, 97.

31 BEREC, *Report Enabling the Internet of Things* (BoR (16) 2016) 41 ('BEREC Report') <http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things> accessed 9 October 2020.

32 Unver (n 29) 100.

33 See Jat Singh and Julia Powles 'Why the internet of things favours dominance' (Guardian, 24 July 2015) <https://www.theguardian.com/technology/2015/jul/24/internet-of-things-centralisation-dominance> accessed 9 October 2020.

34 BEREC Report (n 31) 39.

Against this background, attention needs to be paid to the IoT settings, where interoperability is at stake, whether self-regulated e.g. governed by myriad of ecosystems, or exposed to the proprietary systems and accompanying problems e.g. lock-in, switching costs and market foreclosure. Having said that, diversity of IoT systems and settings hosting distinct standards and of interoperability solutions, has been regarded as worthy of investigation. Thereby, it is hoped that more light is shed on the multi-layered IoT architectures and prevalent industry settings, from which significant reflections could be derived. To sum it up, considering that the IoT offers an important medium for the interoperability gaps and regulatory challenges, which could lead up to generalisable findings, it has been selected as one of the two cases to be investigated.

1.5. Limitations and jurisdictional choice

As the subject-matter of the thesis is universal in a technological sense, the outcomes and findings would be considered as extra-territorial by nature, in particular from a normative perspective. Notwithstanding, the examination of the related (primary and secondary) resources, including the conclusive analysis of the case law, has been conducted on the basis of EU pillars, norms and regulations. While the case study research has been fulfilled following the globally acknowledged technological patterns, standards and facts, the analysis of the real-life situations has also been filtered mostly through the EU regulatory framework, particularly competition law and the ECRF rules. Given this fact, this could be argued as posing a limitation, in terms of scope and boundaries.

In this study, findings from the multidisciplinary doctrinal analysis serve as a stepping stone for the remainder of the research as could be seen through the normative framework drawn at the end of this study. From this point of view, EU legal framework enables a research ground on which the interoperability discourse would be checked and filtered out, considering the wider set of legal rules and principles adopted and implemented under EU law. Originally, many EU rules and principles are often based on or inspired of their US law counterparts such as some exceptional rights under IPR law, essential facilities doctrine under competition law, access obligations under sector-specific regulations. EU law and institutions, while standing on this basis, forge ahead by enacting new rights and obligations i.e. regarding data portability, AI, which poses a widened legal response and measures. Furthermore, one could find more crystallised formulation of these rules and principles under EU law, particularly when it comes to competition law and sector-specific regulation. From the interoperability point of view, more clustered and detailed features of the EU legal system incorporating the relevant case law e.g. regarding refusal to supply, merger cases, offers a wider and promising ground on which a tripartite and comprehensive research would be done.

Wider rules and measures potentially mean wider contours whereby ICT interoperability could be elaborated and investigated ending up with broadly minded evaluation of the gatekeeping roles and functionalities. This is particularly persuasive in view of the competition law and sector-specific regulations so far. For instance, in EU *Microsoft* case, the reason for finding the abuse of dominance was Microsoft's refusal to provide the competitors with interoperability information, whereas the US *Microsoft* case was

not built upon such a discourse.[35] By the same token, after *Trinko* case[36] in the US, it became much harder to consider any denial of access to essential facilities including interfaces as anti-competitive or abusive, as opposed to the EU competition law wisdom that keeps access and interoperability obligations alive and sustainable.[37] Last but not least, this wisdom is supported with the ECRF based rules and safeguards in the EU, whereas neither access remedies nor net neutrality obligations prevail in the USA. In fact, except with the intellectual property legislation and case law, regulation of interoperability has become much obscured and/or underdeveloped within the US law. *Status quo* on the US side thus makes it difficult to cultivate a research regarding ICT interoperability from a multi-disciplinary perspective.

Given this fact and the fact that any proposed regulatory model needs to take account of the prevailing legal standards and thresholds to the most possible extent, the EU law has been chosen as the jurisdictional ground for research. Notwithstanding, regarding IPR rules and exceptions concerning interoperability, US legislation and case law has been referred when it is found useful to compare and contrast the justification(s) behind the applicable safe harbours. In particular, the US perspective to embed the competitive safeguards into the intellectual property legislation and case law would offer a comparative outlook enriching the perspective, as reflected in the Chapter 4.[38] Notably, several doctrines i.e. fair use, merger, patent misuse, developed under the US case law pave the way to a favourable interpretation for enabling interoperability. On the other hand, in the EU law related problems are elaborated from a wider viewpoint in the sense

---

35 United States v. Microsoft Corp., 87 F. Supp. 2d 30, 36 (D.D.C. 2000) at 45. See also Mark Geier, 'United States v. Microsoft Corp.' [2001] 16(1) Berkeley Technology Law Journal 297, 310.

36 *Verizon Telecommunications Inc.* v. *Law Offices of Curtis V. Trinko*, LLP 540 U.S. 398, 2004 ('*Trinko* judgement'). See infra note 459.

37 See the section '5.3.1.3. Refusal to license/supply interoperability information'.

38 See the section '4.2.3. Comparative analysis through the *Nintendo* case'.

that other legal disciplines i.e. competition and sector-specific laws, are mobilised and invoked to deal with the concerns surrounding the lack of interoperability. This provides a wider spectrum of laws and problem solving mechanisms, making the EU law befitting for a research based on multi-disciplinary analysis.

It also needs to be underlined that the research conducted in this study does not only mean doctrinal (blackletter) analysis but also entails multiple case studies that aim to develop a more filtered understanding as to the ICT interoperability. Albeit with the effort to generalise case study research as well as the proposed regulatory model, technology-based framework depicted here would arguably pose some limitations, as well. This argument potentially stems from the very nature of the case study research in that two technological phenomena of cloud computing and the IoT are examined. Some limitations might be posited since these technologies are not necessarily representative of all ICTs and industry settings despite the rationale for them being selected relates to their being widely adopted, usage and direct relevance to ICT interoperability.

However, this plausible limitation is highly obscured because of the universal character of the ICT layers and interdependencies, based on which several research outcomes are developed. In so doing, some concepts e.g. ecosystem, interdependency and coopetition are revisited, many others e.g. layering, gatekeeping are revitalised and reconceptualised. This model is then built up so as to apply to all the ICT networks and services which rely on the well-known layered Internet Protocol (IP) stack, starting with the bottom, infrastructural, layer to the upper, application and content layers.[39] Invoking

[39] For the details of the layered IP stack, see the section '2.2.3. Architectural underpinnings of the internet: Layered IP Stack'. While this IP stack implies technological layers as reflected in the proposed layered model, the distinctive nature of the proposed model should also be noted, in the

the layering approach with some additional elements e.g. 'gatekeeping', the proposed regulatory model comes up with a holistic design and generalisable nature. Overall, it is considered that the selection of multiple cases, along with the interlinks between themselves and with other ICTs being highlighted and being translated into the regulatory model, is believed to mitigate potential arguments of limitations and secure the integrity of the research.

1.6. Structure, outline and main findings of the research

1.6.1. Structure and outline

The thesis commences with the conceptual framework, under which 'interoperability' and related concepts are expounded. Based on this conceptual framework, the study fleshes out the extent of legal regulation of interoperability, and carries on with multidisciplinary doctrinal analysis and case studies respectively. Built upon the cumulative findings and the filtered policy approach, the study ends up with the proposal of a regulatory model. Reflecting this, the thesis is comprised of eight chapters, being structured as follows:

The first, or Introduction chapter consists of the explanation of the background, purpose and scope of the thesis, including the research questions, methodological approach, components and end goals of the research. In so doing, a brief picture is given regarding the doctrinal analysis based on the most featured aspects of the *status*

sense that economic aspects of the ICT networks/services are also incorporated into this model. Interdependency of ICT layers is taken as the baseline to have a coherent idea of regulatory modelling, whereby each layer is acknowledged as a separate (and where necessary, inter-connected) unit for regulatory obligations, in conjunction with the gatekeeping activities. In this regard, 'layering' denotes the technological layout on which the more economic concept of 'gatekeeping' is taken as the key concept for ex ante regulation.

quo and the case study research along with the revelations from the industrial settings. Drawing on these, progressive steps and step-by-step findings are also explained, in the Introduction.

The second and third chapters draw a general framework to clarify the fundamental concepts and the technological underpinnings of the study, and their interplay throughout the thesis. The second chapter deals with the underlying technical and economic concepts and their definitions, whereas the third chapter is focused on the regulation of interoperability in the EU legal fora.

The second chapter starts with the definition and underpinnings of 'interoperability' and deepens with the related concepts, including open and proprietary interfaces, standards and network effects, and ending up with the main characteristics of ICT networks and the internet's architecture e.g. technical layers. Thereunder, key market-based and technological developments e.g. convergence and all-IP migration are also explained, along with their implications concerning interoperability. By this means, it is aimed to ensure a deeper understanding is constructed regarding the evolution of the ICT networks, IP-based ecosystems and technological layers.

In this respect, particular attention is paid to 'convergence' which increasingly refashions the interoperability needs and requirements as are reflected in our everyday lives. It is emphasized that from micro level devices e.g. smart meters, to macro level e.g. next generation networks, interoperability is key to the convergence, which is taking place at the IP level and having an impact on all the related markets, e.g. telecommunications, broadcasting and information technologies (IT). Within this landscape, every sector still continues to be regulated with separate rules and measures,

although this is open to criticism and needs to be checked out from an overall ICT perspective.

The subsequent (third) chapter sheds light on the relevant concerns surrounding the lack of interoperability and the so called gatekeeping concept, and touching base regarding the interoperability-oriented regulations within the EU legal system. Commencing with framing the identified concerns, this chapter clarifies the most prevalent gatekeeping problems caused by the lack of interoperability. Not only competition concerns e.g. vendor lock-in, switching costs and market foreclosure, but also techno-social concerns e.g. end-to-end connectivity, hindered innovation and information flows are highlighted in this context. Then the focus is shifted to how these problems are met and responded to by the policy makers under the distinct bodies of EU law. In this section, IPR rules, competition law and sector-specific rules (ECRF) are examined from the perspective of interoperability, at a rather introductory level. In addition, EU data protection rules are fleshed out, with the emphasis being on 'data portability', given the fact that this recently introduced right enables the consumers to port their data from one platform to another, based on the common data processing systems, and which is closely related to interoperability.

The following three chapters (Chapters 4, 5 and 6) make an in-depth analysis of the EU rules and precedents governing ICT interoperability under the specified three legal regimes, namely IPR rules, competition law and the ECRF. In these chapters, whether and to what extent the (non-)interoperability is given a response from relevant legal regimes is investigated. In so doing, quite a detailed doctrinal (blackletter) analysis is conducted to clarify the scope and limits of each legal regime. Not only legal texts (hard and soft law) and case law, but also previous research and publications, including

journal articles, books, reports and newsletters, are reflected on, in order to deepen the discussion. In this regard, one chapter is dedicated to each legal regime, based on the respective analysis of the investigated primary and secondary resources.

IPR rules constitute the subject-matter of Chapter 4, embracing all the related IPR types, namely copyrights, patents, databases and trade secrets. These IPRs are mainly analysed from the EU legal perspective, and where necessary with references to US case law and legislative measures e.g. Digital Millennium Copyright Act (DMCA). Copyrights, patents, trade secrets and databases are thereby investigated as to whether and to what extent interoperability is enabled under each IPR regime, within the EU framework. EU IPR rules and the applicable exceptions such as the decompilation right are found not to be promising in this respect, particularly for the overprotected interfaces that would otherwise serve opening up the ICT markets to innovative new entries.

In this regard, it is concluded that not only copyrights but also other IPR types pose strict and insurmountable barriers to interoperability, although no IPR rule is designed to augment entry barriers or anti-competitive conducts. Patents, databases and trade secrets are designed to protect their owners from unauthorised third-party uses, and do not touch upon many of the highlighted concerns surrounding lack of interoperability. Given this fact, the role of IPRs becomes controversial, as over-protection of interfaces is not deterred by EU IPR rules, which are usually fragile and not supportive of follow-on innovation e.g. not filtering out the artificial/overzealous IPR uses that hamper innovation. Summing up, after a detailed analysis of IPR rules at the EU level, it is found that such rules do not ensure guaranteed and effective access to the APIs, which

are key to ensuring a competitive and innovative market, and thus revealing a gap from the interoperability perspective.

A comparable, even more detailed analysis has been conducted under Chapter 5, capturing EU competition rules. Under this chapter, it is clearly established that ensuring and/or advancing interoperability does not constitute an aim of EU competition law, but could be considered as such under certain circumstances, often arising out of the refusal practices which are likely to lead to market foreclosure and consumer harm e.g. because of the access denied interfaces. As detailed in this chapter, EU competition law measures provide wide-ranging tools and tests that can be applied to deal with the identified concerns in relation to lack of interoperability.

After the comprehensive analysis, it is found that, unlike with the Article 101 of the TFEU and merger control mechanisms, implementation of Article 102 of the TFEU poses some uneven standards that would make it difficult for timely and effective intervention against the gatekeeping roles and functionalities, broadly speaking. Not only the criteria e.g. regarding 'dominant position' and the tests e.g. to control abusive behaviours invoked by the EU competition rules, but also the lengthy processes and the underlying costs e.g. regulatory and enforcement, are found to be prohibitive for the related parties. It is thus concluded that, although often based on the case-specific analysis and data; competition law exercises, particularly involving Article 102 of the TFEU, which aims to address 'abuse of dominance', would not cope with the ICT-based interoperability challenges in a timely and effective fashion.

The ECRF's perspective and rules are elaborated in Chapter 6, where main characteristics of this regulatory framework, including the interoperability aspects, are

investigated. To have a deeper look through the interoperability aspects, firstly main pillars and the evolution of the ECRF are examined, incorporating the policy objectives and major regulatory tools and mechanisms. In this regard, both the remedies imposed on operators that have 'significant market power' (SMP) and those of a generic symmetric/horizontal nature are examined to have a broader viewpoint. After all, it is seen that, interoperability-specific remedies are limited and subordinated to the access and interconnection remedies that are designed mainly to protect consumer interests and to ensure market competition.

It is also concluded that while this denotes a good 'mix and match' regulatory structure, under which are captured both competitive and other regulatory goals, potential gaps are discernible in view of the ever fast changing ICT markets which depend on increasing interdependencies. Given the IP convergence and the multi-layered nature of ICT networks/services, the promulgated policy objectives and measures of the ECRF are found not to respond to the so-called interdependencies that characterise a holistic landscape. In fact, the fragmentation in regulatory mind-set risks the gatekeeping problems being fragmented and even aggravated, given the competition and techno-social concerns and the shortcomings of competition law mechanisms as well as IPR rules.

Summing up, the doctrinal research of this study values and surfaces the finding that regulatory governance of ICT interoperability should subsist within a holistic policy approach. Following this standpoint, it is considered the multiple case studies would bring out some new and verifying outputs, furthering this groundwork multidisciplinary research towards a crystallised policy approach. It is in the case study

research where the ICT interdependencies are revisited through architectural analysis of emerging technologies, arriving to new findings, as explained below.

1.6.2. Main findings

After having a tentative conclusion at the end of doctrinal (blackletter) analysis, Chapter 7 consists of case study research, seeking to test the former findings and to further these findings with additional inputs based on the industrial settings. To that end, two distinctive but complementary fields, namely Cloud Computing and the IoT, have been chosen. In this regard, it is aimed to find out the industrial responses to lack of interoperability and accompanying concerns. Case study research is mainly led by the analysis of the cloud and the IoT architectures, their technological and economic underpinnings, including industrial processes like standardisation, which have been investigated to gain a fulfilling answer, as against the fragmented legal solutions mentioned above.

Case studies are primarily conducted to verify the former findings gathered from the doctrinal analysis. However, this does not fully reflect the Chapter 7, which also aims to check and find out the gaps relating to ICT interoperability arising out of industrial practices, towards development of the ultimate regulatory model. Crucially, a progressive and multi-faceted research has been conducted throughout the case studies, revealing a set of naturally constructed research components for the overall study. This natural progression is also hidden within the fact that each case study has resulted in distinct but complementary findings, laying down the stepping stones for the ultimate regulatory design.

It is found that, despite the absence of common standards, cloud computing settings point to a thriving industry because of the utility type functioning, ever-faster enhancing cloud adoption and the surrounding ecosystems. However, the IoT settings demonstrate that interoperability gaps, mainly stemming from silo type proprietary systems, bearing noticeable risks that threaten the potential ecosystem settings. These distinctive findings from the case studies demonstrate that industrial settings do not necessarily reflect the ecosystem characteristics e.g. based on coopetition among the ICT stakeholders, and often require a regulatory touch, via which both ecosystem and non-ecosystem settings are captured. Summing up, the case studies not only verified the former findings and supported the plausible need for a holistic regulatory approach, they also helped carving out new concepts e.g. co-opetition against the layer interdependencies.

Chapter 8 (Conclusion) filters the findings gathered from the previous chapters. To build on and also respond to them, *layering theory* has been analysed in conjunction with the established competition law and regulatory concepts e.g. market definition, dominance, essential facilities. While the deficiencies of the established concepts and regulatory patterns are derivable from the doctrinal study (see Chapters 4, 5 and 6), the 'layering theory' is featured in Chapter 8, for it fits well with both ecosystem and non-ecosystem settings having the potential to respond the layer interdependencies as well as gatekeeping activities. This stems mainly from the fact that the 'layering' concept is very conducive to architectural interdependencies, allowing both a holistic/integral viewpoint and individual treatment of each layer; 'access', 'middleware', 'application' and 'content', depending on the identified gatekeeping concerns.

Layering theory while implicating the finding of the regulatory layout for the intended model, paves the way also to find and figure out the way how the gatekeeping roles and functionalities are addressed. Having said that, one could find the widely comprehensible gatekeeping activities as addressed with an appropriate matching between these underlying concepts, namely the 'layering' and 'gatekeeping'. At this point, both concepts transform into key technical terms and thrusts of the model characterising the normative approach to be followed. From this vantage point of view, the 'gatekeeping' concept, which has been referred at the outset of the study, is revitalised to embrace and respond to the interoperability-centric concerns and problems. Hence, this concept has been put at the centre of the proposed 'layered regulatory model', with the view to filter and sort out the related problems not strictly limited to, but also surrounding, the lack of interoperability.

According to this, gatekeeping activities are accepted to exist and be captured by the layered model, as long as they mean an "access and interoperability restriction at the expense of limiting the consumer choices". While it is proposed that such kind of restrictions be prohibited as the starting point or principle, the accompanying principles of transparency, fairness and accountability are also incorporated thereupon. Furthermore, a following set of remedies have also been designated, considering the potential failure(s) to comply with these principles. Having these instruments, the European Commission at the EU level and NRAs at the national level, are expected to firstly designate the gatekeeping activities at each layer and if necessary, at multiple/cross layers and intervene in them in coordination with the stakeholders.

Thereby, it is aimed that the proposed model embraces all the IP, or broadly speaking ICT, layers with responsive principles and remedies that target at gatekeeping

activities. While the proposed model embodies a comprehensive viewpoint as to tackling the gatekeeping activities, interoperability lies at the centre, representing the core thread of the interdependent layers as well as the primary source for the related concerns.

1.6.3. Contribution to knowledge

As stated above, interoperability related concerns are dealt with from a holistic viewpoint in this research, which goes beyond the existing literature and research for they have a narrow-minded approach. Although having a lot of references to the previous research in the field of interoperability, this study upholds an expansive outlook from interoperability towards gatekeeping activities, which marks a remarkable distinction from the existing works. As a matter of fact, existing scholarly works mostly focus on the interoperability concept and seek out the possible ways as to how to improve interoperability within the boundaries of certain bodies of law or industrial solutions.

One research strand compares and contrasts the existing legal disciplines i.e. competition and copyright laws, with a view to find out the best potential solutions from a multidisciplinary point of view.[40] Here is where this study has common aspects with the previous literature, given the Chapters 4, 5 and 6 which respectively examine the EU IPR rules, competition law and ECRF, elaborating on such literature. Notwithstanding, this study expands the multidisciplinary research reflecting on three disciplines, as opposed to the existing works which mainly opt and examine two,

[40] Ashwin van Rooijen, *The Software Interface Between Copyright and Competition Law: A Legal Analysis of Interoperability in Computer Programs* (Kluwer Law International, Information Law Series, Vol. 20, 2011); Weston (n 13); Aaron K. Perzanowski, 'Rethinking Anticircumvention's Interoperability Policy' [2009] 42 University of California Davis Law Review, 101-172.

mostly competition and IPR laws.[41] Conceiving and considering regulation of interoperability 'outside of the box', this thesis aims to explore, expand and refashion the *status quo*, not narrowing down the research to be conducted into the existing legal boundaries.

Another research strand aims to investigate the extent to what certain industry or industries have solved the need to interoperability within their dynamics e.g. collaborative actions, de jure or de facto standards.[42] This group of researches often select an ICT industry to delve deeper into the practices of the industry stakeholders by which to investigate the market forces or self-regulatory measures e.g. code of conduct, often seeking out whether any coercive rule is needed. This thesis benefited also from these group of researches and the relevant literature, given the Chapter 7, which focuses on cloud and IoT interoperability. On the other hand, this study differs from these previous works by avoiding a technologically oriented approach, although being inspired of the technological layers and their interaction. While the ICT standards and protocols are discussed across this research, they do not mean the core activity of research in view of the scope and purpose of the case studies based on the cloud and IoT interoperability.

While interacting with the given research strands, this study broadens the horizon and proposes a regulatory model that would widely respond to the interoperability-based needs and concerns. It is the concluded that, as opposed to the insufficient, partial and

41 See ibid. While there are some references to ECRF under the researches of Van Rooijen and Weston, these references mainly aim to open a parenthesis for the ex ante approach pursued by the given sector-specific regulation, not delving into the ECRF. Both end up with their respective proposals mainly focused on the copyright legislation, which means a stark distinction comparing to this thesis, for being confined to the understanding of the IPR laws and doctrines.

42 See the sections '7.1.3. Interoperability debate in the cloud context' and '7.2.4. Interoperability debate in the IoT context'.

limited solutions derived from the EU legal framework as well as those of the industrial practices, a holistic and multi-layered framework needs to be embedded into the proposed model. Thereby, the proposed 'layered regulatory model' has been devised to have a dynamic nature and functioning for the 'layered' structure that is capable to embody and address the so called 'gatekeeping' activities. Commencing with a set of principles and leaving the corresponding remedies to the overall implementation process, the model opts for a bottom-up approach, instead of imposing top-down and form-based rules. Furthermore, involvement of all the stakeholders in the regulatory process is emphasized so as to filter and sort out the interoperability-based concerns and accompanying gatekeeping problems, which all are intended to be captured by the proposed model.

Against this background, the contribution to knowledge brought by this thesis entails two main elements. Firstly, it is proposed that all the ICT layers and activities are treated in a homogenous and holistic manner through 'layered regulatory model' proposed at the end of this study. Secondly, the proposed model builds on the so called 'gatekeeping' concept, which is revitalised in this study, creating a new horizon for ex ante regulation of ICT layers and activities.

While the previously proposed layered models have overlapping aspects with the 'layered regulatory model', the complete and adaptive nature of this newly proposed model should be emphasized. IP stack (layers) being embedded into this model represents the common aspect with the previously proposed model, as discussed in the last chapter (Conclusion). However, conditions for regulatory intervention under the newly proposed model are distinctive in the sense that the onus in this new framework is the gateways, or technically speaking the interfaces, being exploited to the harm of

consumers across the layers. From this point of view, ‘gatekeepers’ not only controlling the media and information flow, but also access to infrastructural, physical and software interfaces are captured in the definitional framework. According to the proposal, exploitation of the underlying controlling mechanisms, i.e. IPRs, technological protection measures (TPMs), AI-based algorithms for restricting consumer choices would mean presence of gatekeepers and point to a necessity to ex ante regulation.

Within this normative framework, all the players (gatekeepers) across the layers are instructed not to ‘restrict access and interoperability’, should this result in limited consumer choices and freedom. In this vein, it is key to keep in mind that not only reduced consumer surplus from the competition law perspective but also the hindered access to informational resources needs to be taken of utmost account, since these cumulatively constitute the ground of gatekeeping activities. Here, the most featured aspect of the contribution to the knowledge surfaces whereby the interoperability is expanded from a technical term to a techno-social conception, as detailed in the last chapter.

Flowing this spirit, it is aimed that the broadly minded interoperability concerns within the meaning of gatekeeping concept are diagnosed and deterred effectively. While further principles, e.g. transparency, non-discrimination, accountability, and corresponding remedies are also set out within the framework of the layered regulatory model, these rules do not mean direct and straightforward intervention unless contrary practices endure, and ecosystems that are characterised by coopetition or equivalent self-regulatory measures are not in place. Should the so called potentially gatekeeping practices do not denote any restrictive activity e.g. for the existent ecosystem

structures, this needs to be taken into consideration to mitigate the potential remedies, as per the proposed model. Having said that, although having an ex ante nature, newly proposed remedies are designed as circumstantial obligations to be imposed on the so-called gatekeepers. In this context, emphasis is given to the collaboration of the gatekeepers with the regulators, which will determine the extent of the applicable obligations, alongside other factors e.g. coopetition, ecosystem and non-ecosystem structures.

Summing up, it is suggested that gatekeepers operating in each layer ('access', 'middleware', 'application' and 'content') be subject to the governing principles along with the potentially applicable remedies under the given circumstances. Crucially, the governing principles ('prohibition of restriction of access and interoperability at the expense of limiting consumer choices', 'transparency', 'non-discrimination' and 'accountability') are applicable to all the ICT players, regardless of market power. However, the extent to what the remedies are going to be applied to the ICT players, specifically the 'gatekeepers', will be set out within the experimental and learning process of the model. From this point of view, the proposed model is both dynamic and holistic in nature.

As elaborated in the Conclusion, the dynamic nature of the model would bring out some more discussion in terms of implementation of the principles and remedies. Considering this is inevitable and healthy for the prospect of the proposed model, further research is always welcome with regards to how to interpret and implement the 'layered regulatory model' within the context of hidden aspects of algorithmic, artificial intelligence (AI) and data driven services, applications, and its implications for the institutional structure of the EU law.

2. Interoperability in the field of ICTs

2.1. Conceptual framework of interoperability

Interoperability is a topic directly related to ICTs and their governance. As ICTs expand at an ever-growing pace, interoperability has also an expanding and sometimes complicated nature. Below, interoperability is first examined as a core ICT concept, and then investigated from technical, economic and legal perspectives. In this regard, basic information about the related concepts, including network effects, standardisation and ICT networks and services, are given, along with the examination of the architectural thrusts of the internet and internet (IP) based convergence.

2.1.1. Definition of interoperability

ICTs depict a world of digitised and connected devices, systems and networks, which interact with each other towards the same goal of ensuring a communication and/or data exchange. This is ensured through using the same language adopted by the parties or end points. This language, taking distinct forms of bilateral cooperation and recognition, results in the information being sent and received by the parties and understood and transformed into different implementations, including voice, video and data streams. In many cases, this is realised by means of standards being arrived at after long-lasting technical processes and wider scale adoption. For instance, the world wide web (WWW) hosts myriad web resources e.g. text documents, images, on top of the internet. Both the internet and the WWW represent distinct global networks running over standardised protocols e.g. TCP/IP for the former and HTTP for the latter. In both cases, the exchange of data through the protocols is referred to and echoed in the "interoperability" between the end points.

Interoperability is defined as "[t]he ability to transfer and render useful data and other information across systems, applications or components".[43] Interoperability is also defined as "[t]he ability for two different and independent software applications to exchange information without loss of data, semantics or metadata".[44] Other definitions[45] denote a similar meaning and scope, which is also reflected in the Software Directive (2009/24/EC) reading as follows:

> The function of a computer program is to communicate and work together with other components of a computer system and with users and, for this purpose, a logical and, where appropriate, physical interconnection and interaction is required to permit all elements of software and hardware to work with other software and hardware and with users in all the ways in which they are intended to function. The parts of the program which provide for such interconnection and interaction between elements of software and hardware are generally known as 'interfaces'. This functional interconnection and interaction is generally known as 'interoperability'; such interoperability can be defined as *the ability to exchange information and mutually to use the information which has been exchanged*.[46]

---

43 Urs Gasser, 'Interoperability in the digital ecosystem' (2015) GSR15 discussion paper, 2 <http://www.itu.int/en/ITU-D/Conferences/GSR/Pages/GSR2015/GSR15-discussion-paper.aspx> accessed 9 October 2020; John Palfrey and Urs Gasser, *Interop: The promise and perils of highly interconnected systems* (Basic Books 2012) 5; John Palfrey and Urs Gasser, 'Fostering innovation and trade in the global information society: The different facets and roles of interoperability' (2011) NCCR Trade Regulation Working Paper No. 2011/39, 3, <https://www.wti.org/media/filer_public/f7/a7/f7a7ae35-d43a-4e82-8cef-4ca26b7bb778/gasser_and_palfrey_final.pdf> accessed 9 October 2020.

44 Sutor (n 3) 215.

45 There are alternative definitions made so far, among which one refers to "[t]he 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" (Samuelson (n 4) 1946-1947). For the definition introduced by the Institute of Electrical and Electronics Engineers (IEEE) see IEEE, Standards Glossary, 2016, <https://www.standardsuniversity.org/article/standards-glossary/> accessed 9 October 2020.

46 Software Directive, recital 10.

Interoperability does not require that two systems be identical in design or implementation, only that they can exchange information and use the information they exchange.[47] As a result, interoperability allows programmers to develop their software using the formerly accepted format and with no need for decryption or rewriting a similar code. Overall, interoperability, either relating to global IP-based platforms or to the local networks e.g. data centres, would be said to have the same functionality: interaction between software, often together with hardware, components of non-homogenous systems to share and re-use information for a mutually defined objective.[48] As this interaction takes place within and across the ICTs, 'ICT interoperability' could be acknowledged as the same as 'interoperability'. Nevertheless, in the title and many parts of this study, the former is opted for rather than the latter, so as to emphasize the link between 'ICT' and 'interoperability'.[49]

Interoperability might vary from context to context,[50] although the same principles apply in relevant cases. Word processing programs could be considered as an example to comprehend interoperability and the consequences of its absence. It might well be possible to save a document created using one word processing software package in

---

47 Samuelson (n 4) 1947.

48 "Interoperability" has a meaning distinct from "compatibility" and "co-operation". Devices, systems and networks are considered as "interoperable" when they execute together a common task going beyond being compatible and cooperative. Technically, "compatibility" is a specific form of interoperability that represents certain choices in the development of a system. For example, in 2014, the EU authorities put into force a Directive (Directive 2014/53/EU of the European Parliament and of the Council, 2014 O. J. L. 153/62) that called for the use of a common standard for mobile phone chargers, which set out a narrow solution (design choice) as to the "compatibility of the cables that provide power to mobile devices" (Gasser (n 43) 3).

49 From a broader viewpoint, this preference could be argued to be crucial, as a definition of 'interoperability' is not standard in dictionaries. For instance, 'interoperability' is defined as "the ability of computer systems or software to exchange and make use of information" by the Oxford Dictionaries (See Oxford Dictionaries <https://en.oxforddictionaries.com/definition/interoperability> accessed 9 October 2020, whereas Cambridge Dictionary defines it as "the degree to which two products, programs, etc. can be used together, or the quality of being able to be used together" (Cambridge Dictionary <https://dictionary.cambridge.org/dictionary/english/interoperability> accessed 9 October 2020).

50 See Sara Gabriella Hoffman, *Regulation of Cloud Services under US and EU Antitrust, Competition and Privacy Laws* (PL Academic Research 2017) 129.

another file format and to use this file with different software, but one might lose some or all of the text formatting in the case that the word processing programs are not interoperable.[51] The same logic and principles apply to the online music industry,[52] which has so far been fraught with a variety of encryption methods such as digital rights management (DRM)[53] techniques. Aiming at protecting the native users from unauthorised access, DRM tools might go beyond this, creating a barrier for interoperability and the development of digital music content. All these examples show that interoperability between the competing platforms e.g. music distribution channels and software e.g. word processing programmes etc. is not granted at all, but needs to be achieved via the collaboration between the parties.

Achievement of interoperability would stimulate new entries to the relevant market, reducing the up-front costs for investment and switching costs. This means more competition in the relevant markets. The current evolution and state of the mass computer market illustrates interoperability's pivotal role in ensuring market competition between all of the actors involved.[54] Going through a long-lasting journey, the computer industry emanated from the monolithic systems e.g. mainframe computers of earlier decades and reaches to today's modular systems consisting of heterogeneous components e.g. memories, monitors and hard drivers, created by different manufacturers. In the 1970s, once a company purchased a computer system, the company was essentially "locked in" to that system, as the system was not compatible

51 Palfrey and Gasser (n 43) 2011 4.
52 Palfrey and Gasser (n 43) 2011 4.
53 DRM means "[a] bundle of software, services and technologies that confine use of digital content to authorised consumers, and manages consequences of that use throughout the entire life cycle of the digital content" (Carlisle George and Navin Chandak, 'Issues and Challenges in Securing Interoperability of DRM Systems in the Digital Music Market' [2006] 20(3) International Review of Law Computers & Technology 271, 272).
54 Simone Aliprandi 'Interoperability and Open Standards: The Key to True Openness and Innovation' [2015] 3(1) International Free and Open Source Software Law Review 5, 5-6.

with the products manufactured by other companies and the conversion costs were high.[55] Although 'lock-in' was extremely profitable for dominant vendors, such as IBM, its competitors and users suffered from high prices, indifferent service, limited choice and slow innovation.[56] Under various tensions related to such experiences and with huge increases in software development and an accompanying demand, the IT industry was driven by dramatic changes toward more interoperable solutions.

From this point of view, interoperability serves as a key driver for the development of the ICT industry, going beyond what is understood from its basic definition. It is noteworthy that know-how aggregation and specialisation in wide-ranging ICT areas are being transformed into useful and innovative products through interoperability. Today, interoperable hardware and software products manufactured by different vendors are configured to speak to each other, resulting in far-reaching implications from a self-feeding loop of innovation. Given these consequences, interoperability is widely seen as the life blood of the ICT industry,[57] as well as considered to promote socially desirable goals, such as fostering competition and innovation, enhancing consumer satisfaction and promoting economic growth.[58] From a broader perspective, adverse consequences in the absence of interoperability towards information flows and ultimately cultural production and participatory democracy need to be added as follow-on challenges.[59]

---

55 Jonathan Band and Masanobu Katoh, *Interfaces on Trial 2.0* (The MIT Press 2011) 1.

56 Ibid.

57 Ian Walden, 'Open Source as Philosophy, Methodology, and Commerce: Using Law with Attitude' in Noam Shemtov and Ian Walden (edbs), *Free and Open Source Software* (OUP 2013) 32.

58 Samuelson (n 4) 1943-1944.

59 See the section '3.1.2. Main concerns surrounding lack of interoperability'.

2.1.2. Underlying elements of interoperability

Interoperability builds on common, or mutually acknowledged, protocols, interfaces and standards, being used across from telecommunications networks to the everyday used IoT devices e.g. smart TVs and thermostats. ICT systems' ability to read each other's data formats and structures (syntactical interoperability) and understand them (semantic interoperability) as well as being connected to each other technically defines their interoperability. In order to secure interoperability, as often achieved via standards, the data formats and structures which underlie the functionalities of an ICT system must be available to other ICT system(s), and, they need to understand each other to fulfil a common task.

Interoperability can occur when the maker of one ICT system develops 'interfaces' that enable the exchange of data between the entity it is developing and the entities with which its entity will interact.[60] The interfaces used to ensure interoperability among ICT systems are called "application programming interfaces" (APIs), which represent a software package running over pre-defined protocols.[61] While there are some other types of interfaces e.g. user interfaces,[62] interoperability is achieved through "APIs", which reveal wide-ranging examples of usage in a very extensive area e.g. from computer software to next generation networks (NGNs). For instance, the APIs of the popular image-editing program Adobe Photoshop enable third parties to

60 Samuelson (n 4) 1947.

61 ICT interfaces (or APIs) could be considered as the informational equivalents of the standard plug and socket designs that designers of electric appliances must use in order for their appliances to successfully interoperate with the electric grid (Samuelson (n 4) 1947).

62 Nicolo Zingales, 'Of Coffee Pods, Videogames, and Missed Interoperability: Reflections for EU Governance of the Internet of Things', (2016) TILEC Discussion Paper (DP 2015-026), 7; Van Rooijen (n 40) 14.

create image effect filters that can be used within Photoshop, and the open source web browser Mozilla Firefox enables others to create plug-ins through its APIs.[63]

APIs thus function as gateways of the software, or computer, programs. Yet APIs may not be "open" to third parties, such as the widely used archive file format called RAR which is built upon closed interfaces. On the other hand, accessing APIs is not imperative for the third parties to achieve interoperability, so long as underlying protocols and the data formats are disclosed with this purpose.[64]

Instead of opening APIs, using standardised or mutually agreed protocols is often an effective means to secure interoperability. A protocol defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.[65] Adoption of common protocols would enable interoperability being ensured among the parties with no further effort concerning conversion, decryption, etc. Alternatively, through a common data format, it is possible to achieve interoperability in the sense that even though applications may be written in different languages, they would have the same data structure and could be understood on the part of the developers.[66]

Alternative ways could be used to achieve interoperability in order to enable that the machine-readable "object code" of the underlying software are decoded. Notably, programmers can generally design the internal structure of programs to implement interfaces and encode those designs in human readable "source code" in many different

63 Van Rooijen (n 40) 14.
64 See Bain (n 3) 161; Sutor (n 3) 215.
65 Hilde Marita Oen, 'Interoperability at the Application Layer in the Internet of Things' (MSc Thesis, Norwegian University of Science and Technology 2015), 11.
66 Ibid, 42.

ways.[67] To reach out to the source codes, access seekers would attempt to reverse engineer the usually disclosed object codes that conceal the internal design of the underlying software. This, however, is a very costly and time-consuming method to achieve interoperability, as detailed below.

2.1.3. Open and proprietary systems

ICT interoperability stretches along a spectrum, along which different business strategies are developed. At one end of this spectrum exists entirely closed systems that reveal no APIs, whereas the other end of the spectrum is represented by the systems that expose all details of their internal design, such as in case of open source software (OSS).[68] While Apple's iTunes platform, which features digital music and video content that is exclusively open to iPod, iPad and iPhone customers represents the former, Google's Android-based platforms e.g. Google Chrome, Google Play and Google Maps are open to everyone, either an Android user or not, and exemplifies the latter.

From this point of view, codes that underlie the software programs could be either 'open' or 'closed', depending on what policy a software developer adopts as to accessibility (openness) of the source codes to third parties. In the case that the underlying source codes are protected with no controlling software or application, this is depicted by OSS, including open APIs. Control over the interfaces is realised mostly through IPRs, consisting of copyrights, patents and trade secrets, with the view to encapsulate the kernels, the internal design of the software and to close it off against third party access. This situation is referred to as "proprietary" software, or business models vis-à-vis the "non-proprietary" ones. While these two distinctions, 'open –

67 Samuelson (n 4) 1948.
68 Samuelson (n 4) 1952.

closed' and 'proprietary – non-proprietary', are not fully overlapping, in many cases the OSS represents 'non-proprietary' software, just like the 'proprietary' software is often manifested in the closed systems.[69] Notwithstanding, neither 'non-proprietary' nor 'open' software products/systems are necessarily free of charge for third-party access seekers e.g. licensees.

As mentioned above, IPRs are the basic and most effective means to protect the software against third-party usage. In addition to the IPR protection, sometimes a TPM is put in place by the IPR owner to restrict third party accesses.[70] TPMs, whose primary objective is to protect digital copyrighted materials, could be exemplified by DRMs. For example, copy protected CDs typically have DRM-based proprietary systems to ensure that the discs can be played only on record label specific software players. The use of TPMs/DRMs serves to 'lock' users into a particular software, and results in users' devices being restricted to certain platforms e.g. such as the iTunes store being limited to iPod/iPhone/iPad users. This may bring about limited functionality of e.g. handset devices via their original design, leaving users much less able to use their devices as they may wish.[71] In order to jailbreak these devices, however, and to load on an alternative OS and/or access to an alternative app store, certain TPMs need to be circumvented.[72] In most cases, bypassing a TPM/DRM is legally considered as an

---

69 It should also be noted that copyrights, and sometimes patents, come up with the codes written by the developers which usually have a licensing policy. Open source licences are common on various ways, e.g. freely (FOSS), permissive, reciprocal, which manifest a wide range of licensing policies run by the software community. For detailed information regarding the interplay between software OSS and licencing approaches see Ross Gardler, 'Open Source and Governance' in Noam Shemtov and Ian Walden (eds), *Free and Open Source Software* (OUP 2013) 37-68.

70 The legal definition of a TPM is given under Article 6(3) of Directive 2001/29/EC [Directive (EC) 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] L167/10 ('InfoSoc Directive') art 6(3)]. This Directive basically states that a TPM is any technology (software or hardware) which restricts access to a copyrighted material without the consent of the copyright holder.

71 Daly (n 23) 95.

72 Daly (n 23) 94.

individual offence in addition to any IPR infringement that could be potentially claimed.[73]

The OSS movement, which favours open production processes, marks a contrast with proprietary business models, resulting in an inescapable correlation between 'interoperability' and 'openness'. The OSS developers' policy is based on distribution of the software in source codes, aiming at an environment whereby reverse engineering is obviated and further applications and services are built on the original software easily. Moreover, open source developers employ license agreements that not only permit the creation of derivative works e.g. via Berkeley Software Distribution (BSD) licences, but also typically require the licensee to distribute the modified programs to the public only in source code e.g. via General Public License (GPL).[74]

Open interfaces are brought to the life via open source movements and open standardisation.[75] Standards developed primarily by the ICT industry through open processes such as USB interconnections, Ethernet, XML and Wireless LAN technologies, are designed to have open interfaces.[76] Most successful open interfaces are developed out of neo-traditional standard setting organisations (SSOs) that

---

73 Notably, Article 6(2) of the Directive 2001/29/EC (Infosoc Directive) bans the manufacture, import, distribution, sale, rental and advertisement of TPM-protected technologies, devices or components, which "(a) are promoted, advertised or marketed for the purpose of circumvention of, or (b) have only a limited commercially significant purpose or use other than to circumvent, or (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention".

74 Nicos L. Tsilas, 'Open Innovation and Interoperability' in L. DeNardis (eds), *Opening Standards: The Global Politics of Interoperability* (The MIT Press 2011) 109. See also Band and Katoh (n 55), 183-184.

75 For more information regarding standardisation, open standards and their implications for interoperability see the section '2.1.4. Standardisation'.

76 See Jay P. Kesan, 'Open Standards' (2018) University of Illinois College of Law Legal Studies Research Paper No. 18-38, 5-7. <https://ssrn.com/abstract=3260138> accessed 9 October 2020. See also Comptia, *European Interoperability Framework: ICT Industry Recommendations*, (White Paper, 2004) 14, <http://www.urenio.org/e-innovation/stratinc/files/library/ict/15.ICT_standards.pdf> accessed 9 October 2020.

distance themselves from bureaucratic procedures. With such processes ending up in open software and interfaces, IPRs are pooled into a more dynamic process to enable interoperability and follow-on innovation. While a positive correlation between the interoperability and follow-on innovation is remarkable based on the standards, counter arguments could be raised should the standards be determined in a very deterministic and restrictive manner. Likewise, closed and proprietary systems, albeit with limited interoperability, could stimulate innovation alongside the OSS based standards and/or protocols.[77]

2.1.4. Standardisation

ICT interoperability is intrinsically coupled with the standardisation. It is common for the companies that generate revenue from consulting and integration of services to promote standards as an important way of accomplishing interoperability, to create standards' initiatives that target a competitor's existing product in an effort to commoditize it and then to lobby governments to mandate that newly developed standard.[78] Although a standard could be mentioned theoretically, even in the case that two firms agree on a format or protocol; standardisation is a multi-party, cooperative and continuous or dynamic) process in its ideal manifestation.

From this point of view, standardisation ideally takes place when the stakeholders are involved in a learning, sharing and production process, whereby every participant's IPRs are disclosed under fair, reasonable and non-discriminatory (FRAND) terms in order to create a technology or product that enables interoperability.[79] By standardising

77 See Van Rooijen (n 40) 31-37.
78 Tsilas (n 74) 108.
79 Unver (n 30) 98.

competitors' products and creating multiple standards, whose IPRs are often licensed on royalty-free terms and which are implemented in OSS, new value is provided to the customer.[80]

In ICT standards, succeeding technologies and platforms grow upon basic sets of standards, which are created either through the SSOs or led by the market forces, which denote *de jure* and *de facto* standards respectively. Usually de facto standards are conferred in a situation of natural monopoly, arising out of the market conditions that are initially competitive amongst different technologies, with agreement among producers on the standard technology arriving without a formal process.[81] In the case of *de jure* standards, a natural monopoly on technology is agreed upon by a body that may be an association and which is perhaps, but not necessarily, with a public interest mandate, of some combination of technology users and suppliers.[82] While *de jure* standards are truly represented by telecom standards such as ISDN, GSM, LTE; Windows OS, JavaScript, the QWERTY keyboard and HTTP illustrate *de facto* standards. Mass customer demands and the accompanying spillover effects over the complementary products make the dynamic ICT industries more prone than other industries to de facto standards.

Another categorisation could be done according to whether standards are "open" or "proprietary". A *proprietary* standard exists when the functionality of a technology is controlled by a single entity, or by a private, small group of cooperating entities, and

---

80 Tsilas (n 74) 108.

81 Rishab Ghosh, 'An Economic Basis for Open Standards' in Laura DeNardis (ed.), *Opening Standards: The Global Politics of Interoperability* (The MIT Press 2011) 78.

82 Ibid. Bodies with some level of formal process for defining such standards include, but are not limited to, the International Telecommunications Union (ITU), the European Telecommunications Standards Institute (ETSI), the Institute of Electrical and Electronics Engineers (IEEE), the World Wide Web Consortium (W3C), and the Internet Engineering Task Force (IETF).

the rights to the specific technology are available only to the rights holder(s). Proprietary does not necessarily mean "closed"; it mostly indicates that a quicker and an internalised process is used to develop the standard.[83] We see that these types of technologies, like Windows OS, become a de facto standard as they are widely used after being created. Notwithstanding, de facto or proprietary standards, for the popular and mass demand stemming from the developer/user side, could undergo an openness process before the industry SSOs.[84]

On the other hand, open standards from the beginning develop in an environment where no underlying technology dominates the adoption process, such as in the creation of the Extensible Markup Language (XML), a specification developed by the WWW Consortium. Open standards emerge when the situation of natural monopoly on the technology is accompanied by full competition in the market for products and services based on the technology, with no *a priori* advantage based on the ownership of the rights for the rights holder.[85] This occurs when access to the technology is available to all potential economic actors on equal terms, providing no advantages for the rights holders.[86] For these reasons, open standards give users certain flexibility, agility and diversity to develop derivative products.

---

83 Jim Markwith, 'Key intellectual property issues in acquisitions involving open source software' [2008] Computer and Telecommunications Law Review 45, 47.

84 See ibid, reading; "[I]n fact, proprietary standards can be instrumental in achieving interoperability in various situations. They can also evolve into open standards. For example, pursuit of a proprietary standard by a group of companies may make the most sense under certain circumstances because the standard can be developed and adopted more quickly than in the open standards process and because only a few organizations will rely on the standard to achieve interoperability. Later, if that proprietary standard becomes more well known and implemented by other organisations under reasonable licensing terms, it may rise to the status of a de facto industry standard. At such point, it may also be contributed to by an open standard organisation, such as the ITU, ISO, IEEE, ECMA, or ETSI, for formal adoption as an open standard in order to achieve even wider acceptance and implementation. Two examples of this are: (1) the Open XML File Formats, which were developed by Microsoft, later adopted as an open standard by ECMA (ECMA-376), and (2) PDF, which was developed by Adobe, became a very popular proprietary standard, and has been adopted as an open standard by ISO".

85 Ghosh (n 81) 79-80.

86 Ghosh (n 81) 79-80.

There are many definitions of "open standards" made by different entities. Among them, the definition of the European Interoperability Framework (EIF), adopted by the European Commission (Commission), could be given as a prominent example which enlists the following criteria for a standard to be considered as "open":[87]

- The standard is adopted and will be maintained by a not-for-profit organisation, and its ongoing development occurs on the basis of an open decision-making procedure available to all interested parties, in a consensus or majority decision etc.

- The standard has been published and the standard specification document is available either freely or at a nominal charge. It must be permissible to all to copy, distribute and use it for no fee, or at a nominal fee.

- The intellectual property - i.e. patents possibly present - of (parts of) the standard is made irrevocably available on a royalty free basis.

Although open standards are defined and championed by many as being freely used and distributed, many SSOs that develop 'open' standards, including the ETSI, IEEF, IETF, ISO/IEC, ITU, OMA, ANSI and ECMA, do not mandate IPR-free standards or royalty-free IPR licensing.[88] Many industry-wide open standards are being implemented through FRAND licensing. This might be deemed to create a balance in order to establish and drive market competition between IPR owners and implementers. It is argued that, by mandating royalty-free licensing and unfettered sublicensing and by prohibiting other reasonable licensing terms, royalty-free

87 European Commission, European interoperability framework for pan-European eGovernment services (Version 1.0) 2004, 9. Rearding other definitions of "open standards", see Kesan (n 76) 2-15; Tsilas (n 74).

88 Kesan (n 76) 4; Tsilas (n 74) 112. See also Aliprandi (n 54) 17-20.

standardisation would likely deter IPR holders from participating in and contributing to the standards development process.[89]

From this vantage point of view, it is note-worthy that the standardisation process is not entirely immune from anti-competitive concerns. In fact, there sometimes arises risk of collusion e.g. companies using the SSO to facilitate price fixing, as well as risk of exclusion e.g. companies using the SSO to freeze out a competitor, whilst adopting a standard.[90] In order to eliminate such risks, the SSOs often apply a number of safeguards including mandating the participants in the standardisation process to disclose their IPRs, which are essential to the standard setting, and to commit to license such essential IPRs under FRAND terms. However, this does not necessarily reflect the situation for all the SSOs. Moreover, the SSOs do not impose an obligation on IPR owners to conduct a search for, or guarantee the disclosure of all IPRs they own that may be essential to a given standard.[91] Last but not least, while the EU competition rules, Article 101 and 102 of the TFEU, have a mitigative effect, it would be far-fetched to assume anti-competitive risks being dissipated at all in SSO processes.[92]

---

89 Tsilas (n 74) 112. According to Tsilas, this would, first, deprive such standards of the best technological solutions and secondly, would allow the key IPR holders (who would not be subject to the organisation's IPR policies) either to refuse to license their essential technology, or to impose unreasonable terms and conditions on implementers of the standard (Tsilas (n 74) 112).

90 Erica S. Mintzer and Logan M. Breed, 'How to Keep the Fox Out of the Henhouse: Monopolization in the Context of Standards-Setting Organizations' [2007] 19(9) Intellectual Property & Technology Law Journal 5, 5.

91 Damien Geradin and Anne Layne-Farrar, 'The Logic and Limits of Ex ante Competition in a Standards Setting Environment' [2007] 3(1) Competition Policy International 78, 85; Damien Geradin and Miguel Rato 'Can Standards-Setting Lead to Exploitative Abuse? A Dissonant View on Patent Hold-up, Royalty-Stacking and the Meaning of FRAND' [2007] 3(1) European Competition Journal 101, 110-111.

92 See Unver (n 30) 98-99. For discussion of the abusive conducts arising out of the formal standards setting processes and their implications, see Geradin and Layne-Farrar (n 91) 79-106; Piotr Staniszewski, 'The interplay between IP rights and competition law in the context of standardization', [2007] 2(10) Journal of Intellectual Property Law and Practice, 666-681; Adam Biegel, Rod Ganske and Jon Jurgovan, 'Broadened Antitrust Liability for Abusing Standards-Setting Process' [2006] 18(12) Intellectual Property & Technology Law Journal, 4-6. See also the section '5.2. Article 101 TFEU'.

2.1.5. Network effects

As could be derived from the framework above, both standards and IPRs are important tools for innovation and competition, and their intrinsic values vary for each market. They can serve for a market being built up or expanded, with substitutable products surrounding the created standard. While their purposes and functionalities differ from each other,[93] both are covered by the term "network effects". ICT platforms reveal network effects, which entail directly or indirectly enhanced benefits for the prevailing and prospective users on the same network platform.[94] In the case of telecommunications services e.g. voice telephony, adding new customers to a network increases the surplus of other subscribers who are able to call and be called by the new customers and therefore affects customers' demands.[95] When IT or software markets e.g. social networking sites are considered, similar findings could be reached. For example, Facebook now has more subscribers by far than any other social networking site and is valuable to its users precisely because so many of their friends and acquaintances are on it.[96]

The network effects described above are represented by direct network effects, when consumer utility directly depends on the market size, independently of charging method. There also exist indirect network effects, which are generated indirectly

---

93 See N. Pires de Carvalho, 'Technical Standards, Intellectual Property and Competition - An Holistic View' [2015] 47 Washington University Journal Law & Policy 61, 65, reading; "[p]aradoxically, intellectual property is the product of market regulation - in the sense that the acquisition, use and loss of rights are established by law - for the sake of market freedom, whereas, by a vivid contrast, standardization is the product of market regulation that to a large extent curtails rivalry in invention and in offering competing products and services to consumers".

94 Martin Peitz and Tommaso Valletti, 'Reassessing competition concerns in electronic communications markets' [2015] 39 Telecommunications Policy 896, 898.

95 Jong-Hee Hahn, 'Nonlinear Pricing of Telecommunications with Call and Network Externalities' (2002) 2 <http://www.krannert.purdue.edu/centers/ijio/Accepted/1720.pdf> accessed 9 October 2020.

96 Jonathan E. Nuechterlein and Philip J. Weiser, *Digital Crossroads: Telecommunications Law and Policy in the Internet Age* (2nd edn, The MIT Press 2013) 7.

through market mechanisms such as economies of scale, scope and density. In industries that display strong initial direct network effects, a critical mass of users is needed for users to receive sufficient value from the use of products, such as the telephone, fax machine or social networking services.[97] In industries that display strong indirect network effects, a critical mass of complementary products e.g. hardware and software are needed for users to receive sufficient value from the use of computers, video games, or video or music players.[98]

A remarkable level of interdependence among the ICT players is a result of the industry-level network effects, as depicted in the 'interconnection agreements'[99] signed between the telecom operators. Central to interconnection agreements is the fact that interconnecting networks yield positive network externalities in which the value of the network to each customer increases as the number of customers increases.[100] Therefore, the total value of a customer joining the network depends on not only the private benefits but also the external benefits of being able to send and receive call(s) from any other parties within the network.[101] An operator lacking an interconnection with other operators would be able to just serve its own subscribers

---

97 Jeffrey L. Funk 'Standards, critical mass, and the formation of complex industries: A case study of the mobile Internet' [2011] 28(4) Journal of Engineering and Technology Management 232, 232.

98 Ibid.

99 "Interconnection" can be defined as the commercial and technical arrangements under which service providers can connect their equipment, network and services, to enable their customers to have access to the customers, services and networks of other service providers. When operators agree in order to provide interconnection between their networks, this agreement is called an 'interconnection agreement', an agreement that stipulates the rights and obligations of each contracting party with regards to interconnection (See Colin Blackman and Lara Srivastava, *Telecommunications Regulation Handbook* (10th Anniversary edn, International Bank for Reconstruction and Development / World Bank, Infodev and ITU, 2011) 123-125 <https://www.itu.int/pub/D-PREF-TRH.1-2011> accessed 9 October 2020. See also the section '6.2.1.1. Interconnection'.

100 Mehmet Bilal Unver, 'Essential Facilities Doctrine under EC Competition Law and Particular Implications of the Doctrine for Telecommunications Sectors in EU and Turkey' (MS Thesis, Middle East Technical University 2004), 68.

101 Ibid.

and lose consumers who would opt larger networks which are interconnected with others and thus benefit from network effects, via outgoing and incoming traffic. Hence, interconnection between telecommunications networks serves to externalise network effects from the operator-level to the industry-level, along with the corelated consumer surplus.

As a result of (extended) network effects, a self-perpetuating innovation could be mentioned on the part of the dominant platform or network owner as this would influence both preferences and predictions of the related parties e.g. end-users, software designers. This self-reinforcing process is echoed with *market tipping* as well as representing the technological *lock-in*. Eventually, one network or platform amongst a number of competitors could win the race for the vast majority of consumers, even though the winning product may not be superior to its rivals.[102] In such a situation, as new and innovative technologies might not be optimally disseminated, there is a risk of welfare losses because of the selection of the inferior technology by the users.[103]

Dissemination of a network product might depend on various causes that are conducive to the process of open innovation and its constitutive elements. Successful

---

[102] IPRs in interface information that belong to dominant companies can be used to prevent the emergence of superior technology which is not compliant with the de facto industry standard (Weston (n 13) 46).

[103] Van Rooijen (n 40) 28. In network industries, existing direct and indirect externalities, when equipped with other predatory actions i.e. degradation of interoperability, often cause market tipping towards the dominant product and make other products excluded from the market. Commission's findings concerning Microsoft's refusal to supply interface information related to Windows OS illustrates this. In that case, by denying compatibility to Solaris (Sun's operating system), Microsoft was not only maintaining the market position of its work group server software but also protecting itself from any threat that would emerge out of (horizontal) competition in that market (Maria J. Gil-Moltó, 'Economic Aspects of the Microsoft Case: Networks, Interoperability and Competition' (2008) University of Leicester, Working Paper No. 08/39, 13 <http://www.le.ac.uk/economics/research/RePEc/lec/leecon/dp08-39.pdf> accessed 9 October 2020.

development and take-up processes might first benefit from a level of interoperability, which steers the users into a proprietary ecosystem based on the network effects.[104] On the other hand, the emergent network effects could find a way to carve industry-level standards and products in time.[105]

From a broader point of view, open innovation and open standards would drive stakeholders towards a comparable result of achievement of network effects, such as in a great many OSS and open business models i.e. based on Google's Android OS. Linux could be given as an example for an OSS that creates network effects extending to secondary markets. In fact, any organisation or individual can use Linux (demand-side) and offer Linux-compatible software application (supply-side). Any party can bundle the Linux OS, subject to the rules of the open source community that maintains the OS kernel.[106] Promoting Linux and other OSS, IBM mostly pursues a policy of industry-level network effects, e.g. by transferring the IPRs regarding its Eclipse software development tools, to an independent foundation based on the open source community.[107]

---

104 This strategy was perfectly pursued by Microsoft following the launch of its Windows-based OS, which ultimately gained a prominent reach by means of compatible software and applications. The network externality benefits of using Windows and Windows-compatible software, which gained an early advantage in installed base and availability of complementary goods, enabled the platform to lock several would-be contenders, such as Geoworks and Next, completely out of the market (Melissa A. Schilling, 'Protecting or diffusing a technology platform: tradeoffs in appropriability, network externalities, and architectural control' in Annabelle Gawer, (ed.), *Platforms, Markets and Innovation* (Edward Elgar 2009) 196.

105 See supra note 84.

106 Thomas R. Eisemann, 'Geoffrey Parker and Marshall Van Alstyne, Opening platforms: how, when and why?' in Annabelle Gawer (eds), *Platforms, Markets and Innovation* (Edward Elgar 2009) 132.

107 See ibid, 143.

2.2. Main characteristics and evolution of ICT networks

2.2.1. Architectural underpinnings of the internet: Layered IP Stack

Architectural and functional underpinnings of the internet have a crucial role for the operation of ICT networks and services. Basically, the internet aims to provide universal communication services to applications running on the hosts attached to distinct but interconnected networks.[108] Having said that, the internet's architectural design reveals a unique set of principles e.g. packet-switching,[109] by which global IP connectivity is ensured and consisting of the governing protocols across the technological (software) layers. The lack of a hierarchy behind the internet, coupled with a layer-based and modular structure, ensures permission-less and limitless innovations induced by the layered IP stack.

The internet is standardised by the Internet Engineering Task Force (IETF).[110] The internet, based on the standardised TCP/IP stack, or simply saying IP stack, relies on a unique 'protocol layering'. "TCP/IP", started in the early 1970s to serve as the main *protocol stack (suite)* used in the global internet and it was afterwards in 1978 that it split into two main protocols, the Transmission Control Protocol (TCP) and the Internet

---

108 Barbara van Schewick, 'Internet Architecture and Innovation' (The MIT Press 2012) 83.

109 Ian Walden 'Access and Interconnection' in Ian Walden (eds) *Telecommunications Law and Regulation* (4th edn, OUP 2012), 400. How the internet works through packet-switching between two hosts is explained by Yoo as follows:

> In the typical Internet transaction, a process generates a message and transfers it to the OS running on the host. The OS divides the message into packets configured for the Internet and hands them off to the first-hop router of a communications network. The sending communications network will convey these packets to the receiving communications network, which in turn passes them to the receiving host's operating system. The OS then passes them to the process running on the receiving host. (Christopher Yoo, 'Protocol Layering and Internet Policy' [2013] 161 University of Pennsylvania Law Review 1707, 1719).

The technological process commencing with the circuit-switched networks ending up with (packet-swictched) NGNs is explained in the section '2.2.3. Transition from legacy networks to NGNs'.

110 Toni Janevski, *NGN Architectures, Protocols and Services* (John Wiley & Sons, Ltd. 2014) 29.

Protocol (IP). The "TCP" part of the TCP/IP stack governs the assembly and reassembly of the data at each end, including checking for errors such as missing data, whereas the "IP" part is responsible for routing data from one node to another.[111] These elements of the internet enable a computer in one corner of the world to find a different computer in another corner of the world and exchange information that can be understood by the applications software loaded onto the computers at each end of the transmission.[112]

To provide universal communication services across distinct, interconnected networks, the internet's architecture partitions network functionality into certain layers, with one or more protocols implementing the functionality assigned to each layer.[113] This, being expressed by the term 'protocol layering', underlines the logic and principles governing the internet. TCP/IP, representing the most acknowledged protocol suite, is based on a four-layer stack (suite) adopted by the IETF. Not only this but also other protocol suites have been developed through the scientific collaboration and standardisation efforts so far.

In this study, TCP/IP is referred to as the main protocol stack (suite) as it is far more used for transmitting data packets through the internet, when compared to other protocols.[114] For various reasons, e.g. global network effects, the challenges from proprietary protocols, TCP/IP works and is now the de facto standard for open

---

111 Nuechterlein and Weiser (n 96) 167.

112 Ibid, 165. One end host (computer) might be a powerful server running on the UNIX OS, and the other might be a Windows-based PC, or an iPad running iOS, or an Android smartphone. The critical point is that all "computers" connected to the internet speak the same IP-based logical-layer language (Ibid, 165-166).

113 Van Schewick (n 108) 84.

114 The 'layered regulatory model' proposed at the end of the study builds upon a layering structure, if not a protocol layering one can figure out purely in a technical sense. Notwithstanding, the proposed model by and large reflects on this TCI/IP protocol suite, along with some modifications. With regard to further details, see the section '8.4.1. Main features of the model'.

systems.[115] Although the Open Systems Interconnection (OSI) Model was in use at the same time after being developed by the International Organization for Standardization (ISO), TCP/IP became more widespread, enabling multi-vendor interoperability.[116] The OSI Reference Model consists of seven specific layers to describe networked systems, including three upper layers (application, presentation, session) corresponding to the application layer of the IETF's TCI/IP suite. Seemingly, for the lack of software supporting the model, OSI has not achieved a widespread adoption unlike with its first rival, TCI/IP.[117] There are key principles for TCP/IP layering that are also crucial to understand the ICT interoperability, as reflected below.

To implement the partitioned services or roles of the internet, each layer uses the services provided by the layer below. As widely acknowledged, the lowest layer is called the *physical layer*, denoting the bottom layer,[118] although it is not covered by the original TCP/IP stack. The TCP/IP stack contains the sequentially structured four layers: *data link layer, network (Internet) layer, transport layer* and *the application*

---

115 [T]he dominance of TCP/IP over proprietary suites such as DECNET and SNA/APPN can be largely explained by: (1) the increasing rejection of manufacturer-dominated, that is, proprietary, standards; (2) the increasingly widespread demonstration of the benefits and ease of use of open standards; and (3) the failure of some major industry players to adapt to the new more decentralised environment (Stanley M. Besen and George Sadowsky, 'The economics of Internet standards', in Johannes M. Bauer and Michael Latzer (eds.), *Handbook on the Economics of the Internet* (Edward Elgar 2016) 211, 216).

116 For detailed information about the standards that raced to govern the internet, incorporating their developmental processes and the factors for their success or failures, see Ibid 213-217; Rachelle Miller, 'The OSI Model: An Overview' (SANS Institute Information Security Reading Room, 2019) <https://www.sans.org/reading-room/whitepapers/standards/osi-model-overview-543> accessed 9 October 2020.

117 Some believe that the outcome of TCP/IP-OSI war was largely the result of the fact that TCP/IP was deployed first and developed an early lead, which, through network effects, created a 'bandwagon' that OSI could not overcome; whereas others have argued that TCP/IP was, in many ways, superior to the OSI model (Besen and Sadowsky (n 121) 214).

118 Yoo (n 109) 1747; Martin Fransman, *The New ICT Ecosystem: Implications for Policy and Regulation* (Cambridge University Press 2010) 8-11; Rohan Kariyawasam 'Defining Dominance for Bits and Bytes: A new Layering Theory for Significant Market Power?' [2005] 26(10) European Competition Law Review 581, 587; Kevin Werbach 'Breaking the Ice: Rethinking Telecommunications Law for the Digital Age', [2005] 4 Journal on Telecommunications and High Technology Law 59, 66-67; Craig Mc Taggart, A Layered Approach to Internet Legal Analysis, [2003] 48 McGill Law Journal 571, 582.

layer.[119] Coupled with the physical layer, the five-layer internet architecture resembles an hourglass run by the protocols across the layers. The Internet Protocols covering IPv4 and IPv6, or Internet Protocol (IP), simply saying, enables the network to run an arbitrary variety of transmission technologies, which is facilitated by a thin, simple layer in the middle of the protocol stack, like the thin waist in an hourglass, and as illustrated in Figure 2.[120]

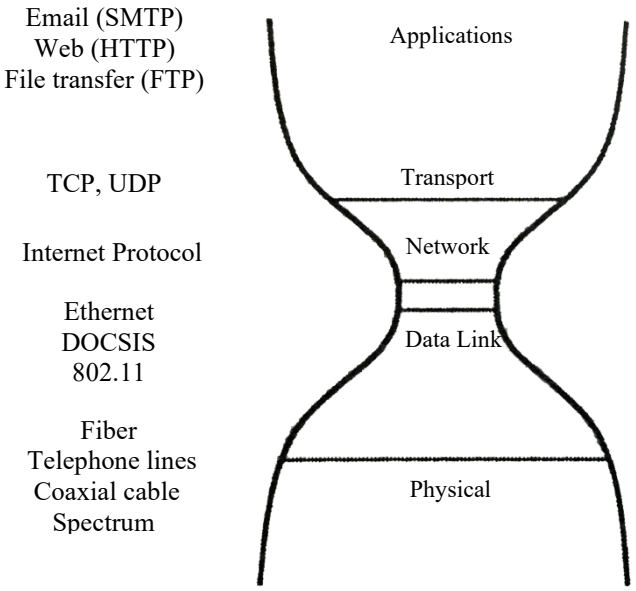

Figure 2: The Hourglass Model of the Internet Protocol Stack

(Source: Yoo (n 109) 1751)

Layers, while defining the value chains through which products and services are ultimately delivered to end-users,[121] also ensure interoperability between the end points by the virtue of governing protocols and interfaces. Fundamentally, all of the layers are software code that manipulates bits of information to form a network

---

119 Four layers (link, application, network, application) identified by the IETF denote the software layers that serve on top of the physical layer, representing the Internet architecture. This physical layer, included into the so-called IP stack (suite) in the shown figure below (Figure 2), should not be understood as a standardised element, but as a scholarly addition by which the infrastructural elements are highlighted as the baseline for all the upper-software layers.

120 Yoo (n 109) 1751.

121 Werbach (n 118) 67.

communications system.[122] Even the physical layer, the most rigidly fixed, includes software and protocols that define how information travels across physical links.[123]

While every layer, including the data link and physical layers, is represented by various protocol(s), the internet (network) layer is exclusively run by the IP. Physical and data link layers are managed at the core of the network, where the central routers hand over the traffic and transmit the bits within the IP cloud. However, the upper layers i.e. transport and application layers, are controlled totally at the hosts. Inter-connections and the flow of information amongst the layers are ensured via the interfaces, the so called protocols, that serve the interdependence between layers, which do not have to coordinate with each other. For interoperability to be achieved across the layers or simply saying for the internet connectivity, the protocols serve as the interfaces to let in and across the layers enabling the functionality of the whole system. They enable flows of information across the layers which would otherwise be inhabited and controlled by the potential gatekeepers..

2.2.2. Convergence

During the legacy period of earlier decades, voice telephony services used to be, and are still partially being, offered over the circuit-switched analogue networks,[124] while the conventional way to provide internet access services was through cable networks. Around two decades ago, internet access commenced to be offered through PSTN-based dial-up mode, which is an overlay method on top of the telephone networks and

122 Werbach (n 118) 67.
123 Werbach (n 118) 67.
124 A circuit switch sets up a dedicated transmission path from the calling party to the recipient for the duration of a call. Circuit-switched networks are networks which establish an end-to-end transmission path in order for a communication to be transmitted from one end to the other, as is illustrated by conventional (PSTN) telephone networks (Walden (n 109) 400).

based on circuit-switch technology. In the cable networks, the single purpose earlier was offering dedicated television, pay TV) services, in rivalry with the free-aerial TV services that were open to everyone. Cable networks were offering TV services to their customers, similar to the terrestrial and satellite networks that were dedicated to broadcasting radio and television signals. Likewise, voice telephony was the primary goal of the legacy PSTN networks that were running through a set of principles, such as Time Division Multiplexing (TDM), which allows the creation of channels within a transmission stream over the telephone lines.

Vertical integration of the telecommunications industry over the course of the 20th century was one of the thrusts behind this single-minded approach. In this structure, traffic was subject to a variety of different rules and pricing regimes because of the legacy business structures and technologies, such as TDM.[125] As a result, each phone company operated as a "silo" of its own, determining the suite of services it would offer to customers and managing the internal addressing and directory processes as integral to those offerings.[126] Hence, the model of telecommunications was point-to-point communications on a two-way switched network, with its own technology e.g. TDM based circuit-switch, its own firms, its own services and its own framework. This 'silo' model was reflected on in the 1996 US Telecommunications Act, whereby 'telecommunication services' are regulated under Title I Act, while Title II is dedicated to regulating the broadcast services, and Title III the cable services. As the decades passed, along with the increasing convergence of networks, services and terminals, this single-minded, application-specific, vertically integrated logic or convention has

125 Werbach (n 118) 62.
126 Werbach (n 118) 62.

vanished, making the regulatory systems, like the US Telecommunications Act, outdated.

For more than two decades, by means of digitalisation, cable networks are able to provide both voice telephony - globally known as Voice over Internet Protocol (VoIP) - and broadband internet, in addition to TV services. Similarly, it is possible to deliver all data, including TV services, along with voice telephony, over the legacy PSTN networks. Using the same physical medium as the telephone networks, the internet has gone through a radical innovation based on "convergence" through two facts: (i) digitisation and (ii) IP connectivity.

In this new era we see various kinds of content e.g. voice, data and video) being transmitted through the internet, within the form of *bits*, short for "binary digits", corresponding to an abstract mathematical representation of the two states of the circuits, which are "on" and "off", for describing anything from the sound of a voice, to a video clip, to a thousand-page document.[127] While this means digitisation, IP connectivity ensures the so-called binary digits go through the internet architecture, namely internet protocol (IP) suite or layered IP stack, as explained below.[128] Based on these thrusts, IP convergence not only enables the signal transmission in a compressed and speedy manner, but also builds up an interoperable ecosystem surrounded by the internet.[129]

---

127 Nuechterlein and Weiser (n 96) 160.

128 For the details of the layered IP stack, see the section '2.2.3. Architectural underpinnings of the internet: Layered IP Stack'.

129 Regarding the multi-dimensional analysis of convergence, see J. M. Bauer, M. P. C. Weijnen, A. L. Turk, and P. M. Herder, 'Delineating the Scope of Convergence in Infrastructures' in W. A. H. Thissen and P. M. Herder (eds), *Critical Infrastructures State of the Art in Research and Application* (Kluwer Academic Publishers, 2003) 209-232. For discussion of the convergence dynamics with a policy elaboration on Internet regulation see Philip Weiser, 'Networks Unplugged: Towards A Model of Compatibility Regulation Between Information Platforms' (29th TPRC Conference, Washington, September 2001).

The internet runs on top of the standardised protocols, mainly based on Internet Protocols (IP), which secure interoperability across the globe. As long as these protocols are adopted and implemented, all sorts of digital content can be transmitted over any kind of physical infrastructure, whether wired (cable, copper, fibre) or wireless (mobile, terrestrial, satellite). In this environment, cable can deliver voice and internet services as well as television service; wired telephony providers can deliver voice service and internet service; wireless telephony providers can also deliver internet service, streaming video and other services; and voice service, audio or video broadcasts, streaming video, audio downloads and more services can be delivered over the internet, provided by ISPs – over cable, DSL or mobile technologies or modems.[130] The convergence, as exemplified above, is truly realised by the virtue of IP which permits multi-level interactions between the networks, terminals and services, as manifested below (see Figures 3 and 4).

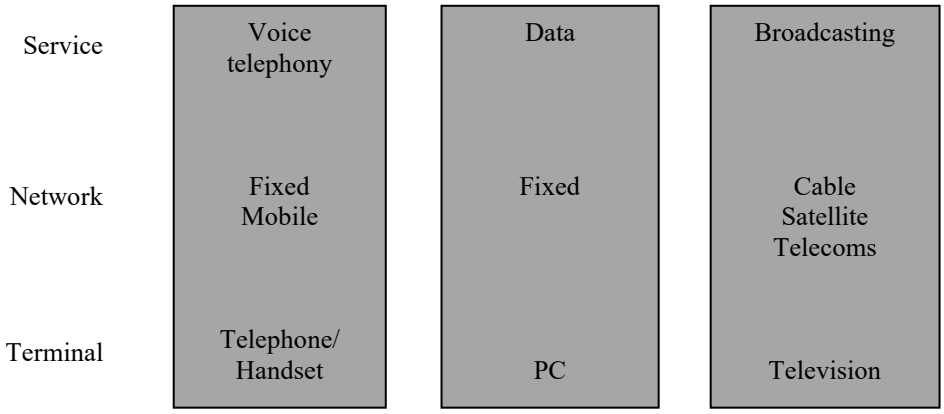

Figure 3: Before convergence

[130] Douglas C. Sicker and Lisa Blumensaadt, 'Misunderstanding the Layered Model(s)' [2006] 4 Journal of Telecommunications and High Technology Law 299, 304.

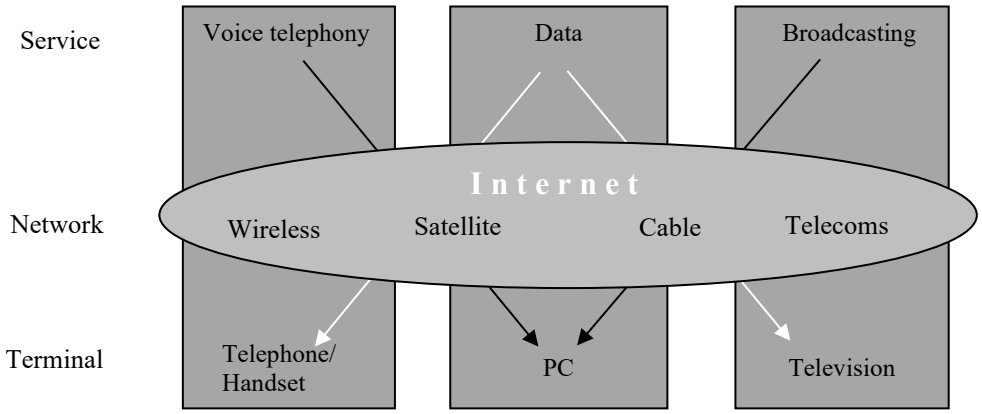

Figure 4: After convergence

(Source: 'EU Telecommunications Regulations & Law' Conference Proceedings, Brussels, June 2002).

The internet should be understood as a conceptual aggregation of many individual networks, most of which are privately owned, using a common protocol and addressing scheme in the allocation of IP addresses to each connected device and for transporting packets of 1s and 0s between computers and other smart devices.[131] In the internet environment, computing or information technologies are thus coupled with electronic communications, previously called "telecommunications". Going through the convergence, internet and surrounding technologies denote a historical process which also characterises the transition from legacy networks to the NGNs, as explained below.

2.2.3. Transition from legacy networks to NGNs

ICT networks enable their users to communicate and/or exchange data with each other. Out of the wide-ranging ICT networks, some rest on their one-way, point-to-

[131] Nuechterlein and Weiser (n 96) 19. For an alternative definition of the 'internet' see Rohan Kariyawasam, 'Interconnection, Access and Peering: Law and Precedent' in I. Walden and J. Angel (eds), *Telecommunications Law* (Blackstone Press Limited 2001) 185, reading; "The internet is the interconnection of a whole range of packet-switched networks, some of which are virtual, most of which are in the public domain, and some of which are private".

multipoint, connections, while some others mean mutual, point-to-point, connections. Use of a decoder to receive digital signals and translate them into analogue signals on the TV screen is an example of the former, whereas voice telephony taking place through point-to-point (P2P) connections, represents the latter. At the heart of both the one-way and P2P access/interconnection lies 'interoperability' across the converging networks i.e. broadcasting, electronic communications and the computing (IT) networks. While IP convergence involves a wider range of interoperability, the basic or primitive forms of ICT networks also rely on and operate based on interoperability.

In a circuit-switch, legacy telephone network (Public Switched Telephone Network, known as a PSTN), the signals are controlled and switched at the central (core) network, with interoperability between the end-users being secured through the switching and routing capabilities of the networks and with the help of electric and electromagnetic transmission.[132] Today's circuit switches are essentially very large computers that, in addition to establishing circuits for given calls, perform a variety of other "intelligent" functions, including call forwarding, caller identification, call waiting and billing.[133] Whereas all these functionalities take place within a hierarchy, all management is conducted at the centrally owned and controlled network exchanges.

Unlike circuit-switched networks, "connectionless" packet-switching technologies do not set up a dedicated circuit for the duration of a communication. Instead, the transmitted information is converted into discrete digital packets, and the packet switch sends each of them separately from the others, potentially along different transmission paths.[134] In packet-switching technology used for broadband data transmission, all data

[132] Nuechterlein and Weiser (n 96) 25.
[133] Nuechterlein and Weiser (n 96) 29.
[134] Nuechterlein and Weiser (n 96) 30.

packets follow the shortest possible way to arrive at the identified destination (after-by-after). This brings enormous efficiency and flexibility, enabling the network operators to manage all end-to-end data transmission within the same network management system. Packet-switched technologies are increasingly being used to carry voice, as well as data, and operators are using packet-switched architectures when modernising their backbone and access networks to NGNs.[135]

The internet is made up of interconnected, or linked, packet-switched networks, representing the very evolution from circuit-switched networks into a globalised form. Standardised internet architecture and connectivity is also crucial for the development of NGNs. The choice of the internet as a single packet-switching technology for the ICT world has raised the need for the standardised integration of different architectures, concepts, approaches, and services found in traditional and modernised types of telecommunications.[136] Such need and accompanying efforts have ended up with the standardisation process of the so-called NGNs in the first decade of the 21st century.[137] ITU, having a pioneering role in this process, defines "NGN" as follows:

> NGN is a packet-based network able to provide telecommunication services to users and able to make use of multiple broadband, QoS-enabled (quality of service) transport technologies and in which service-related functions are independent of the underlying transport-related technologies.[138]

---

135 Walden (n 109) 400.
136 Janevski (n 110) 69.
137 Janevski (n 110) 69.
138 ITU-T Rec. Y.2001. See also <http://www.itu.int/ITU-T/studygroups/com13/ngn2 004/working _definition.html> accessed 9 October 2020.

While the era of broadband internet access represents a transition from application-specific homogenous service provision; traditional circuit-switched voice telephony and TV broadcasting on the one side, best-effort internet on the other, to IP-based heterogenous service provision,[139] with the emergence of NGNs means standardised QoS-based networking capabilities furthering the so-called transition.[140] The most prominent and innovative aspect of these newly emerging networks is their potential to drive the all-IP migration based on the QoS parameters.

NGNs, whether fixed or mobile, represent a new upgrade of networking technologies, if not a revolution.[141] Significant changes are brought about by the NGNs surrounding *decoupling* of the services from the networking and accompanying advantages that enable the service providers to provide multiple service packages, consisting of voice, data and video, in a far more efficient and high-speed manner.[142] In a NGN environment, networks are simply configured to convey data, while services are controlled by software programs embedded in ubiquitous computers.[143] This process, echoed with the 'decoupling', facilitating triple or quadruple play service provision, enables third party application service providers to more effectively compete with the operator of the physical network in the provision of services.[144] All these

---

139 See Volker Stocker 'Interconnection and Capacity Allocation for all-IP Networks: Walled Gardens or Full Integration?' (43rd TPRC Conference, Arlington, September 2015) 3.

140 According to legacy models enforced by the "best effort" principle, TCP/IP based passive traffic management is performed by communicating edges (Ibid). On the other hand, differentiated traffic services based on active traffic management, incorporating virtualisation of network functions and capacity allocation between different service types manifest the multi-purpose NGNs, also representing the so-called all-IP process.

141 See Janevski (n 110) 69-70.

142 Decoupling thus marks a core difference from the legacy (internet overlay) networks, which are modernised to provide internet services, although being originally designed to support specific services, such as voice telephony over PSTN and TV broadcasting over terrestrial, satellite and cable networks. In a NGN environment, networks will simply be conveying data while services are going to be controlled by software programs embedded in ubiquitous computers.

143 See Wolfgang Reichl and Ernst-Olav Ruhle, NGA, IP-Interconnection and their Impact on Business Models and Competition [2008] 69, 1st Q Communications & Strategies 41, 49-50.

144 J. Scott Marcus and Dieter Elixmann, 'Regulatory Approaches to NGNs: An International Comparison' [2008] 69, 1st Q Communications & Strategies 19, 21.

developments denote the trajectory of how the IP convergence evolves along with the modernisation of networks.

3. Legal regulation of interoperability

3.1. General overview

3.1.1. Interoperability debate

As many firms attempt to exercise proprietary control over the interfaces they run, how to ensure interoperability becomes one of the Gordion knots to be solved in the field of ICT. Crucially, interoperability information is non-rivalrous in many cases,[145] potentially drawing the boundaries of follow-on innovation and market competition. From a broader perspective, one could also say that transmission of information to the third parties in an uninterrupted and seamless way would serve a great many concerns being resolved surrounding cultural freedom and social production. On the other hand, interoperability debate and related solutions seem to have been portrayed within ascertained boundaries of each body of law, i.e. under IPR, competition and sector-specific rules.

From the IPR viewpoint, the interoperability debate basically means whether and to what extent copyright or patent or trade secret holders ought to permit their IPR-protected assets being used/accessed by third parties. Not only IPRs themselves, but also DRMs and TPMs, which are categorised differently yet legally protected,[146] exemplify the tools for retaining the interfaces, via which incumbent firms could close up their systems to third parties. This however would mean technologically blocking new entries and/or derivative products, particularly when IPR-protected assets depict a marketplace.

---

145 See Kevin Coates, *Competition Law and Regulation of Technology Markets* (OUP 2011) 237.
146 See supra note 73.

Against this background, it becomes questionable when the rights holders conceal the interface specifications by distributing software only in object code, and using legal mechanisms e.g. copyright, patent, and anti-circumvention laws to prevent any decryption or decompilation which aims at uncovering such specifications.[147] Therefore, the issue from the IPR perspective revolves around how IPR exceptions are established statutorily and by precedents, incorporating the counter-legal mechanisms that would preclude reverse engineering, etc.

From the competition law perspective, the question turns into whether lack of interoperability in different settings e.g. abuse of dominance, collaborative and concentrative acts would result in exclusion of the potential or actual competitors in an ICT market - which would presumably be occupied by dominant firm(s) that rely on critical (often IPR-protected) assets, software or a platform. This might create a tension from the competition point of view, since in such cases APIs might function as the 'gateways' for the third parties to interoperate with and compete against the incumbent networks. Such tension is often augmented in the face of network industries, which are exposed to 'network effects' and may not be subject to ex-ante regulations.

Ex-ante interoperability rules are embedded within the context of sector-specific (electronic communications) regulations, as exemplified by the ECRF. The ECRF itself is originally structured and built on the premise of achieving interoperability between networks and services for the well-being of EU citizens and consumers. Mirroring the end of ensuring access and interconnection at the highest possible level, interoperability has so far been emphasized under the ECRF, through specified rules

147 Band and Katoh (n 55) 184.

i.e. mandatory access to CASs and mechanisms i.e. standardisation. That is to say, a number of ex-ante interoperability-based measures are embedded under the ECRF, to be invoked in tandem with the ex-post competition rules. Below, firstly, the main concerns surrounding lack of interoperability are given, and then introductory information about each EU legal regime is given respectively.

3.1.2. Main concerns surrounding lack of interoperability

ICT interoperability entails various technical parameters based on the real-life situation, user needs and requirements. So, lack of interoperability emerges as a common problem for ICT networks and services, which essentially depend on seamless and uninterrupted communication and data exchange. However, this is not the default or inherent situation found in many cases because of the proprietary/closed systems, accompanying abusive behaviours, exploitation of consumer loyalty and/or inertia, network effects, etc. While these factors are conducive to the lack of interoperability and its adverse effects, the potential outcomes include but not limited to vendor lock-in, switching costs, restricted follow-on innovation, hampered end-to-end connectivity, lessened cultural production and freedom.

Often representing network industries, ICT networks/services manifest either de facto or de jure standards and/or path dependencies caused by network effects. This situation first and foremost brings out the very possibility of 'vendor lock-in'. Vendor, or technology, lock-in means a product being opted for by the consumers when they are reluctant to switch from that product, even for a better one, either due to switching costs or because they are lazy (euphemistically called "end-users inertia" by the

Commission).[148] While vendor lock-in is not necessarily unwanted in every situation e.g. for small and medium size enterprises' market penetration and innovation, switching costs following up vendor lock-in would be criticised for many reasons.

Switching costs are mentioned as a barrier for a firm to overcome when it wishes to enter a market after a small but permanent price increase.[149] There is theoretical and empirical research showing that consumer switching costs confer market power on firms.[150] Given this fact, switching costs might have an impact of slowing or preventing market entry as well as creating consumer harm, particularly when the impact stems from the consumers sticking to technologically inferior products available in the relevant market. The systemic impact arises from the struggle over interoperation and compatibility, when firms are likely to exploit captive markets by raising prices to locked-in consumers to the height of switching costs - this can lead them to compete extensively by investing in incompatibility.[151] Having said this, a clear link could be established between lock-in risk, reinforced by the switching costs, and market tipping/foreclosure that resulted from network effects; where in many cases these consequences are driven by the lack of interoperability.

Lack of interoperability across the ICT networks, including the IoT and cloud platforms, might have anti-competitive effects particularly in the presence of network effects. This risk is directly corelated to the scenarios when consumers face interoperability problems because of the incompatible files, devices and/or software

148 Suiyi Zhang, 'How have network effects affected the European Commission's enforcement of competition law in technology enabled markets?' [2015] 36 European Competition Law Review 82, 85.

149 Tom Björkroth, 'Loyal or Locked-in – And Why Should We Care?' [2013] 10(1) Journal of Competition Law & Economics 47, 54.

150 Ibid, 47.

151 Jonathan Cave, 'Prisoners of Our Own Device - An Evolutionary Perspective on Lock-in, Technology Clusters and Telecom Regulation' (*SSRN*, 15 August 2009) TPRC 2009 <http://ssrn.com/abstract=1995551> accessed 9 October 2020.

that are used by the service e.g. cloud providers.[152] Such problems would surface more should customers opt switching from one provider to another. Normally, the fact that a cloud computing provider decides to choose a specific antivirus software could be interpreted as a choice over which customers should not have a say.[153] Thus, not only security programs but also other software used by the cloud users would confer lock-in risk for the consumers, unless switching costs are eliminated by fierce competition or statutory portability mechanisms. Similar concerns are valid for the IoT context, whereby the consumers would be hindered from moving to a new platform because of the switching costs.[154] As this is usually attended by the proprietary and non-interoperable platforms, competitors would then be excluded e.g. in the absence of countervailing buying power that ameliorates the network effects.

---

152 The essence of the problem is that each vendor's cloud environment supports one or more OSs and databases, incorporating a cloud API and a specific licensing model (Bill Claybrook, 'Cloud interoperability: Problems and best practices', (*Computerworld*, 1 June 2011) <http://www.computerworld.com/article/2508726/cloud-computing/cloud-interoperability--problems-and-best-practices.html> accessed 9 October 2020). Therefore, undertakings may exploit the fact that their customers have been locked into their cloud computing service and impose the use of their own software (Laise Da Correggio Luciano and Ian Walden, 'Ensuring competition in the Clouds: The role of competition law?' (*SSRN*, 7 April 2014) <http://ssrn.com/abstract=1840547> accessed 9 October 2020).

153 Luciano and Walden (n 152) 274. In fact, in case a cloud customer adapts their systems to work with one particular cloud service, they may not be able to choose an equivalent service from a different provider without having to adapt their systems again for the new provider. In order to make the cloud systems interoperable with each other, issues such as transport protocols, encoding syntaxes for communication messages or data, semantics, and organisational and legal policy issues need to be addressed. (ECIS, 'Special paper on cloud computing: Portability and interoperability of software and data across cloud services' (27 June 2016), <http://www.ecis.eu/2016/06/special-paper-on-cloud-computing-portability-and-interoperability/> accessed 9 October 2020. See also Andrea Renda, 'Competition, neutrality and diversity in the cloud' 85 [2012] Digiworld Economic Journal 1st Q 23 28-30; Sluijs, Larouche and Sauter (n 25) 18.

154 Karen Rose, Scott Eldridge and Lyman Chapin, 'The Internet of Things: An Overview' (Internet Society, 2015) 47 <http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf> accessed 9 October 2020. For example, in the home automation market, light bulbs from one vendor may not be interoperable with a light switch or control system manufactured by another (Ibid).

In the case of *contestable* markets, which are depicted by low barriers to entry and exit along with short-term prices and price-sensitive consumers,[155] such problems would not exist nor does a disruptive effect emerge over the competitive functioning of the markets. Against such a potential for competition and when switching is easy and fast, lack of interoperability would no longer have the effect of preventing new entries and/or innovation. In most cases, ICT markets are not representative of contestable markets because of the network effects and the potential for market tipping; and lack of interoperability thus would bear far-reaching negative implications in these markets.[156]

On the other hand, interoperability-based problems in the ICT sector are not limited to vendor lock-in, switching costs, etc. As a matter of fact, the interoperability-centric problems are not exclusively related, or conducive, to anti-competitive behaviours and/or the hampered follow-on innovation. Alongside the competition and innovation related concerns, some other consequences would also result from lack of interoperability surrounding restricted consumer choices and information flows. A broader viewpoint is compelling to understand such adverse effects and consequences which often go beyond the conventional understanding of consumer harm and reach out to media pluralism, cultural diversity, etc.

In this regard, 'end-to-end connectivity' or broadly speaking 'any-to-any communication' is the first and foremost issue that needs to be underlined and addressed. In fact, without the interoperability standards/protocols, any person could

---

155 José Alberro and Rainer Shcwabe, 'The Theory of Contestable Markets and its Legacy in Antitrust Practice', [2016] 16(1) Economics Committee Newsletter 20, 21.

156 In order to deter such potential outcomes, statutory rights and obligations, particularly 'data portability', should be underlined as lessening the risk of vendor lock-in, or of switching costs. For detailed information regarding 'data portability', see the section '3.2.4. Data protection rules: Right to data portability'.

not communicate with anyone else. Expressed with the term 'end-to-end connectivity', this situation confers interoperability a crucial meaning and purpose. By the same token, the ECRF has a number of obligations inclusive of interoperability, mostly echoed by the 'interconnection' imposed on the telecom operators that ensure end-to-end connectivity. Under the ECRF there also exists another obligation based on interoperability, aiming at the transmission of digital TV signals through the set-top boxes, i.e. CAS systems, on a fair, reasonable and non-discriminatory basis. This latter obligation, unlike interconnection, aims at enhancing media plurality and cultural diversity.[157]

Interconnection and CAS obligations aim to address interoperability-based concerns not necessarily related to market competition or innovation. While they might have competitive implications, these obligations mainly address the concerns surrounding the media plurality and diverse cultural productions which can be extended to participatory democracy.[158] Access and interoperability obligations under the ECRF, as examined above, serve such concerns being mitigated in relation to the intermediary network and platforms that control the information flows.

'Information flow', which was first conceptualised by Elkin-Koren,[159] has a particularised meaning for this study by which to emphasize information being disseminated and exchanged across the end points. The exclusionary effect of the IPRs

157 See the section '6.2.1.2. Conditional access obligations'.

158 See N. Elkin-Koren, 'Cyberlaw and Social Change: A democratic approach to copyright law in cyberspace' [1996] 14 Cardozo Arts and Entertainment Law Journal 215, 231, referring to Seyla Benhabib, 'Models of Public Space: Hannah Arendt, the Liberal Tradition, and Jürgen Habermas' in Craig Calhoun (eds) Habermas and the Public Sphere (MIT Press 1991) 87, reading; "when democracy is defined not merely by formal political institutions, but as a process of "discursive will formation," participation is no longer confined to a narrowly defined political realm, but is instead perceived as an activity that can be realized in the social and cultural spheres as well"

159 Ibid, 257.

surfaces here since the access-denied (or restricted) content is often not tangible nor in a bounded form but would often have a fluid form transcending the boundaries of ICT networks/platforms. This transition, namely from the 'stock's to 'commodity flow's,[160] needs to be noted as a key change driven by the ever fast evolving ICTs and the accompanying 'networked information economy'.[161] In this regard, commodified information coming up with the fluidity through codes and bits bring out the question as to the appropriateness of the stock-focused property regimes including IPR rules, particularly against the key role of information flows in the digital age.[162] While responding this question goes beyond the scope of this study, it is noteworthy that the construction of information is not reflected merely through classification, but also through the network of links that creates the path which leads to the information.[163] Having said that, not only (theoretical) access rights[164] or permitted circumvention of

---

160 James G.H. Griffin, 'A call for a doctrine of "information justice"' [2016] 1 Intellectual Property Quarterly 44, 45-46.

161 According to Benkler, "radical decentralization of intelligence in our communications network and the centrality of information, knowledge, culture, and ideas to advanced economic activity are leading to a new stage of the information economy - the networked information economy" (Yokhai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006) 32).

162 Griffin describes this contradictory situation along with a unique exposition inspired of quantum theory:

> The increasing convergence of capital and information, and their quantum states in the information society, undermines the traditional notion of bounded property. In addition to that, the information itself is increasingly digital and thus potentially literacy in character, which paradoxically presupposes a greater degree of bounded proprietary protection. However, the reality is that the growth in copyright scope matches directly - an exponentially - with the desire to increase protection of information concerning content use. Thus, any increase in the copyright's proprietary protections and consequent bounding is intimately tied with the quantum aspect of legal protection not just being bounded but also being a flow. (Griffin (n 160) 46-47).

163 Elkin-Koren (n 158) 238.

164 Marcella Favale, 'The Right of Access in Digital Copyright: Right of the Owner or Right of the User?' [2012] 15(1) The Journal of World Intellectual Property, 1-25; Zohar Efroni, *Access-Right: The Future of Digital Copyright Law* (OUP 2011) 146-149; Marlize Conroy, 'Access to Works Protected by Copyright: Right or Privilege' [2006] 18(4) South African Mercantile Law Journal, 413-422; Jane C. Ginsburg, 'Essay: From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law' [2003] 50 Journal of the Copyright Society of the U.S.A., 113-132; Stephen B. Popernik, 'The Creation of an Access Right in the Ninth Circuit's Digital Copyright Jurisprudence' [2013] 78(2) Brooklyn Law Review, 697-740.

access controls e.g. as enshrined under DMCA under certain conditions,[165] but also, even more importantly, information flows across the technological layers, networks and platforms gain importance in the current ICT landscape.

Decentralisation and diffusion of power is not the same thing as less power exercised over human beings; nor is the same thing as democracy.[166] Power does no disappear in a digital networked world, and shifts from the arbitrary will of specific individuals and the imperatives of large bureaucratic organisations to the channelling effects of software code, surveillance technologies, and information networks.[167] Although we are increasingly integrated into information networks in some ways, we are also alienated from them in others,[168] which would mean restricted information flows as well as increased control over content.

As underlined by Elkin-Kohen, concentration of ownership and control over content may reduce pluralism and result in a "marginal" or "meaningless" diversity of the type of content created.[169] Control over content may affect the extent to which people can

---

165 17 U.S. Code § 1201 (d), (e), (f), (g), (h), (i), (j).

166 Jack M. Balkin, 'Information Power: The Information Society from an Antihumanist Perspective' in Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information: Legal, Social, and Cultural Perspectives* (New York University Press 2011) 232, 240.

167 Ibid, 239-240. Proliferation of power, as elaborated and put forward by Karl Marx, Max Weber and Michel Foucault, would have different forms and appearances, which seems to continue in the internet driven world. Although not directly covered within the subject-matter of this study, the idea of power proliferation is note-worthy. As emphasized by Balkin, a proliferation of power perspective argues that the information technologies which human beings implement to transfer, store, and analyse information do not necessarily bring a net increase in either human freedom or human empowerment (Ibid, 239).

168 Ibid, 240.

169 See Niva Elkin-Koren, 'It's all about control: Rethinking copyright in the new information landscape' in N. Elkin-Koren and N. Weinstock Netanel (eds), *The Commodification of Information* (Kluwer Law International 2002) 79, 102. Elkin-Koren explains the relationship between the power (or concentration of ownership) and control over content as follows:

> "… those who control the means of arranging and tagging information possess the power to impose specific meanings. The more control one has over information resources, the more one is able to impose her meanings and force users to conform to those meanings" (Elkin-Koren (n 158) 238-239).

appropriate content and adapt it to reflect their own agenda.[170] From the viewpoint of information flows, this would also lead up to the information asymmetries as well as non-transparencies on the part of the dominant information actors or agencies. Ultimately, this would encourage these actors/agencies to be gatekeepers that have the capacity to exploit the consumers and maximize capital flow from this.

As far as informational goods are concerned, the viewpoint one should have needs to be elaborated with civic virtue because information users would better be captured by the term 'citizens' rather than 'consumers'. Information flow concerns would thus need to be taken of utmost account also considering the enabling tools of 'interoperability' against the gatekeeping roles and functionalities. While interoperability measures would increase the spectrum for information goods, its absence would mean not only heightened control mechanisms but also lacking links between the parties that would impart and receive the information. Considering this and other consequences resulting from lacking interoperability, one could draw out a number of concerns in relation to interoperability.

In the figure below, could be seen the manifestation of the major concerns that potentially result from the lack of interoperability.

[170] Elkin-Koren (n 169) 103.

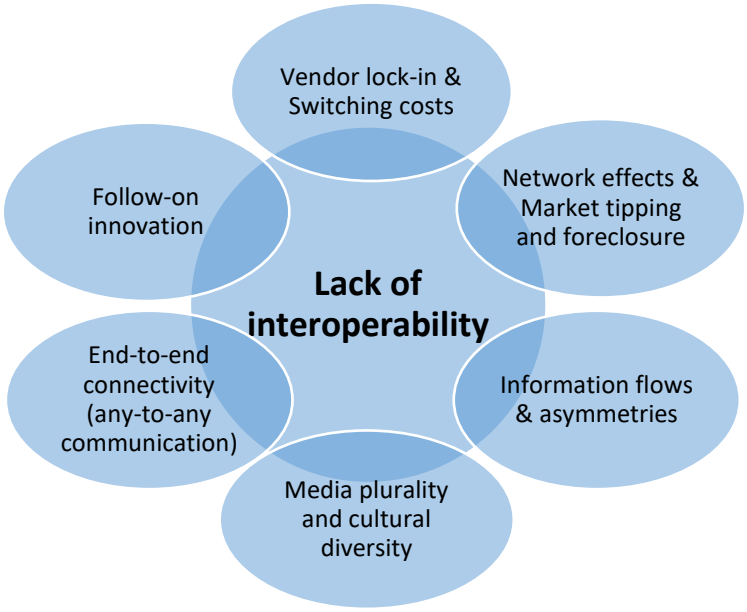

Figure 5: Major concerns surrounding lack of interoperability

Source: Constructed by the author

3.1.3. Brief analysis of major concerns on the cumulative ground of 'gatekeeping'

As the above figure denotes, 'lack of interoperability' would cause several concerns. Such concerns could be analysed within two main groups, based on their most salient aspects, more explicitly, for predominantly having an economic, mostly *competition-oriented* or non-economic, mostly *techno-social* nature.[171] The former group reflect the concerns surrounding vendor lock-in, network effects and (hindrance of) follow-on innovation, whereas latter group of concerns i.e. end-to-end connectivity, media

[171] 'Techno-social' is one of the key attributes used in this study inspired by the work of Frischmann, and Selinger who authored a book called 'Re-Engineering Humanity'. In their book, they define and frequently refer to the term of 'techno-social engineering'. According to their definition, techno-social engineering refers to "processes where technologies and social forces align and impact how we think, perceive and act" (Brett Frischmann and Evan Selinger, *Re-Engineering Humanity* (Cambridge University Press 2018) 4-5). Based on this definition, the techno-social concerns is conceptualised to mean the concerns mostly manifested in algorithmic/AI-driven software that manipulates online users affecting their behaviours and choices leading up to unfair outcomes and/or transformative effects.

pluralism and information asymmetries, is constructed separately for the arising informational, societal and epistemological consequences out of the underlying ICT architectures. We cannot radically isolate these concerns since these information or media related aspects also entail economic factors or implications, if not to the same degree one would expect of the former group of concerns.

Hereby, it is important to distinguish that every ingredient of the emergent 'network information economy' is not calculable and would not fit into the traditional market economy or competition law and policy mindset. Pursuing competition law terms, one should need to look to the 'consumer welfare' or to 'total welfare' according to the US antitrust law, seeking out an answer as to whether there exists any potential or actual consumer harm for the conduct, agreement or merger scrutinised. If an action of a dominant firm is likely to harm consumers by reducing the 'consumer surplus' which is mostly calculable, then that firm falls into the spotlight of the competition or regulatory authorities. On the other hand, this could hardly be gauged against the latter concerns which potentially and primarily mean restrictions over information flow and freedom.

Should we reconsider the 'consumer welfare' from a broader viewpoint elaborated with the civic virtue around the information flows, a distinction between the abovementioned concerns would be easier. Benkler's discursive analysis concerning the individual autonomy and information environment would be helpful understand such distinction:

> To understand the effects of concentration, we can think of freedom from constraint as a dimension of welfare. Just as we have no reason to think that in a concentrated market, total welfare, let alone consumer welfare, will be optimal, we also have no reason to think that a *component of welfare* – freedom from constraint as a condition to access one's communicative environment – will be optimal.[172]

Flowing from Benkler's point of view, it should be noted that the welfare components are not limited to the consumer welfare or surplus that is calculable and is acknowledged necessary to find out the Pareto efficiency or optimality. In fact, defining an optimal person extends to civic virtue that is not quantifiable and largely related to existence of participatory culture and democracy within a society. Citizens develop their ideas, shape their positions, identify their interests, and ascertain their identity in the public sphere, which represents the main scene of our democratic life.[173]

It is recognizable that digital fences are heightened in the internet era, which brings out significant costs and consequences as opposed to the supposed outcomes of internet freedom and liberties.[174] That is to say, in the digitised IP world, stronger

---

172 Benkler (n 161) 157.

173 Elkin-Koren (n 169) 101.

174 The advent of internet marked emergence of a concern on the part of the rights holders for the ease and low cost of access to and copy of the available materials online. The perceived internet threat was based on the rhetoric "as copying costs approach zero, intellectual property rights must approach perfect control" (See James Boyle, *The Public Domain: Enclosing the Commons of the Mind* (Yale University of Press 2008) 61). The repercussions were largely reflected in the Clinton Administration's 'Report of the Working Group on Intellectual Property Rights' published in 1995, called 'White Paper', that preceded the DMCA and set out the copyright and information policy principles of the US while entering the internet era. As well established by Vaidhyanathan, 1995 White Paper represented four surrenders of important safeguards in the copyright system:

- The surrender of balance to control: As a result of the chief piece of legislation in subsequent years, the DMCA; content providers can set the terms for access to and use of a work.
- The surrender of public interest to private interest: The rhetoric of "intellectual property" in the 1990s was punctuated by appeals to prevent theft and efforts to

effects could be found out in overzealous use of IPRs and TPMs, which often function as newly erected digital fences enabling 'perfect control',[175] and are ironically protected by the modernised copyright and patent laws.[176] In effect, such heightened digital fences i.e. through highly increased TPMs and IPRs, mean barriers preventing free flow of information[177] having the potential to affect participatory democracy as well as cultural production.[178] These informational barriers, which would mean a strain over the democratic culture,[179] augment the concerns categorised in the latter group.

From this vantage point of view, one might ask to what extent all the major concerns referred above are addressed under the *status quo.* Or it would be asked how far these concerns and their omnipresence are infused under the EU regulatory thinking. Leaving these questions to the relevant parts of the thesis, suffice it to say, co-existence

---

extend markets. There was little public discussion about copyright as a public good that can encourage a rich public sphere and diverse democratic culture.

- The surrender of republican deliberation within nation-state to unelected multi-lateral nongovernmental bodies: WIPO and WTO assumed a greater role in copyright policy as multinational media companies sought global standards that satisfied their ambitions.
- The surrender of culture to technology: The DMCA forbids any circumvention of electronic locks that regulate access to copyrighted material" (Siva Vaidhyanathan, *Copyright and Copywrongs: The rise of Intellectual Property and How It Threatens Creativity*, (New York University Press 2001) 159-160).

175 Boyle (n 174) 60-62; Lawrence Lessig, *Code; version 2.0* (Basic Books 2006) 176-180. According to Lessig, the 'perfect control' which he coins with 'trusted systems' "provide the authors with the same sort of protection [of copyright laws]". He puts forth his firm and substantiated reasoning as follows:

> Copyright orders others to respect the rights of the copyright holder before using his property; trusted systems give access only if rights are respected in the first place. The controls needed to regulate this access are built into the systems, and no users (except hackers) have a choice about whether to obey them. The code complements the law by codifying the rules, making them more efficient. (Ibid, 179)

176 Vaidhyanathan (n 174) 159, 174-175; Lessig (175) 186; Boyle (n 174) 61, 100-101.

177 Niva Elkin-Koren, 'Copyrights in Cyberspace - Rights without Laws' [1998] 73 Chicago-Kent Law Review, 1155, 1192. Regarding free flow of information, see Elkin-Koren (n 169) where it is argued that "control rather than remuneration becomes the focus of legal disputes concerning copyright" (p. 84) and "this transforms copyright law from a law that sought to serve policy goals and secure incentives for creators into a law that facilitates control in information markets" (p. 106).

178 See Elkin-Koren (n 158) 267-268.

179 See Emily B. Laidlaw, *Regulating Speech in Cyberspace; Gatekeepers, Human Rights and Corporate Responsibility* (Cambridge University Press, 2015) 33, 46; Balkin (n 166) 240, 244-5.

of both competition and techno-social concerns highlighted above compels regulatory thinking to have a broader mind-set. While the following chapters aim at filtering out all the available measures and shortcomings, suffice it to say here that there is a pressing need to comprehend all the major concerns under a common ground. At this point, this thesis takes a step further to synthesise these concerns on the cumulative ground of 'gatekeeping'.

'Gatekeeping' has been used as a term mostly in field of media and communication studies, since it has been conceptualised by Kurt Lewin[180] and David Manning White, who first applied gatekeeping theory in journalism research.[181] White analysed how a single editor of a local newspaper selected which stories were and were not covered, and found that the news was heavily influenced by the individual preferences of the editor.[182] The people that are in a strong position to influence this selection process have been conceptualized as gatekeepers: they control gates in the communication channels through which news flows into society.[183] While this type of gatekeeping suggests an 'intermediary' role, this should not be considered as the defining aspect, since these actors do not necessarily operate on a multi-sided platform or network. Rather, their exploiting the so called 'gates' as a controlling mechanism is crucial to understand this concept.

---

180 Lewin, who coined gatekeeping, was interested in understanding how widespread social changes can be promoted, and studied this by analysing the factors that influence food consumption habits (Kasper Welbers, 'Gatekeeping in the Digital Age' (PhD Thesis, Vrije Universiteit Amsterdam 2016) 26, referring to K. Lewin 'Frontiers in group dynamics II: Channels of group life; social planning and action research' [1947] 1(2) Human Relations 143-153).

181 Ibid, 3.

182 Ibid.

183 Ibid, 1.

This notion of 'gated' and controlling access to it seems to be key also in view of the 'network gatekeeper theory' developed by Barzilai-Kahon, who introduces his theory of 'network gatekeeping' based on the concept of 'information control'.[184] According to her, network gatekeeping is best conceptualized through information control lenses, and carries three main goals: (a) a "locking-in" of gated inside the gatekeeper's network; (b) protecting norms, information, gated, and communities from unwanted entry from outside; and (c) maintaining ongoing activities within network boundaries without disturbances.[185] Based on this premise, gatekeeping activities, according to Barzilai-Kahon, include, among others, selection, addition, withholding, display, channelling, shaping, manipulation, repetition, timing, localization, integration, disregard, and deletion of information.[186]

In view of the human rights to be used by the gated and the emerging impact on the 'democratic culture', Laidlaw constructs a new definition of gatekeeping resulting in a model of 'internet information gatekeepers'.[187] This rights-oriented notion of gatekeeping builds upon the traditional gatekeeping concept, together with a classification of micro and macro gatekeepers, to be determined according to the extent to which (i) the information has democratic significance and (ii) the reach or structure

---

184 Karine Barzilai-Nahon, 'Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control' [2008] 59(9) Journal of the American Society for Information Science and Technology 1493, 1496. See also Karine Barzilai-Nahon, 'Gatekeeping: A critical review' 2009 43(1) Annual Review of Information Science and Technology 1, 44.

185 Ibid, 1496. According to the author, "In a network context, this definition [of gatekeeping] is translated to treat gatekeeping as a type of control exercised on information as it moves in and out of gates, and provides one of the broadest views of gatekeeping" (Ibid, 1496).

186 Ibid. The mechanisms include, for example, channelling i.e. search engines, hyperlinks; censorship i.e. filtering, blocking, zoning; security i.e. authentication controls, integrity controls and access controls; value-adding i.e. contextualisation, customisation, personalisation; infrastructure i.e. network access, network configuration; user interaction i.e. add-on, navigation tools; editorial mechanisms i.e. technical controls, content controls, design tools of information content (Ibid, 1498).

187 Laidlaw (n 179) 47.

of the communicative space.[188] While this definition and classification would serve reinvigoration of the concept against the far-reaching consequences, particularly in relation to protection of human rights, subtle differences seem to exist between the traditional gatekeeping concept or the network gatekeeping concept theorised by Barzilai-Nahon and the one developed by Laidlaw in terms of their approach to the access and information controls employed by the gatekeeping firms. Among these, Barzilai-Nahon's theory comes to the forefront providing an interdisciplinary layout and perspective as to the information controls, also laying the foundation for Laidlaw's model. On the other hand, Laidlaw's attempt to create a socio-legal framework governing the gatekeepers and their activities is notable, although open to critique for the featured remedial mechanisms conflated with the extra-legal tools and their complicated interplay.[189]

As the above analysis suggests and summarised by Helberger et al., two major types of gatekeepers can be roughly distinguished: (i) gatekeepers which control access to information and (ii) gatekeepers which have a facilitating role through control of critical intermediary resources or services that are necessary to link users and content, to mediate between the different players in the information chain, to produce, transport and distribute content, etc.[190] While the former aspect is represented by those who are in the position to have an editorial control over the information to be published either

---

188 Laidlaw (n 179) 57. According to the Laidlaw's model, "Whether human rights responsibilities should be incurred and the extent to these responsibilities depends on the extent to which the gatekeeper controls the deliberation ad participation in the forms of meaning-making in democratic culture.". This model results in and merges up with the proposed 'corporate social responsibility' (CSR), meaning that businesses are responsible for human rights within their 'sphere of influence', a concept which is articulated in the UN's framework of CSR (Laidlaw (n 179) 47).

189 See Laidlaw (n 179) 259. The debate over this concept and its potential role against the ultimate findings is left to the Chapter 8, as the gatekeeping conception becomes more crucial and surfacing following the doctrinal analysis and the case studies.

190 Natali Helberger, Katharina Kleinen-von Königslöw and Rob van der Noll, 'Regulating the new information intermediaries as gatekeepers of information diversity' [2015] 17(6) Info 50, 52.

online or offline (traditional gatekeeping concept), the latter matches the more structural network gatekeepers like CAS providers i.e. cable or pay-TV platform owners, or the ISPs that control the means of access to the information. Remarkably, as the recent literature emphasizes,[191] gatekeeping activities are more visibly seen through the digital platforms which maintain control over 'access by third-party firms to its users' or 'access to content, products and/or services'.[192]

From a broader viewpoint, this gatekeeping notion which also surfaces in a recent EU consultation paper,[193] needs to be expanded to all across the IP layers and the networks, services, applications and content provided through them. In this regard, not only video streaming platforms, e.g. Netflix, Amazon Prime, YouTube, social media platforms, e.g. Facebook, Twitter, search engine/app store/browser providers, e.g. Google's

---

191 Peter Alexiadis and Alexandre de Streel, 'Designing an EU Intervention Standard for Digital Platforms' (EUI Working Paper RSCAS 2020/14) 5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544694> accessed 9 October 2020

192 According to this rather narrow definitional framework introduced by Alexiadis and De Streel, in the former scenario, the gatekeeper controls access by third-party firms to its users. For example, an online social network has, to some extent, control over access to its users by online advertisers, particularly for those consumers who spend most of their time on that social network. In the second scenario, the gatekeeper controls access to content, products and/or services. For example, a search engine controls the access of users to web content via its ranking algorithm, while a music streaming service controls access to its large catalogue of music titles through its personalised recommendations, etc. (Ibid, 5).

193 The Commission, on 2nd June 2020, published a consultation document by which to seek the stakeholders' views as to the regulation of digital platforms for their gatekeeping functionalities. Commission, emphasizing wide-ranging capabilities of such platforms, e.g. access to large amounts of data and leveraging this into new advantages/markets, bundling a broad range of platform and other digital services into a seamless, data-driven offer, put forth three policy options for ex ante regulation. These include, (i) revise the horizontal framework set in the Platform-to-Business Regulation (EU) 2019/1150; (ii) adopt a horizontal framework empowering regulators to collect information from large online platforms acting as gatekeepers; and (iii) adopt a new and flexible ex ante regulatory framework for large online platforms acting as gatekeepers (See European Commission, Digital Services Act package ex ante regulatory instrument for very large online platforms with significant network effects acting as gate-keepers in the European Union's internal market, Document Ares (2020) 2877647, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AAres%282020%292877647> accessed 9 October 2020). While there is not a draft published yet, it seems that first option along with some elements from other options seems to be forging ahead, given the recent news leaks (Dr2 consultants, 'The Digital Services Act – How does it affect businesses in the EU?' (14 September, 2020) <https://dr2consultants.eu/digital-services-act-how-does-it-affect-businesses-in-the-eu/> accessed 9 October 2020.

Chrome, Apple's iTunes, Microsoft's Edge, but also content distribution networks, e.g. Akamai, Cloudflare Polish, and connectivity providers, e.g. Virgin, BT, Three, need to be considered.

For the purpose of this study, 'gatekeeping' or 'network gatekeeping' is used to describe the digital gateways employed across the IP layers through which information flows and users' access to informational or infrastructural resources are controlled. Most remarkably, this study invokes and relies on this concept with a view to address all the underlying concerns on the basis of access and interoperability constraints. In so doing, this study not only highlights well-known problems of network effects, vendor lock-in, market foreclosure, etc. but also indicates that this term could be a component of a wider normative framework.[194]

While gatekeeping or network gatekeeping is not acknowledged as a technical term within the EU legislation or precedents,[195] the recent EU proposal could change the *status quo*, conferring this term a statutory meaning to approach a range of controlling powers in the ICT landscape. Marking a more distinctive path, this study invokes this term as one of the key concepts around which interoperability is revitalised along with a normative framework in the end.

194 See the section '8.4.2. Revitalising 'gatekeeping' and gatekeeping activities'.
195 See also Alexiadis and De Streel (n 191) 5.

3.2. Pertinent legal regimes and rules

3.2.1. Intellectual property rights (IPRs) and legislation

In the 1970s, the arrival of computer products for mass markets – notably personal computers and computer games – put paid to "first generation" notions that functioning elements and above all "computer programs",[196] could be adequately protected within the framework of IPRs.[197] While these legal mechanisms have remained vital, they have come to be underpinned, first by copyright in software and, to an increasing extent, also by patents on inventive techniques associated with programming.[198] This trend has become an overarching reality following the mass production of computer hardware and software and the accompanying pressure coming from the manufacturers.[199]

Accordingly, computer programs were regarded and protected as 'literary works'[200] under international copyright law, particularly within the context of the 1979

---

196 [A] computer program is a list of instructions or statements for directing the computer to perform a required data-processing task. There are various types of programming languages that can be written for a computer, but the computer can only execute programs which are represented internally in binary form (e.g. a series of 1s and 0s). Programs written in other languages must be translated to the binary representation before they can be executed by the computer. The binary code representation is also known as machine language. For example, a machine language instruction may add two numbers, move data from one memory location to another, or determine whether a number is equal to zero. A machine language instruction such as the bit (binary digit) sequence 01101011 might correspond to the instruction to 'add the contents of one register to another'. Very few programmers can readily understand machine language, and almost no program would currently be written directly in this form (John Abbott, 'Reverse Engineering of Software: Copyright and Interoperability' [2003] 14 Journal of Law and Information Science 7, 9).

197 William Cornish, David Llewelyn and Tanya Aplin, *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (8th edn, Sweet & Maxwell 2013) 818.

198 Ibid.

199 Ibid. See also Pamela Samuelson, 'The Past, Present and Future of Software Copyright Interoperability Rules in the European Union and United States' [2010] 34(3) European Intellectual Property Review, 229-236.

200 Any work not dramatic or musical and is written, spoken or sung, denotes 'literary works' in general. Either expressed in print or writing, such works are regarded as 'literary works' insofar as they involve "skill, labour and judgement" within the legal understanding (e.g. under the UK Copyright Designs and Patents Act 1988).

International Berne Convention for the Protection of Literary and Artistic Works.[201] This was also embraced by the World Trade Organization (WTO) Trade-Related Aspect of Intellectual Property Rights (TRIPS) Agreement[202] which entered into force as of 1st January 1995. The written program code, both object and source codes, is thus protected under copyright law by analogy with other literary works, such as the text of a novel or poem.[203] As interfaces denote the occurrence of transferring data or instructions repetitively between elements of a computer system,[204] they could normally be considered as part of software or computer programs, subject to the same copyright protection. However, this is still questionable given the EU legislation that favours interoperability and creates exceptional rights along the same lines. The Software Directive (2009/21/EC) represents the most significant means to ensure interoperability in association with the software related copyrights, at the EU level.

The Software Directive grants copyright protection to the "*expression* in any form of a computer program", whereas "ideas and principles which underlie any element of a computer program, including those which underlie its interface, are not protected".[205] Based on the legal doctrine known as the idea expression dichotomy,[206] the written program code, both source and object codes, could be categorised under the latter and considered as protected under EU copyright law. Along the same lines, APIs are

---

201 Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), <http://www.wipo.int/treaties/en/ip/berne/> accessed 9 October 2020.

202 Agreement on Trade-related Aspects of Intellectual Property Rights ('TRIPS Agreement') is a multilateral agreement, Annex 1C of the Marrakesh Agreement Establishing the WTO, setting out the minimum standards of legal protection and enforcement for a number of different forms of IPRs. See WTO, TRIPS, <https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm> accessed by 9 October 2020.

203 Simoneta Vezzoso, 'Copyright, Interfaces, and a Possible Atlantic Divide' [2012] 2 Jipitec 154 <https://www.jipitec.eu/issues/jipitec-3-2-2012/3444/vezzoso.pdf> accessed 9 October 2020.

204 See Weston (n 13) 234.

205 Software Directive, art 1(2).

206 The main rationale behind the idea/expression dichotomy is that it is socially desirable to allow for the free use of the fundamental building blocks, the "ideas" of knowledge production, within the area of copyright protection.

expected to be covered by this copyright regime as they represent the expressive elements of a computer program which are supposedly "original" within the meaning of the Software Directive.[207]

From this general standpoint, the so-called idea/expression dichotomy and the exclusion of functional/expressive elements from copyright protection would apply to the methods in APIs as well as the kernels of the computer programs. Yet software interoperability is underscored in the Software Directive, which grants an exception to the codes that are indispensable for the achievement of interoperability:

> The unauthorised reproduction, translation, adaptation or transformation of the form of the code in which a copy of a computer program has been made available constitutes an infringement of the exclusive rights of the author. Nevertheless, circumstances may exist when such a reproduction of the code and translation of its form are indispensable to obtain the necessary information to achieve the interoperability of an independently created program with other programs. It has therefore to be considered that, in these limited circumstances only, performance of the acts of reproduction and translation by or on behalf of a person having a right to use a copy of the program is legitimate and compatible with fair practice and must therefore be deemed not to require the authorisation of the rights holder.[208]

---

207 Software Directive, art 1(2). According to the Software Directive, "a computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection" (Software Directive, art 1(3)).

208 Software Directive, recital 15.

The given emphasis and the exceptional situation concerning interoperability is reflected in Article 6(1) of the Software Directive, titled 'Decompilation'. Article 6(1) limits the application of the so-called exceptional decompilation right to 'reverse engineering' with the aim of ensuring mutual functionality of non-interoperable computer programs. According to this provision, authorisation from the rights holder of a computer program is not required for *reproduction* or *translation* of the program in question, provided that these acts are "indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs".[209] It is acknowledged that the issue of 'functionality', which ensures the compatibility of computer programs, lies at the core of the Directive's rationale to set out the decompilation right.[210]

On the other hand, there is an ongoing debate over the so-called functional behaviours of a computer program that covers the APIs and whether such interfaces could be deemed as an exception, as ideas and/or principles underlying the computer program in question. This question is remarkably important as APIs would then be imitated or reproduced, if not copied, by third parties who could create derivative software on top of the existing products. On the other hand, the Court of Justice (CoJ)'s ruling in *SAS Institute Inc v World Programming Ltd (SAS v WPL)* affirmed that either the functionality of a computer program, or the programming language and the format of data files used in a computer program, do not constitute a form of expression and

209 Software Directive, art 6(1).

210 Hart describes the level of compatibility intended by the Software Directive as 'multi-vendor interoperability'. He however stresses that the Directive's wording does not refer to the full functioning of all the elements of the programs with which the independently created program is required to interoperate (Robert Hart, 'Interoperability Information and the Microsoft Decision' [2006] 7 European Intellectual Property Review 361, 362).

accordingly do not enjoy copyright protection under the Software Directive, yet the Court did not touch on the APIs within the same category.[211]

While the EU copyright regime is blurry in terms of ensuring a safe harbour for the APIs, patentability of software, including interfaces, is less controversial in view of the European patent regime. Patents are granted for "any inventions which are susceptible of industrial application, which are new and which involve an inventive step"[212] and software products could be covered under this via a broad interpretation. However, 'programs for computers' are in the list of the subject matter or activities which are explicitly excluded from patent protection under the European Patent Convention (EPC).[213] As this exclusion applies "only to the extent to which a European patent application or European patent relates to such subject-matter or activities *as such*",[214] computer programs that are claimed 'as such' would not be a patentable invention. Overall, the reading of "as such" made by the Board of Appeal of the European Patent Office (EPO) is in the sense that a patent cannot be granted if the software is a mere implementation of an invention with no technical teaching. However, there will be no bar to patent protection for those inventions that are implemented through computer programs, if that implementation represents the solution to a technical problem.[215] From this point of view, the application of software architecture to a specific technical invention, of a technical character, may be

---

211 See the section '3.1.3. Copyrightability of interfaces: Analysis through the lens of *Softwarová* and *SAS v WPL* cases'.

212 EPC, art 52(1).

213 In Article 52(2), the EPC excludes the following from patentability:
(a) discoveries, scientific theories and mathematical methods;
(b) aesthetic creations;
(c) schemes, rules and methods for performing mental acts, playing games or doing business, and *programs for computers*;
(d) presentations of information.

214 EPC, art 52(3).

215 Zingales (n 62) 9.

patentable as part of a bigger patentable concept, but the scope of protection is limited to this specific application.[216]

Given the fact that patents are application-specific, when access to the information contained in the interfaces does not imply the "making" or the "using" of the patented invention, there would be no patent infringement.[217] On the other hand, patent protection for a single software component could prevent the 'making' or 'using' of the whole of a complex program including the temporary uses required for decompilation or reverse engineering.[218] Given this fact, patentability of computer programs would have unpredictable effects in hindering interoperability. Moreover, within a computer program there often exists patented applications/inventions and copyrighted software elements. The more complex a program is, the more difficult it will be to access interfaces through reverse engineering.[219] This complexity is augmented by other IPRs such as trade secrets, *sui generis* databases, etc. which reside and operate collectively in the creation and implementation of the software.[220]

From this point of view, overuse of copyright, patents and other IPRs might have hazardous effects on market competition and innovation, resulting in the aggravated concerns surrounding lacking interoperability. While IPRs might be over-protectionist

---

216 Begoña G. Otero, 'Compelling disclosure of software interoperability information: A risk for innovation or a balanced solution?' in G. B. Dinwoodie (eds), *Intellectual Property and General Legal Principles: Is IP a Lex Specialis*? (Edward Elgar 2015) 82-83.

217 Ibid. Patent infringement might take place when a third party makes or uses a patented invention without receiving the permission from the patent proprietor. According to the TRIPS Agreement, given that a patent is an exclusive right, the patent proprietor has the right to prevent third parties who do not have the owner's consent from doing the following acts:
- making, using offering for sale, selling, or importing for these purposes the patented product, or
- where the subject-matter of the patent is a process, using offering for sale, selling or importing for these purposes at least the product obtained by the patented process. (TRIPS Agreement, art 28(1)). See EPO, 'Fundamentals of infringement' <https://e-courses.epo.org/wbts_int/litigation/FundamentalsOfInfringement.pdf> accessed 9 October 2020.

218 Weston (n 13) 241.

219 See Samuelson (n 4) 1961.

220 For detailed information about other types of IPRs and their relation to interoperability, see the section '4. Intellectual property rights: European IPR regime'

and have potentially negative outcomes along with the interoperability-based concerns, a suspicion is valid as to whether statutory rules respond well to such concerns. Generally, interface IPRs e.g. patents might be considered as posing a serious risk for competition and follow-on innovation; when they are held by established firms with market power, and/or when there are incentives for firms to enforce interface patents, or copyrights, trade secrets, etc. in a manner that provides the opportunity for leveraging a dominant firm's power in one market into that of an adjacent market, or last but not least, when exercise of such IPRs are essential to interoperability.[221] The following Chapter 4 is dedicated to a comprehensive analysis of interoperability related IPR tools and safeguards within the meaning of the EU law.

3.2.2. Competition law

Competition law is concerned with promoting consumer welfare by stimulating and balancing static efficiency i.e. service and price based competition and dynamic efficiency i.e. innovation and facilities based competition.[222] Competition law has a remedial concept regarding the monopolistic behaviours and surrounding hazards towards consumers by means of prohibition, prevention and punishment, where necessary. EU competition rules, having a central role for the functioning of the EU, are laid down in the Articles 101-109 of the TFEU. Article 101 prohibits anti-competitive agreements, decisions and concerted practices, such as joint ventures, cartels or tacit collusions that impede effective competition in the relevant markets. On the other hand, Article 102 prohibits abuse of dominant position, whether through exclusionary practices, such as predatory pricing, refusal to deal and exclusive dealing,

221 See Samuelson (n 4) 1945.
222 Van Rooijen (n 40) 99.

or exploitative conducts e.g. unfair prices and degrading service quality. While these aim at protecting competition and enhancing consumer welfare predominantly through ex post remedies, the EU merger regime envisages ex-ante measures and procedures to pre-empt likely anti-competitive effects that would arise from mergers and acquisitions.[223]

The primary purpose of Articles 101 and 102 of the TFEU on the one hand, and the 2004 Merger Regulation on the other, is to preserve the competitive constraints to which firms are subject.[224] Within the given context, national competition authorities and the European Commission at the EU level are equipped with a number of powers and tools aiming at supervising firms' exercise of proprietary control over their resources, whereby the negative effects of overzealous exercise of IPRs are also considered.[225] This prevailing role of the EU competition law could also be read through the TFEU provisions and foundational basis of the EU which relies on the freedom of persons, goods, services and capital.[226]

From this point of view, it is acknowledged exclusionary conducts driven by hindered interoperability would harm competitive forces or restraints residing in the relevant market. When interfaces are concealed by IPRs or TPMs, an overzealous exercise of

---

223 See Regulation (EC) 139/2004 on the control of concentrations between undertakings [2004] OJ L24/1 ('EU Merger Regulation' or 'EUMR') which allows the Commission to prohibit or require modifications of mergers that 'significantly impede effective competition' (SIEC) in cases whereby a dominant position is created or strengthened.

224 Pablo Ibáñez Colomo, 'EU Competition Law in the Regulated Network Industries' (2016) LSE Law, Society and Economy Working Papers 08/2016, 6 <http://dx.doi.org/10.2139/ssrn.2747785> accessed 9 October 2020.

225 See Van Rooijen (n 40) 99.

226 According to Article 3 of TFEU, 'the establishing of the competition rules necessary for the functioning of the internal market' is set out as one of the areas whereby the Union has exclusive competence. This also relates to and is strengthened by the major freedoms that underlie the EU as a supra-national organisation. Article 26(2) of the TFEU states that "The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties".

the rights granted to the parties e.g. dominant undertakings, might be at stake making the competition authorities or the Commission concerned. This is more relevant in a case where distortion of competition happens such as in vendor lock-in following misuse of market power and/or network effects, along with the likelihood of lessened consumer surplus. Clearly, although not an aim of EU competition law itself, achieving interoperability has thus far emerged as an important means to break off lock-ins and to eliminate anti-competitive effects under the TFEU.

Under this light, lack of interoperability between competing platforms, networks and services could become a source of concern particularly because of the potential network effects and the risk of exclusion in the relevant market(s). This situation might be aggravated by making use of IPRs over APIs which often function as a gatekeeper for the upstream ICT markets. If secondary (downstream) markets are locked into a proprietary platform particularly by means of using IPR-protected interfaces, the ultimate goals of IPR rules such as stimulation of follow-on innovation or original products becomes compromised, leaving a bigger room for competition law remedies.

Following this spirit, Article 102 of the TFEU, which prohibits abuse of dominant position, has effectively been invoked against 'exclusionary' abuses e.g. involving hindered interoperability information. While *Microsoft* is known as the leading case regarding 'refusal to supply interoperability information', the precedents involving refusal to license practices trace back to the cases, *Magill*[227] and *IMS Health*,[228] where

[227] Joined Cases C-241/91 P and C-242/91 P, *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP)* v. *Commission* [1995] ECR I-743, [1995] 4 CMLR 718 ('*Magill* judgement').

[228] Case C-418/01 *IMS Health GmbH & Co. OHG v NDC Health GmbH & Co KG,* Judgment of 29 April 2004, [2004] 4 CMLR 1543 ('*IMS Health* judgement').

we see distinct criteria based on deterrence of new products, foreclosure of secondary markets, etc.

The referred EU antitrust cases represent the cornerstone decisions setting out the *"exceptional circumstances"* that define abusive 'refusal to license' acts within the meaning of the Article 102 of the TFEU. According to the case law, refusal to license a dominant product that is protected by IPRs may amount to a finding of an abusive behaviour, providing that the 'exceptional circumstances' exist in the particular case. To reach such a conclusion, it needs to be established whether the following cumulative conditions have been met:[229]

1. the refusal relates to a product or service that is *objectively necessary to be able to compete effectively* on a downstream market;
2. the refusal is *likely to lead to the elimination of effective competition* on the downstream market; and
3. the refusal is *likely to lead to consumer harm*.

As hindered interoperability is meant to be the result of 'refusal to licence or supply' interfaces, the tripartite test stated above is of high importance in dealing with the abuses that involve interoperability information. Having said that, tripartite 'exceptional circumstances' test needs to be emphasized in finding out whether a dominant undertaking's 'refusal to licence or supply interoperability information' amounts to a violation of Article 102 of the TFEU.

[229] See Communication from the Commission-Guidance on the Commission's enforcement priorities in applying Article 82 of the Commission Treaty to abusive exclusionary conduct by dominant undertakings, 2009, OJ C 45/7 ('Commission Guidance') para 81.

While the concerns shift from abusive market foreclosure to more sophisticated merger-specific concerns, the applicable test based on 'significant impediment to effective competition' (SIEC) and the underlying harm theories, would have a more pro-active nature focused on likely negative impacts on the market dynamics e.g. on price and innovation. The resorted remedies also differ in merger cases, being not limited to behavioural remedies but also consisting in structural ones. For instance, divestiture of the IPR portfolio underlying the videoconference communication services surfaced in the *Cisco/Tandberg* case, whereas more typical behavioural remedies were invoked in the *Intel/McAfee*, *Microsoft/LinkedIn* cases. While both structural and behavioural remedies aimed to enhance interoperability in the referred cases, one could not mention an ascertained and refined test with regards to the interoperability-based merger cases,[230] as opposed to the 'exceptional circumstances' test applied under Article 102. The same discrepancy could be upheld for the cases of Article 101, which aims to assess the agreements, decisions and concerted practices that would have anti-competitive consequences, either by means of their object or effect.[231]

Overall, albeit with some common elements i.e. market definition, various contexts of EU competition law e.g. Article 101, 102, have distinctive elements that need to be underlined. A detailed and comprehensive analysis is made in Chapter 5, particularly dealing with the refusal to supply and license cases with an emphasis to lack of interoperability. In this regard, a particular attention is paid to draw out the pitfalls as well as the proven benefits of the criteria, and tests e.g. exceptional circumstances, applied under Article 102 of the TFEU. In addition to this, Article 101 and merger

230 See the section '5.4. Merger Regulation'.
231 See the section '5.2. Article 101 of the TFEU'.

cases are also incorporated within the overall analysis, uncovering the reach and limitations of EU competition law.

3.2.3. Sector-specific rules: Electronic communications law and regulations

"Electronic communications networks"[232] constitute the backdrop on which all kinds of ICT platforms, services and applications are run. In this scope are included all kinds of wired and wireless networks, like cable, mobile, etc., that enable end-to-end connectivity i.e. any-to-any communication, through transmission of voice, data and video. Through these networks are offered the "electronic communications services", which were originally defined as "a service normally provided for remuneration which consists wholly or mainly in the *conveyance of signals on electronic communications networks*, including telecommunications services and transmission services in networks used for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and service".[233]

As can be seen, the core part of the 'electronic communications services' comes from the "conveyance of signals on electronic communications networks", marking a distinction from the conveyance of the content via these networks/services. From this point of view, electronic communications law, or more specifically speaking the EU regulatory framework (ECRF), is built upon the idea of regulation of all transmission networks and services in a technology-neural and harmonised manner. While a significant overhaul of

232 For more detailed information regarding 'electronic communications networks' see the section '6.2.2.2. Introduction of new ECS categories'.

233 Framework Directive, art. 2(c). The core part of this definition has been kept in the EECC, being rephrased as "service normally provided for remuneration via electronic communications networks" (EECC Directive, art 2(4)), with an enlarged scope and categories. See the section '6.2.2.2. Introduction of new ECS categories'.

the ECRF has taken place recently with the EECC, this new consolidated Directive does not practically or radically change this main logic pursued so far.[234]

The original ECRF, or the '2002 regulatory framework', has entered into force incorporating a number of directives, regulations, Commission recommendations and decisions, to be applicable in the field of electronic communications.[235] Such pieces of hard and soft law mean a toolbox delivering a number of regulatory tools and measures to cope with the structural, and to a lesser degree, behavioural market failures encountered in electronic communications markets. While the mainstream idea is to pre-empt the market failures, this is extended by a more consumer-centric, protectionist perspective, encompassing the issues of universal rights and data privacy.[236]

From the competition policy point of view embedded into the ECRF, regulatory authorities (NRAs) define ex-ante markets in broader terms than their competition law counterparts,[237] although they often use the ex post competition law terms and instruments e.g. market analysis and dominance. Their market analyses give some signals as to the prospective market failures, signifying a forward-looking approach based on the existing market data. At the end of this process, a number of remedies are supposed to be imposed on the dominant players or technically speaking operators

---

234 For more detailed information regarding the 'EECC' see the section '6.2.2.1. OTT Impact and a new carve-out under the EECC'.

235 For the details of the EU regulatory framework (ECRF) see the section '6. Sector-specific regulations: Electronic communications law'.

236 Notwithstanding, interoperability is a matter of competition for the ICT markets, including those of electronic communications, and from this viewpoint this study elaborates the ECRF, focusing on the dimensions of competition and innovation at stake.

237 Peter Alexiadis, 'Balancing the Application of ex post and ex ante Disciplines under Community Law in Electronic Communications Markets: Square Pegs in Round Holes?' (2012) 139 <https://www.gibsondunn.com/wp-content/uploads/documents/publications/Alexiadis-BalancingtheApplicationofExPostandExAnteDisciplines.pdf> accessed 9 October 2020.

which enjoy 'significant market power' (SMP) to ensure an effectively competitive market functioning.

While interoperability might appear as an issue of competition policy echoed by the remedies directed towards the dominant/SMP operators,[238] it could also become a matter of standardisation policy aiming at promotion of common specifications and standards. For instance, Article 39 of the EECC encourages the use of the standards and/or specifications adopted by the European SSOs and entitles the European Commission to mandate a standard *to the extent strictly necessary to ensure such interoperability and to improve freedom of choice for users.*[239]

Regardless of standards, some interoperability-centric obligations are remarkable within the context of the ECRF, particularly in two specific areas. Firstly, Article 62(1) of the EECC Directive imposes an interoperability obligation on CAS (set-top box) providers to ensure that technical services e.g. conditional access that enable *digitally-transmitted services to be received by viewers,* are given to all access seekers (broadcasters) in a non-discriminatory way. Secondly, the interconnection obligation, which enables end-to-end connectivity as well as interoperable networks and services, is given special weight under various provisions e.g. Articles 3-5 of the Access Directive. While these are worth being elaborated, as reflected in Chapter 6,[240] hereby suffice it to say that interoperability is one of the central tenets in the ECRF. Therefore, interoperability could be considered as one of the aims kept on by the ECRF from the

238 EECC Directive, art 69 to 74 and art 76 to 81.

239 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36 ('European Electronic Communications Code' or 'EECC') art 39(3).

240 See the section '6. Sector-specific regulations: Electronic communications law'.

beginning, which marks a distinction against other EU legal bodies e.g. IPR and competition law rules.

Against this background, it needs to be noted down that the existing ex-ante instruments placed under the ECRF for the achievement of interoperability,[241] add another important dimension to the ICT interoperability. This dimension is of a central importance because of the very nature of the ECRF and its role for the ICT networks/services. Chapter 6 offers a comprehensive analysis and enhanced debate regarding this role played by the ECRF to be followed by further regulatory discussions in the subsequent chapters.

3.2.4. Data protection rules: Right to data portability

EU data protection framework has undergone a big revision through the General Data Protection Regulation (GDPR) which entered into force on 25th May 2018. This Regulation introduced significant improvements concerning the rights of the individual users, namely 'data subjects', and the obligations of the entities that have the role of 'data controller' or 'data processor'.[242] The intention appears as not only protecting personal data[243] but also boosting the data-driven economy, particularly to

241 Such instruments were even enhanced in number and type within the context of the Commission's ECC Proposal published in September 2016. For the details see the section '6.2.2. Introduction of new ECS categories and reach of interoperability problems'.

242 See Articles 12-31 of the GDPR (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 [2016] OJ L 119/1 ('General Data Protection Regulation' or 'GDPR'), art 4(1)).

243 Under the GDPR 'personal data' is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (GDPR, art 4(1)).

allow a modernised data protection regime for all the parties.[244] Given this fact, one of the initiatives under the Digital Single Market (DSM) Strategy for Europe was the enactment of the GDPR, through which a wide-range of new statutory rights are created, including the 'right to data portability' (RtDP). This right, regulated under Article 20 of the GDPR, has potential effects to reduce the switching costs. Not only this fact, but also the close link between the RtDP and interoperability makes this new-born right important for the competitive supply of the data-driven ICT services.

RtDP has two key elements: (1) the right of the data subject to obtain a copy of personal data from the data controller; and (2) the right to transfer that data from one data controller to another.[245] Although aiming to enhance the data subjects' controlling power vis-à-vis data controllers, the GDPR delimits the scope of the RtDP by adding that the controller would only transfer the data to another controller, where such a transfer is "technically feasible".[246] Another limitation relating to the RtDP is the restraint on the 'personal data'. More explicitly, RtDP could be applied "where the data subject has provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract".[247]

Thus, the RtDP has a limited reach as non-personal data e.g. data created for the purposes of management, analytics and/or advertising, is excluded from the scope of the Regulation. Last but not least, while the GDPR encourages "to develop

244 See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions COM (2015) 192 final.

245 Aysem Diker Vanberg, 'The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?' [2018] 21(7) Journal of Internet Law 11, 11.

246 Aysem Diker Vanberg and Mehmet Bilal Unver, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?' [2017] 8 European Journal of Law and Technology 1, 2.

247 The GDPR, recital 68 and art 20 1(a).

interoperable formats that enable data portability",[248] no obligation exists to secure 'interoperability' for the transfers of data across different platforms under the GDPR. Even with standardised data formats, 'interoperability' could not be fully achieved via 'data portability', as the former entails a higher requirement of technical, syntactic and semantic compatibility, going beyond the latter, namely the RtDP.[249]

Granting enhanced control to the data subjects, the GDPR addresses the issue of data portability from the perspective of the end-user. Given this fact, the RtDP does not fully resolve vendor lock-in particularly in ICT markets where data hosting, processing and analytics is not just related to personal data.[250] In fact, all the IoT-embedded information is not covered by the definition of 'personal data', and the non-personal data flowing through the IoT systems could have a strategic management purpose and cause a serious risk for lock-in unless the data at hand is portable across different platforms.[251]

Vendor or technological lock-in would particularly take place in the case of two affiliated markets which affect each other.[252] For example, some IoT products may operate in a two-markets setting where suppliers use free or low cost pricing to build a network or installed base of IoT products – perhaps at significant cost to the supplier – with the intention of monetizing the network through data analytics that are directed to customers on another side of the market.[253] In such cases, hindering data portability by restricting data transfers via technical tools such as restricted APIs, imposed on

248 The GDPR, recital 68.
249 See also Unver (n 30) 106, reading; "it is apparent that 'interoperability' envisioned here is limited to data processing systems of the software platforms".
250 See Unver (n 30) 105-107.
251 See also infra note 254.
252 Gregory G. Wrobel, 'Connecting Antitrust Standards to the Internet of Things', [2014] 29(1) Antitrust ABA 62, 63.
253 Ibid, 66.

collaborators and advertisers, could result in aggravation of the related concerns. Mandated data portability under the GDPR serves pre-emption of such potential problems at the outset. Nevertheless, the portability constraints relating to the non-personal data, when considered and coupled with the broader interoperability concerns, would need to be handled from a broader competition and/or regulatory perspective.[254]

4. Intellectual property rights: European IPR regime

Intellectual property relates to information or knowledge which can be incorporated into tangible objects in an unlimited number of copies at different locations anywhere in the world.[255] IPRs are rights "that exclude non-owners for a specific duration and over a specified breadth from commercially exploiting the IPR without the owner's permission".[256] Intellectual property protects applications of ideas and information that are of commercial value.[257] There exist a variety of IPRs, stretching across a wide range of generis and sui generis rights, including copyrights, patents, trade secrets, databases, etc. Patents give a temporary protection to technological inventions and design rights to the appearance of mass-produced goods; copyright gives longer-

254 While the lack of data portability has not been considered as an antitrust problem to be remedied so far, data portability would constitute the subject-matter of antitrust investigations, as happened in the Google case, where one of the scrutinized issues was 'whether Google has restricted the portability of online advertising data to competing online advertising platforms' (European Commission, 'Antitrust: Commission Probes Allegations of Antitrust Violations by Google' (Press Release, IP/10/1624, 30 November 2010), <http://europa.eu/rapid/press-release_IP-10-1624_en.htm> accessed 9 October 2020). Notwithstanding, a number of global players, namely Google, Microsoft, Facebook and Twitter have been involved in an open source project to facilitate portability of non-personal (See infra note 776).

255 United Nations Conference on Trade and Development (UNCTAD) (Trade and Development Board Commission on Investment, Technology and Related Financial Issues), *Competition Policy and the Exercise of Intellectual Property Rights* (Report by the UNCTAD Secretariat, 2008), 3, <http://unctad.org/en/Docs/c2clpd68_en.pdf> accessed 9 October 2020.

256 Ibid, 4.

257 Cornish, Llewelyn and Aplin (n 197) 6.

lasting rights in, for instance, literary, artistic and musical creations,[258] trade secrets encompass manufacturing or industrial secrets and commercial secrets against unauthorized use of such information.[259] Databases, representing a sui generis right, are compared to copyrights, yet have distinctive features based on recognition of the investment done for compiling data in the form of databases.

The benefits attributable to IPRs, are not limited to, but include encouragement of (1) innovation by increasing the returns from research and development, (2) dissemination and (3) the further development of those inventions which have little value or are not commercially viable until improvements are made.[260] One characteristic shared by all types of IPR is that they are essentially negative: they are rights to stop others doing certain things – rights, in other words, to stop pirates, counterfeiters, imitators and even in some cases third parties who have independently reached the same ideas, from exploiting them without the licence of the rights holder.[261] Some aspects of intellectual property confer positive entitlements, such as the right to be granted a patent or register a trade mark upon fulfilling the requisite conditions, but these are essentially ancillary.[262]

With all these aspects, IPRs create a private sphere for the rights holders with an ultimate view to enhance dissemination of knowledge and innovation, along with significant

---

258 Cornish, Llewelyn and Aplin (n 197) 3. While there is a variety of IPRs, including industrial designs and trademarks, for the purpose of this study, the analysis has been dedicated to copyrights, patents, trade secrets and databases.

259 World Intellectual Property Organisation (WIPO), 'What is a Trade Secret?' <https://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm> accessed 9 October 2020.

260 Ray Finkelstein, 'Legal protection of business research and development: can it harm competition?' in M Pittard, A L Monotti and J Duns (eds) *Business, Innovation and the Law: Perspectives from Intellectual Property, Labour, Competition and Corporate Law* (Edward Elgar 2013) 252-253.

261 Cornish, Llewelyn and Aplin (n 197) 6.

262 Cornish, Llewelyn and Aplin (n 197) 7.

effects over the 'global information infrastructure'.[263] Having said that, copyright law is supposed to give us a self-regulating cultural policy in which the right to exclude others from one's original expression fuels a vibrant public sphere indirectly driven by popular demand.[264] By similar token, patent law is supposed to give us a self-regulating innovation policy in which the right to exclude others from novel and useful inventions creates a cybernetic and responsive innovation marketplace.[265]

However, the fact that IPRs are prescribed in a manner offering an exclusive usage ironically poses a potential risk over social and cultural production as well as new entries to and competition in the relevant market(s).[266] This is more compelling when the gateway type interfaces are not open to the third parties that would seek to develop derivative programs. To emphasize, not only original content or creations, protected by copyrights, patents, etc. and hosted by the ICT platforms, but also APIs that illustrate software-enabled gates for third party access to such platforms, are usually subject to the IPRs. At the centre of this debate lies the notion of interoperability, and its treatment under distinct IPR regimes. Below are analysed the main types of IPRs

---

263 Robin Mansell and W. Edward Steinmueller, 'Intellectual property rights: the development of information infrastructures for the information society' (A study carried out for the STOA programme of the European Parliament, Final Report, 1995) 1-2 <http://eprints.lse.ac.uk/24969/> accessed 9 October 2020.

264 Boyle (n 174) 7. It is rightfully established by the scholars that "[C]opyright law, (…) mediates two conflicting public interests: the public interest in maximizing the production of information, and the public interest in providing maximum access to information". (Niva Elkin-Koren, 'Public/Private and Copyright Reform in Cyberspace' (1996) 2(2) Journal of Computer-Mediated Communication, referring to Mark Rose, Authors and Owners (Harvard University Press 1992) 140 <https://doi.org/10.1111/j.1083-6101.1996.tb00059.x> accessed 9 October 2020).

265 Boyle (n 174) 7.

266 Notably, IPRs themselves would qualify as a barrier to entry under certain circumstances. This is argued to be so when the IPRs raise the costs of potential infringers per se (I. Eagles and L. Longdin, *Refusals to License Intellectual Property: Testing the Limits of Law and Economics* (Hart Publishing 2011) 99). According to Eagles and Longdin, this is most likely to occur when the right in question is used in such a way as to:

a) inhibit the creation of new markets by limiting derivative or developmental use of protected products or processes;
b) facilitate market segmentation by erecting geographic obstacles to product movement;
c) permit rights holders to use the power conferred by the right to deter entry into markets not covered by the right, or requiring would-be entrants to enter all markets simultaneously or not at all (Ibid, 99-100).

under the EU legal framework, with an emphasis paid to copyrights, patents and trademarks, from the viewpoint of interoperability.

4.1. Copyright

4.1.1. General pillars of EU Copyright Law and its applicability to ICTs

Copyright is a long-inherited and internationally acknowledged legacy right for protecting 'original' creations. While the economic rationale for copyright law is to give an incentive to produce creative work i.e. literary and artistic works[267] and avoid 'underproduction', the main rationale behind copyright and the conferred exclusive rights is to raise the supply of works closer to a socially desirable level.[268] The Berne Convention[269] represents the very first and widely ratified international treaty setting out the rights of the authors in their "literary and artistic works". Comprising a non-exhaustive list of examples regarding literary and artistic works, and the rights of the copyright holders i.e. translation, reproduction, public performance, communication to the public, along with the applicable exceptions, the Berne Convention could be regarded as a baseline for the emergence of many national and regional copyright regimes. Based on similar pillars i.e. minimum rights, the EU copyright framework consists of a set of eleven directives and two regulations, which all together constitute copyright *acquis*.[270]

---

267 Such kinds of works as progressively extended and categorised so as to cover dramatic and artistic works set the ground for delineated areas of protection; yet each area of copyright protection requires standard criteria, e.g. originality. Behind this lies the root requirement that sufficient "skill, judgement and labour", or "selection, judgement and experience", or "labour, skill and capital", be expended by the author in creating the work (Cornish, Llewelyn and Aplin (n 197) 435).

268 Weston (n 13) 197.

269 Berne Convention for the protection of Literary and Artistic Works, (as amended on September 28, 1979) (Berne Convention).

270 See the European Commission, 'Digital Single Market: The EU copyright legislation' (28 August 2015) <https://ec.europa.eu/digital-single-market/en/eu-copyright-legislation> accessed 9 October 2020.

Within the context of EU *acquis*, the InfoSoc Directive[271] plays a cornerstone role as it establishes the key rights and limitations with regard to the subject matter of the copyrights, to be adopted across the EU. The Directive harmonizes the basic economic rights (rights of reproduction, communication to the public, and distribution) in a broad and arguably 'Internet-proof' manner,[272] and introduces special protection for DRM systems.[273] The InfoSoc Directive features a horizontal harmonization instrument for copyright protection, not only in relation to the information society but also in general.[274] Based on Article 114 of the TFEU (ex Article 95 TEC) under EU law,[275] the InfoSoc Directive also serves to fulfil the international obligations of the member states arising out of the World Intellectual Property Organization (WIPO) Treaties i.e. the Berne Convention as well as the WTO Agreements i.e. TRIPS. When considered with other rights and directives i.e. the Software Directive, it is fair to say that the EU legislator is consistently focused on increasing the scope and intensity of protection, often further than the minimum standards of the Berne Convention and Rome Convention.[276]

Besides the main rights stated above, TPMs also find a very first place for protection under the InfoSoc Directive. According to Article 6(1), Member States should provide "adequate legal protection against the circumvention of any effective, technological

---

271 See supra note 70.

272 However, the recitals 28 and 29 compromise this argument as the former reads: "Copyright protection under this Directive includes the exclusive right to control distribution of the work incorporated in a tangible article". Whereas the latter reads: "The question of exhaustion does not arise in the case of services and on-line services in particular".

273 Mireille Van Eechoud, P. Bernt Hugenholtz, Stef van Gompel, Lucie Guibault and Natali Helberger, *Harmonizing European Copyright Law: The Challenges of Better Lawmaking* (Kluwer Law International 2009) 9.

274 Bernd Justin Jütte, Reconstructing European Copyright Law for the Digital Single Market: Between Old Paradigm and Digital Challenges (Hart Publishing 2017) 112-113. Article 2 of the InfoSoc Directive illustrates this generic scope. Indeed, the reproduction right enshrined thereunder covers "direct or indirect, temporary or permanent reproduction[s] by any means and in any form, in whole or in part".

275 Article 114 of the TFEU grants powers to harmonize the laws of the Member States to the extent required for the functioning of the internal market (See Van Eechoud et al (n 273) 13).

276 Jütte (n 274) 116-117.

measures" and other acts, such as the "manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services" in relation to TPMs.[277] Article 7 obliges Member States to provide for adequate legal protection against acts in relation to the removal of electronic rights-management information for the purpose of inducing, enabling, facilitating or concealing infringements of copyrights or related rights.[278] Finally, Member States must provide for effective sanctions and remedies for copyright and related rights infringements.[279]

While the scope of the InfoSoc Directive is related to information society issues covering a wide-ranging area, it should be noted that "computer programs"[280] are specifically regulated under the Software Directive. Although there is no anti-circumvention regime for the computer programs, expression of them is protected, being regarded as "literary works" in line with the international copyright legislation and paradigms.[281] It has been held that the "expression" includes the source and object codes underlying a computer program, but not its functionality, programming language, individual or complex commands, graphic user interface or data file formats.[282] Therefore, generated codes by the authors, i.e. software developers, are considered as 'literary work' within the meaning of European Copyright Law, as well as under the criteria acknowledged globally and in many developed and developing countries. For instance, under the 1998 UK Copyright, Designs and Patents Act (CDPA), "literary work" which in general is any work that is dramatic or musical and

277 Jütte (n 274) 113.
278 Jütte (n 274) 113.
279 Jütte (n 274) 113.
280 For description of computer programs see supra note 196.
281 TRIPS Agreement, art 10; WIPO Copyright Treaty, art 4.
282 Cornish, Llewelyn and Aplin (n 197) 821. See also the section '3.1.3. Copyrightability of interfaces: Analysis through the lens of *Softwarová* and *SAS v WPL* cases'.

which is written, spoken or sung, now explicitly includes a computer program and separately, preparatory design material for a program.[283]

From the EU perspective, copyright protection is essentially based on the rights enshrined under the InfoSoc Directive and the Software Directive. While the former provides for a very broad definition of IPRs (copyrights and related rights), coupled with the effective endorsement of TPMs,[284] the latter establishes a special treatment for the computer programs, which have a key role for the ICTs. Further to these, a new Directive, called the 'Directive on Copyright in the Digital Single Market',[285] has come into force on 7th June 2019, incorporating new rules regarding text and data mining, collective rights management practices, protection of press publications, treatment of user-generated content, etc.[286] The incorporation of these new copyright issues primarily reflects the need to align copyright *acquis* with the realities of the internet era, recalling the first legislative reactions to the advent of public internet.[287]

The trend of enhanced controls through increased TPMs, IPRs and new statutory rights e.g. under DMCA, CDPA, InfoSoc Directive, EU Database Directive is an important factor to be taken into account concerning the development of information and innovation infrastructures, given the interlinks between the proprietary systems and network effects and the information flows. Information channels and platforms would

283 The program must be recorded in writing or otherwise; but this is defined to include writing code, not necessarily by hand, and "regardless of the method by which, or medium in or on which, it is recorded" (Cornish, Llewelyn and Aplin (n 197) 435).

284 Andrea Renda, Felice Simonelli, Giuseppe Mazziotti, Alberto Bolognini and Giacomo Luchetta, *The Implementation, Application and Effects of the EU Directive on Copyright in the Information Society* (CEPS Special Report, No. 120, November 2015), 125.

285 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 [2019] OJ L 130 ('Directive on Copyright in the Digital Single Market').

286 Regarding the details of the Directive on Copyright in the Digital Single Market, see CREATE, 'EU Copyright Reform' <https://www.create.ac.uk/policy-responses/eu-copyright-reform/> accessed 9 October 2020.

287 See supra note 174.

need to be compared to the economic goods and services in terms of the role they play and the impact they pose. In the face of the 'networked information economy' as elaborated by Benkler,[288] this particular need surfaces and echoes in access and interoperability being blocked off for the "enclosure" of IPR-protected content.[289]

In this enclosed world with IPRs and TPMs, a massive amount of internet content and information is excluded from the public domain,[290] resulting in significant consequences exceeding the traditional consumer harm or losses and reaching out to lessened cultural production and participatory democracy. Within this broader debate, interoperability is of a key role connecting the networks, services and their users, and potentially diminishing the gatekeeping roles and functionalities that are often shielded by IPRs and TPMs. In this context, copyrights have an important stake as they are spontaneously born with the creation of the subject-matter and provide the rights holders with a legal protection against digital copying particularly on the internet.

Technically speaking, the Directive on Copyright in the Digital Single Market maintains the legacy copyright principles and rules under the InfoSoc Directive and the Software Directive, including those related to interoperability. That is to say, interoperability regime of the EU copyright *acquis* has remained the same throughout the years, even after the recent changes in the EU law. Having said that, examined

---

288 See supra note 161. Hereby it is remarkable to recognise that IPRs have a key role in this transition as they are "supposed to create a feedback mechanism that dictates the contours of information and innovation production" and from a broader perspective it could be said that they are "designed to shape out information marketplace" (Boyle (n 174) 7).

289 The term of 'enclosure' is used by Boyle in his exposition concerning the IPRs and public domain in which expansion of the former at the expense of the latter is highlighted with the phrase, 'second enclosure movement'. According to his analogy, this follows the first enclosure movement around feudal systems within which was existing concentration of economic in exchange for large-scale investment and management (Boyle (n 174) 42-45).

290 Boyle (n 174) 46; Lessig (n 175) 186.

below are the key aspects of the European copyright system concerning 'interoperability' with a focus on the Software Directive.

4.1.2. Reverse engineering and achievement of interoperability under EU copyright law

Within the EU legal system, a well-known idea/expression dichotomy[291] could be said to have been directly translated into the copyright protection of 'computer programs', along with some exclusive rights attributed to the subject matter. The so-called copyrightable subject matter, is referred to as "the expression in any form of a computer program", whereas "ideas and principles which underlie any element of a computer program, including those which underlie its interfaces" are excluded from copyright protection.[292] While the existence of an "author's own intellectual creation" is considered to meet the 'originality' threshold for copyright protection,[293] the rights holders are given a number of exclusive rights[294] that are subject to certain exceptions regulated under Articles 5 and 6 of the Software Directive.

Article 5(3) of the Directive allows any person to "to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program" without the authorisation of the rights holder. This practice,

---

291 Separate treatment between expressive parts of computer programs and the underlying ideas and principles is usually simplified as the 'idea/expression' dichotomy.

292 Software Directive, art 5(2).

293 Software Directive, art 1(3), reading; "A computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection".

294 Such rights cover "the right to … (a) … reproduction of a computer program … (b) the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, … (c) any form of distribution to the public, including the rental, of the original computer program or of copies thereof" (Software Directive, art 4).

called "black box analysis",[295] helps finding interoperable solutions across the mainstream platforms through observation and testing processes realised by the competing firms. This could be construed as a point of divergence from the established copyright paradigm and rules surrounding the idea/expression dichotomy. Taking a step further, Article 6 of the Software Directive establishes an exception directly aiming at interoperability. While Article 5(3) allows reverse engineering for a broader set of objectives mentioned above, Article 6 specifically addresses the issue of interoperability between computer programs.

Article 6(1) of the Software Directive sets out the "decompilation" right which is often called "white box analysis", as it allows for underlying source code to be analysed so as to find out the functionality of the program, namely how it works internally. Broadly echoed with the term 'reverse engineering', the so-called decompilation right is confined to the aim of 'mutual functionality' being achieved between computer programs.[296] According to Article 6(1), authorisation from the rights holder of a computer program is not required for *reproduction* or *translation* of the programme in question, provided that these acts are "indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs".[297] If the information necessary to achieve interoperability is readily available, the decompilation right would no longer be applied. Moreover, even if the given requisites are fulfilled, decompiling the program could not be done "for the development,

---

295 This is considered as a type of 'reverse engineering' along with other acts, i.e. disassembly and decompilation, distinguished by certain technical and functional aspects. For detailed analysis of reverse engineering including typical examples see Abbot (n 196) 11-14.

296 It is acknowledged under the Software Directive that "The function of a computer program is to communicate and work together with other components of a computer system and with users" (Software Directive, recital 10).

297 The Directive restricts the application of the decompilation right to "the parts of the original program which are necessary to achieve interoperability" (Software Directive, art 6(1/c).

production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright".[298]

The Software Directive, through the exceptions under Articles 5(3) and 6, purports to balance the rights between the copyright holders and licensees (access seekers) who would intend to have a back-up copy to come up with new ideas and/or create compatible programs. In this vein, when black box analysis is insufficient to achieve interoperability, reverse engineering is permitted if, in order to achieve interoperability of an independently created computer program with other programs, it is necessary to reproduce the code and translate its form.[299]

Hereby, the goal of rewarding original creations of computer programs is weighed up against the creation of derivative programs by third party software developers that rely on interoperability information i.e. interface specifications. Thereby, the trade-off between the socially desirable goals is embodied through the exceptional reverse engineering rights, with the view to encourage computer programs that are interoperable with the existing ones. This allowance also relates to the fact that interoperability information is usually distributed to the public in object code and could not be learnt without disassembly, in other words, decompilation. In other words, it is envisaged that the opportunity cost for creating interoperable computer programs is reduced to a certain extent as to allow follow-on innovation and compatible computer programs.

Conversely, the balanced approach based on a trade-off is seen in the Directive's prohibiting the information obtained through decompilation "to be used for the

298 Software Directive, art 6(2/b).
299 Weston (n 13) 39.

development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright" (Article 6 (2/c)). Given this fact, it could be stated that the effect of the Software Directive is not just to protect certain configuration of a program, but also the rights of the holder in reproductions, translations, transformations, changes, improvements etc. that in themselves constitute original works.[300]

4.1.3. Copyrightability of interfaces: Analysis through the lens of *Softwarová* and *SAS v WPL* cases

Whereas APIs directly serve interoperability being achieved between computer programs, it is worth questioning to what extent usage and dissemination of the interfaces is warranted under the EU copyright regime, namely under the Software Directive. It should be reiterated that it is already legitimate to achieve interoperability between computer programs by means of reverse engineering. It is thus clear that the Directive permits those who reverse engineer the object code to reach out for the underlying human-readable source code. However, a crucial question remains to be answered: are the interfaces identified through either black or white box analysis, protected the same as the copyright-protected subject matter, i.e. the internal programming or kernels of the computer program, under the Software Directive?

The Software Directive, compromising between different aims and concerns, implicates a mid-way between the copyright holders and access seekers that want to develop compatible programs. While the latter firms are attempting to access the source code through black or white box analysis, they would reach out to the interfaces that underlie

[300] Weston (n 13) 204, referring to Begoña González Otero, 'Compelling to Disclose Software Interoperable Information' [2013] 16(1-2) The Journal of World Intellectual Property 5.

the computer programs they observe and/or analyse. Regardless of the 'originality', should they use an insubstantial part of the interfaces to create interoperable software, this would normally be accepted as concurring with the scope and purpose of the Software Directive. Thus, when the very aim of the Directive is taken into account, interfaces would need to be conferred an equivalent meaning and protection as the internal codes or kernels of software under the copyright regime of the Software Directive.[301]

Having said that, it should also be born in mind that interfaces comprise not only the code that implements them but also the ideas, rules or principles in the specification of the interface.[302] Although the source code and machine code of interfaces may not *per se* be outside the protection of copyright, there are certain aspects, such as specifications and protocols (the aspects relevant to standards) which are not expressions but the underlying ideas and principles.[303] Whereas interface specifications, which can be regarded as the rules and methods underlying an interface and governing the program's behaviour, could be said to fall outside the scope of the copyright protection, the "implementation" of an interface into a program's code will arguably constitute a protectable expression as long as it meets the originality requirement.[304] As could be inferred here, interfaces posit a shakeable ground for the purpose of copyrightability to which the EU precedents do not have a clear-cut response.

---

301 On the other hand, this could be contested with the argument that the pro-interoperability approach of the Directive is compromised under Article 6 of the Directive, which limits decompilation to the licensees and/or equivalent rights holders [art 6/1(a)], with the limitation to "the information necessary to achieve interoperability [that] has not previously been readily available" [art 6/1(b)] and to "the parts of the original program which are necessary in order to achieve interoperability" [art 6/1(b)]. Likewise, the Directive bans usage of the obtained information "for goals other than to achieve the interoperability" [art 6/2(a)] and prohibits dissemination of such information "except when necessary for the interoperability of the independently created computer program" [art 6/2(b)] (See Otero (n 216) 88).

302 Weston (n 13) 200.

303 Weston (n 13) 200.

304 Inge Graef, 'How can software interoperability be achieved under European competition law and related regimes?' [2011] 5(1) Journal of European Competition Law & Practice 6, 16.

The *Softwarová*[305] judgement illustrates this elusive situation, where the CoJ was asked to determine whether the graphical user interface (GUI) of the computer programs would constitute an expression within the meaning of Article 1(2) of the Software Directive. As the question was related to the GUI, which is a user interface,[306] a possible answer would not directly solve the problems as to the APIs that ensure compatibility between the competitors. Nevertheless, some implications could be derived from the judgement. The CoJ made it clear that as a GUI does not enable the reproduction of a computer program it does not constitute a form of expression under the Software Directive.[307]According to the Court, the source code and object code of a computer program that permit reproduction in different languages constitute a protected form of expression.[308] While the GUI is not found to be protectable under the copyright regime of the Software Directive, the Court did not exclude the possibility that the interfaces could be copyrightable within the meaning of the InfoSoc Directive, namely the ordinary and generic copyright regime of the EU. However, copyrightability of APIs was not the issue that has been resolved under the case.

The issue has been brought before the Court by means of another case, *SAS Institute Inc v World Programming Ltd ('SAS v WPL')*,[309] which reveals a cornerstone decision for idea-expression dichotomy and copyrightability of software. The case arose out of the conflict that took place following a firm, World Programming Ltd (WPL), that developed a program that emulated the functionality of the popular statistical analysis

---

305 Case C-393/09, *Bezpečnostní Softwarová Asociace - Svaz Softwarová Ochrany v Ministerstvo Kultury* [2011] ECDR 3 *('Softwarová* judgement').

306 GUIs, which are not seen as part of the code but only as a result of the code, are also referred to as the "look and feel" enabling communication and interaction between the user and the computer program (Weston (n 13) 208).

307 *Softwarová* judgement, para 35.

308 *Softwarová* judgement, para 35.

309 Case C-406/10, *SAS Institute Inc v World Programming Ltd* [2012] 3 CMLR 4 ('*SAS v WPL judgement*').

program, SAS. Based on observing and testing SAS programming language and related manuals, WPL's attempt was a target-based response to the market demand for ensuring SAS-based statistical operations be performed on alternative platforms. The fact that WPL had no access to SAS source code or to the internal design documentation of the program, either directly or through decompilation,[310] makes the conflict interesting and potentially significant. After SAS sued WPL for infringement of copyright over its behaviour and the data formats of the SAS program as well as the SAS programming language, the case was taken to the CoJ for its interpretation under Article 267 of the TFEU.

The CoJ affirmed that there has been no copyright infringement in line with the finding of the UK High Court. The CoJ held that "neither the functionality of a computer program nor the programming language and the format of data files used in a computer program in order to exploit certain of its functions constitute a form of expression".[311] According to the CoJ, "to accept that the functionality of a computer program can be protected by copyright would amount to making it possible to monopolise ideas, to the detriment of technological progress and industrial development".[312] However, the Court statement pointed to the possibility that the access sought functional elements of the computer program in question would be considered as a subject matter of generic copyright protection i.e. under the InfoSoc Directive.[313]

---

310 Samuelson (n 199) 229.

311 *SAS v WPL* judgement, para 39.

312 *SAS v WPL* judgement, para 40. It is conceivable that this viewpoint is complementary to the *Softwarova* ruling, where the CoJ, whilst not excluding the copyrightability of graphic user interfaces, found that such interfaces do not constitute a form of expression of computer programs but enable users making use of their features.

313 *SAS v WPL* judgement, para 45.

The *SAS v WPL* case clearly shows that the ideas/expression dichotomy has been expounded by the Court with a favourable interpretation to enhance follow-on innovation, yet with no mention about the APIs. As explained above, the Software Directive sets out the rules for ensuring interoperability through reverse engineering bypassing the renowned copyright principle of the ideas/expression dichotomy. Copyrightability of interfaces being left unsettled both under the Directive and the CoJ's jurisprudence in *SAS v WPL*, the functional character of APIs[314] and the merging of ideas and expression on them,[315] blurs the distinction based on the so-called dichotomy with respect to the APIs. Therefore, although the copyright regime of the Software Directive provides control over the information embodied in the subject matter *per se*,[316] APIs would not be directly put into the same basket i.e. Article 1(2) of the Directive, considering their very functional nature and the inherent features of incorporating the non-expressive parts of the computer program.

If Article 6 of the Software Directive indeed reflects such a policy by allowing access via decompilation of a program's code to study its internal structure and other expressive aspects of program text, when this process is indispensable to achieving interoperability, it would make no sense to establish a right to access program internals and then to condemn the reuse of interface information discerned in this process as infringing when it is necessary to achieve interoperability.[317] Assuming the case for IPRs in computer programs is to improve the creation, innovation and dissemination

---

314 See also Vezzosso (n 203) 159, reading; "…[t]he functional character of APIs, being even stronger than with computer programs in general, would very often place them well below the originality threshold, and the general support in favour of interoperability expressed by the Software Directive could possibly present a further counterargument [against copyrightability of interfaces]".

315 Otero (n 216) 86, reading; "Since a computer program's form of expression is functional, variations of its expression will not matter because these possible variations come from utility reasons and not the 'aesthetic freedom' or whim of its developer. Therefore, expression and function merge. …"

316 Otero (n 216) 86. See Software Directive, art 1(2).

317 Otero (n 216) 86.

of knowledge to enable a competitive and prosperous software market,[318] the functional character of the interfaces ought to be taken utmost into account, alongside the pro-interoperability policy of the Software Directive. Last but not least, any prospective interpretation and solution would rather be in harmony with international copyright legislation, particularly TRIPS and WCT provisions, which expressly distinguish 'methods of operation' from copyrightable subject matter.[319]

4.2. Patents

4.2.1. General overview of the EU patent regime

Patents are granted to protect and stimulate inventions. Patents are of high importance in the high technology markets, as every ICT equipped device, including smartphones, computers and semiconductors are built on the patented technologies.[320] In general, for an invention to be patentable, some conditions must be fulfilled. The inventor who meets these criteria obtains the right to exclude all others without licence from making, using or selling the invention in the particular jurisdiction, usually for 20 years.[321] In return, patent holders are required to publicise (fully disclose) their inventions. There are several international conventions governing patents, among which, the most prominent ones are TRIPS and the UN WIPO Treaties. According to Article 27(1) of the TRIPS Agreement; "Subject to the provisions of paragraphs 2 and 3, patents shall

318 Weston (n 13) 198.

319 According to Article 9(2) of TRIPS Agreement and Article 2 of the WCT, copyright protection shall extend to expressions but not to the "ideas, procedures, methods of operation or mathematical concepts as such".

320 See Stefano Comino, Fabio M. Manenti and Nikolaus Thumm, 'The Role of Patents in Information and Communication Technologies (ICTs): A Survey of the Literature' (2017) Marco Fanno Working Paper N. 212, 3. According to the Organisation for Economic Co-operation and Development (OECD) and the WIPO figures, about one third of the patent applications were filed within the ICT-related sectors (Ibid).

321 Finkelstein (n 260) 249.

be available for any inventions, whether products or processes, in all fields of technology, provided that they are new, involve an inventive step and are capable of industrial application".[322] Similarly, the Paris Convention,[323] being administered by the WIPO, requires that 20 year patent protection be available for all inventions, whether of products or processes, in almost all fields of technology.[324]

In addition to the abovementioned treaties, the EPC has also a key role in the regulation of patents across the EU.[325] In EU Member States, inventors can apply through either the national or EPC route, which creates a twin-track system. The EPC route involves an application to the EPO in Munich, the inventor choosing ('designating') the European countries in which he wants a patent and paying the relevant fees.[326] Both European and national patents are granted the same treatment in terms of effectiveness. However, there is neither an EU legal framework nor European court dealing with the patent related issues e.g. infringement and revocation. Therefore, national courts have competence in their jurisdiction to give an affirmative decision as to whether a patent has been infringed, without being bound up with the EPO case law. Because the EPC does not provide for any supra-national court to rule on European patents once granted, as its Boards of Appeals are merely internal judicial organs overseeing decisions in respect of the grant of patents, there is a serious risk of the courts of the Contracting States applying different standards in cases concerned with validity and infringement.[327]

---

322 TRIPS Agreement, art 27(1).

323 Paris Convention for the Protection of Industrial Property (as revised at Stockholm in 1967).

324 Śaila Jaina and R. K. Jain, *Patents: Procedures and Practices with Examples of Complete Specifications and Important Judgements* (Universal Law Publishing Co. Pvt. Ltd. 2011) 174.

325 Regulation of patents originally goes back to the 1883 Paris Convention for the Protection of the Industrial Property, which allows special agreements between the members insofar as they do not create a contrast with the Convention itself.

326 Sir Robin Jacob, Daniel Alexander QC and Matthew Fisher, *Guidebook to Intellectual Property*, (6th edn, Hart Publishing 2013) 29.

327 Hellen Norman, *Intellectual Property Law*, (OUP 2011) 83.

According to Article 52(1) of the EPC, European patents could be granted for the inventions "which are susceptible of industrial application, which are new and which involve an inventive step".[328] As defined by the EPC for patentability, the invention should possess *novelty, an inventive step* and *industrial applicability*, not consisting of *excluded subject matter* or any of the *exceptions* to patentability.[329] According to Article 52(2) of the EPC, the following items *in particular* are not regarded as inventions for the purpose of patentability:

(a) discoveries, scientific theories and mathematical methods;

(b) aesthetic creations;

(c) schemes, rules and methods for performing mental acts, playing games or doing business, and *programs for computers*;

(d) presentations of information.

While the above given non-exhaustive list denotes the excluded subject matter,[330] 'exceptions' to patentability are placed under Article 53 of the EPC. Such exceptions include the inventions which are contrary to public order or morality, those involving plant and animal varieties or essentially biological processes for the production of plants or animals, and those incorporating the methods of treatment and diagnostic methods practised on the human or animal body.[331]

---

328 EPC, art 52(1).

329 EPC, art 52-57. See also Stavroula Karapapa and Luke McDonagh, *Intellectual Property Law* (OUP 2019) 401; Norman (n 327) 102.

330 This could also be seen from the wording of Article (52/3) which reads as follows:
"The provisions of paragraph 2 shall exclude patentability of the subject-matter or activities referred to in that provision only to the extent to which a European patent application or European patent relates to such subject-matter or activities *as such*".

331 EPC, art. 53.

4.2.2. Patentability of software and interfaces under the EU patent regime

While there is no argument against the patentability of computer technology in the sense of hardware, significant issues arise on the software side.[332] Principally, non-patentable items under the EPC consist of a number of "subject-matter or activities *as such*", including computer programs. Nevertheless, it is widely acknowledged that computer-implemented inventions could be covered by Article 52(1) of the EPC, which affirms patentability of industrial applications. Having said that, computer programs could not be patentable if they are meant to be inventions themselves. That is to say, software components of inventions could benefit from the European patent regime insofar as they are purported to be an industrial application. The key point that needs to be taken into account for patentability is the 'technical character' required for the computer programs. According to the EPC, they need to meet the criteria of 'novelty', 'inventive step' and 'industrial application'.[333]

According to the EPO, the subject matter for which patent is sought must have a technical character, more precisely, involve a "technical teaching"; that is an instruction addressed to a skilled person as to how to solve a particular technical problem, rather than, for example, a purely financial, commercial or mathematical problem, using particular technical means.[334] The Board of Appeal of the EPO set forth that a patent cannot be granted if the software is a mere implementation of an invention

---

332 Cesare Bartolini, Cristiana Santos and Carsten Ullrich, 'Property and the cloud' [2018] 34 Computer Law and Security Review 358, 369.

333 Paul Van den Bulck, 'Patentability of Software' (*ULYS Net*), <https://www.ulys.net/upload/conferences/doc/Patentability%20of%20Software.pps> accessed 21 August 2018. See EPO, Patents for software? European law and practice (2009) <https://tt.tecnico.ulisboa.pt/files/sites/41/PI-Pack-INPI-E-Patents-for-Software-EPO.pdf> accessed 9 October 2020. Similar criteria are also sought under the TRIPS and WIPO Treaties for patentability (See the section '4.2.1. General overview of the EU patent regime').

334 Van den Bulck (n 333).

with no technical teaching.[335] However, there will be no bar to patent protection for those inventions that are implemented through computer programs, if that implementation represents the solution to a technical problem.[336] Therefore, inventions having a technical character that are or may be implemented by computer programs e.g. refrigerators, washing machines, mobile phones, anti-lock braking systems (ABS) for cars, DVD players, medical imaging (X-Ray) and aircraft navigation systems, may well be patentable.[337]

To put in a nutshell, patents could be granted for programming the software aiming at a computerised (industrial) solution. This very aim also goes for the 'interfaces' that either enable a computer program's internal design or ensures its interoperability with other competing programs. Such interfaces are often distributed to third parties in object, machine-readable codes, so as to prevent unlicensed uses and copies. As the concealed, human-readable APIs could not normally be found out by executing commercially distributed object codes, access seekers would have to use reverse and social engineering i.e. observation and testing processes, to identify the interfaces at stake. To pre-empt such attempts from the outset, many software programmers and/or product designers hold patents, as well as copyrights, pertaining to such interfaces. The main factor that makes patents preferable is their power to enable the rights holders to far more easily detect and claim infringement against unlicensed products.[338] Indeed, the exclusionary power of patents is strong and effective even

335 See Case T 258/03, Auction Method/HITACHI [2004] OJ 2004, 575.
336 Zingales (n 62) 9.
337 Van den Bulck (n 333).
338 See also Peter Drahos and John Braithwaite, *Information feudalism* (Eartscan Publications 2002) 173, reading; "the companies that colonise the internet with these kinds of patents [i.e. 1-Click patent] and are able to enforce them using a combination of software tracking tools and the threat of litigation are in a position to become, in effect, the internet's private regulators".

when the technical design disclosed in the patent is only modestly innovative or an arbitrary variation on an existing technique.[339]

The fact that ICTs are based on incrementally developed software that are highly dependent on abstract algorithms arouses a long-standing debate as to what extent software ought to be patented, incorporating the interfaces. On both sides of the Atlantic, patentability of software and related interfaces has thus far been a matter of conflict among access/license seekers and patent holders. The ease for rights holders to claim infringement does have an effect to dissuade third parties from *making* or *using* the patents.[340] Moreover, there is not an exceptional right e.g. such as decompilation, for the purpose of interoperability under the European patent regime as opposed to the copyright regime. As is well-known from the patent wars in the smartphone industry, patents are claimed by their owners as a strategic and pre-emptive tool against their competitors.[341]

Hence, the allowance of widespread software patents in both the European and global systems is open to criticism. The cumulativeness and complexity of innovation in ICTs makes the role of patents less clear-cut, provided that a strengthening of the protection they guarantee may have heterogenous effects on the different generations of innovators.[342] The social value of early innovations is not only related to the utility generated from their use, but also to the positive externality they contribute to future

339 Samuelson (n 4) 1962-1963.
340 See supra note 217.
341 Based on survey data of inventors from 23 countries (European countries, Israel, USA and Japan)) filing applications at the EPO between 2003 and 2005, an empirical study shows that a substantial share of patents are not being used by firms internally or for market transactions and they interpret this evidence as support for the importance of strategic patenting (Comino, Manenti and Thumm (n 261) 4) referring to Torrisi et al, 'Used, Blocking and Sleeping Patents: Empirical Evidence from a Large-Scale Inventor Survey', [2016] 45(7) Research Policy, 1374-1385).
342 Comino, Manenti and Thumm (n 320) 4.

applications/developments.[343] From this viewpoint, it would be argued next generation inventions should be given leeway by the preceding ones.

Patent related critics gain importance in conjunction with the surge in patents in the ICT field and their potential to be used against the potential infringers as a strategic tool. Thereby, IPRs' passive and defensive role is turning into an offensive tool being aggressively used to keep out potential rivals from the relevant, mainstream or complementary, markets. This very impact potentially means unforeseen consequences for both consumer welfare and follow-on innovation, making a contradiction with the general meaning and purpose of the IPRs. Outnumbered patents for software-enabled products, sometimes resulting in patent thickets and hold-up problems, would need to be revisited from a socially oriented perspective.

At the EU level, several attempts have been made to create an exceptional right within the European patent system in favour of interoperability, culminating with a Directive proposal on the patentability of computer-implemented inventions in 2002.[344] During the negotiations on the proposed Directive, one of the spotted problems was the unfettered patent protection that would make acts initially permitted under the copyright *acquis* that allows reverse engineering in order to achieve interoperability, 'illegal'.[345] To deal with this problem, it was envisaged that the conferred rights under Articles 5 and 6 of the Software Directive would not be affected by the patent rights to be granted under the proposed Directive. It was proposed that those benefitting from

343 Comino, Manenti and Thumm (n 320) 5.

344 European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the patentability of computer-implemented inventions' (2002/C 151 E/05) COM (2002) 92 final - 2002/0047(COD).

345 Istvan Erdos, 'A Measure to Protect Computer-Implemented Inventions in Europe', [2004] 3 Journal of Information, Law and Technology <https://warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/erdos> accessed 9 October 2020.

Articles 5 and 6 of the Software Directive would not require the authorization of the rights holder with respect to the right holder's patent rights in or pertaining to the computer program.[346] During the review of the proposal by the European Parliament, several amendments were made including an additional provision stating that the use of a patented computer program for the purpose of achieving interoperability would not be considered a patent infringement.[347] However, the proposal was defeated by a vote of the European Parliament in July 2005.

4.2.3. Comparative analysis through the *Nintendo* case

While it might be argued that the fact that software patents are limited to the specific applications underlying certain inventions of technical character does not present major obstacles to market competition, their cumulative effect, in combination with copyrights, should not be underestimated, particularly in terms of interoperability. Their largely hidden nature would make potential infringements unrecognisable for the third parties creating a clear impact of blocking markets to competitors. This is well illustrated by the *Nintendo*[348] case analysed below.

4.2.3.1. Brief analysis of the case

The *Nintendo* case, originated in the US, has arisen out of the patent, as well as copyright, infringement claim by Nintendo after a rival manufacturer, Atari Games (Atari), had produced game cartridges compatible with Nintendo Entertainment System (NES), namely Nintendo's home video game console on which Nintendo

346 Ibid.
347 Graef (n 304) 15.
348 *Atari Corp. and Tengen Inc. v. Nintendo of America Inc. and Nintendo Co. Ltd.,* 975 F.2d 832, (Fed. Cir. 1990) ('*Nintendo* judgement').

games are authorised and played. While non-Nintendo games, or the games not licensed by Nintendo, were originally prevented from running on the NES platform (game consoles) via an authorisation technique called "10NES", the game cartridges produced by Atari allowed its users to play Atari games on the NES. Following Atari launching its compatible game cartridges,[349] Nintendo sued its rival for the infringement of its patents and copyrights for the authentication technique it had been running on the NES platform.

Atari, who failed to maintain its already installed base against the exclusive contracts and more sophisticated videogames of Nintendo, brought antitrust files under the US Sherman Act. Claiming that such exclusive deals amounted to monopolization in the videogame console market, Atari took the issue with Nintendo's misuse of "10NES", particularly by means of a patented lock-out chip that operates through a dedicated computer program.[350] The US District Court for the Northern District of California consolidated the two cases and preliminarily enjoined Atari from exploiting Nintendo's copyrighted computer program by upholding that Nintendo had shown a likelihood of success on its copyright infringement claims.[351]

The Federal Circuit, on appeal, affirmed the findings of the California District Court with the exception that Atari's reverse engineering was found legitimate under "fair use doctrine". Emphasizing that "an individual cannot even observe, let alone understand, the object code on Nintendo's chip without reverse engineering",[352] the

349 Normally an initiation technique (10NES) was originally designed by Nintendo with the aim to create a specific access code for the authorized games to run on the Nintendo platform. Atari succeeded to produce game cartridges generating a similarly functioning data stream to initiate 10NES and allow Atari games to run on the NES consoles (Samuelson (n 4) 1965).

350 Zingales (n 62) 20.

351 *Nintendo* judgement, 1.

352 According to the Court, "An author cannot acquire patent-like protection by putting an idea, process, or method of operation in an unintelligible format and asserting copyright infringement

Court also pointed out that "fair use did not give Atari more than the right to understand the 10NES program and to distinguish the protected from the unprotected elements of the 10NES program".[353] According to the Federal Circuit, the District Court's finding of copyright infringement was affirmed by the fact that Atari's Rabbit program, or chip, embedded into the Atari cartridges "incorporates elements of the 10NES program unnecessary for the chip's performance", thereby going beyond unlocking the 10NES program.[354]

Following the Federal Circuit's remind decision over the antitrust allegations, the two parties ended up with a settlement. However, the Federal Trade Commission (FTC) took the antitrust issue, with a focus on Nintendo's exclusive licences hindering access to its proprietary platform by third parties. The FTC's challenging decision was followed by the same basis intervention of the European Commission, resulting in Nintendo's changed licensing policies (with Sega and Sony, for they pursued similar strategies).[355] Despite the lifting of restrictions in its licensing agreements, the Japanese company continued to rely heavily on lock-out chips by embedding copyrighted software into its consoles; it ensured that only cartridges containing the code for that particular Nintendo console could be played.[356] Over time, this strategy triggered the hostility of the user community and led to widespread deployment of so-called "modchips", i.e. electronic devices which disable the encryption mechanisms

against those who try to understand that idea, process, or method of operation" (*Nintendo* judgement, 9).

353 *Nintendo* judgement, 11.

354 *Nintendo* judgement, 12.

355 See European Commission, 'Commission opens proceedings against Nintendo distribution practices' (Press Release, IP/00/419, 28 April 2000) <https://europa.eu/rapid/press-release_IP-00-419_en.htm?locale=en> accessed 9 October 2020.

356 Zingales (n 52) 22. This code served also to segment markets geographically, by requiring videogames to be run only on hardware sold in the same geographic area, such as North America, Europe and Asia (Ibid).

embedded in the console to enable the interoperability of videogames made or distributed by non-authorized developers.[357]

Consideration of "modchips" under the circumvention provision, i.e. Article 6(2),[358] of the InfoSoc Directive has been addressed by the CoJ, following several cases filed before the national courts resulting in different rulings.[359] Although the finding was inconclusive on the matter, the CoJ made clear that the legal protection offered by Member States must respect the principle of proportionality, not prohibiting devices or activities which have a commercially significant purpose or use, other than circumventing a TPM for unlawful purposes.[360]

The Court's reference to proportionality is practically meant "to examine whether other measures, or measures which are not installed in consoles, could have caused less interference with the activities of third parties not requiring authorisation by the rights holder of copyright, or fewer limitations to those activities, while still providing comparable protection of that rights holder's rights".[361] Accordingly, the Court's ruling could be interpreted in permitting the design of TPMs with a view to allow legitimate activities in view of the nature, costs and other aspects, but not illegal copying.[362] In similar cases, access seekers are thus charged to demonstrate the TPMs they attempted to access are more intrusive than necessary to prevent circumvention

357 Zingales (n 62) 22.
358 See supra note 73.
359 *Nintendo Co Ltd and others v PC Box Srl*, Case C-355/12, (23 January 2014) ('*Nintento* preliminary ruling').
360 Zingales (n 62) 22.
361 *Nintendo* preliminary ruling, para 32.
362 The factors underlined by the Court to be taken into consideration include; "the relative costs of different types of technological measures, of technological and practical aspects of their implementation, and of a comparison of the effectiveness of those different types of technological measures as regards the protection of rights holder's rights, that effectiveness however not having to be absolute" (*Nintendo* preliminary ruling, para 33).

and copyright infringements. The key complication in that respect is that the burden of proof for this inquiry is borne by the defendant (access seeker), who would usually not have sufficient evidence as occurred in the abovementioned case giving rise to the preliminary reference.[363]

4.2.3.2. Beyond *Nintendo*: Balancing between legitimate rights

Under the light of sequential conflicts and debates following the *Nintendo* case, the judicial solutions based on the 'fair use' doctrine and the legitimacy of 'reverse engineering' seem to have a balanced approach against the legally and economically justifiable rights. When tracing back to the roots of 'reverse engineering', one will meet the 'fair use' defence that was largely echoed in the US jurisprudence before being codified under Title 17, Section 107 of the 1976 US Copyright Act (USCA).[364] Initially framed under the *Sega Enters. v. Accolade Inc.*[365] judgement, the 'fair use' doctrine has been built upon four factors, as translated under Title 17, Section 107 of the USCA. Before this codification, the courts, both in the *Sega* and *Nintendo* cases, recognized the unique characteristics of software and understood that if reverse engineering were not permitted, the developer would receive *de facto* protection over uncopyrightable ideas.[366] As rooted in these US precedents, the

---

363 Zingales (n 62) 23.

364 Title 17, Section 107 of the USCA reads as follows:

> "The fair use of a copyrighted work… for purposes such as criticism, comment, news reporting, teaching, … scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include:
>
> (i) The purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes;
>
> (ii) The nature of the copyrighted work;
>
> (iii) The amount and substantiality of the portion used in relation to the copyrighted work as a whole;
>
> (iv) The effect of the use upon the potential market or value of the copyrighted work".

365 *Sega Enterprises Ltd. v. Accolade, Inc*., 977 F.2d1510 (9th Cir. 1992).

366 Band and Katoh (n 55) 19.

reverse engineering privilege more explicitly recognizes the value of interoperability and copyright's role in promoting it.[367]

When evaluating legitimate interests of the third parties for alleged copyright infringements, the 'fair use' doctrine goes beyond the boundaries of 'reverse engineering', even conceivable arguably to reach out to patent holders, under the US legal system.[368] While the former is codified in the US Copyright Act (17 USCA § 107), the latter was permitted under a broadly-formulated provision under Section 103(f) of the DMCA (17 USCA § 1201(f)).[369] Having served as a key tool for the permissibility of reverse engineering in the years preceding the DMCA, the 'fair use' defence complements other jurisprudence tools, i.e. merger doctrine, patent misuse and enabling internal safeguards for the IPR regime in the USA.

On the other hand, IPR rules and specifically the patent regime in the EU lack internal safeguarding tools responding to actual or potential anti-competitive results that would arise from overprotection of interfaces and accompanying reasons i.e. anti-circumvention rules. Alternative interpretative ways or solutions based on the 'proportionality' principle, as implicated by the CoJ in the *Nintendo* proceedings, would require much more fine-tuning to respond to the legitimate interests of the access seekers, including reverse engineering for the patented products.[370] While the

---

367 Perzanowski (n 40) 116.

368 See Samuelson (n 4) 2008, reading; "It is also conceivable although somewhat less likely, that U.S. courts will adopt the fair use defense proposal … to balance the patent holders' and public interests at stake in cases involving patents affecting interoperability".

369 Section 1201(f) titled 'Reverse engineering' permits the development and use of technological means of circumventing a technological measure for the purpose of enabling interoperability, providing exceptions to relevant prohibitions i.e. on the circumvention of access controls and on the manufacture and distribution of devices that circumvent access controls and/or copy controls (See Band and Katoh (n 55) 82-83).

370 The attempts in the EU aiming to ensure that patented software products are to be subject to reverse engineering exemption, such as copyrighted computer programs, have failed so far. See Graef (n 304) 15. See also the section '4.2.2. Patentability of software and interfaces under the EU patent regime'.

CoJ's way of interpretation would give way to less restrictive TPMs signalling a further leeway for interoperability, patent-based real life problems still prevail, threatening market entries and innovative derivations on top of the protected products. In this vein, the limitedness of reverse engineering to ensure interoperability of copyrighted computer programs as well as lack of internal safeguards, unlike in the US system, appear as the major deficiencies of the patent and more broadly IPR regime in the EU.[371]

Patents' monopoly granting features makes it more difficult for the competitors who lack US-like internal safeguards not to face infringement claims when they intend to reach interface information.[372] Overprotection of interfaces which might serve as standards is a matter potentially going beyond the boundaries of the IPR regimes, with far-reaching implications as framed above that could be affiliated to patent protection.

Overall, not only the EU copyright acquis but also the EU patent regime and related mechanisms fail to adequately address the indirect effect of proprietary controls over interface specifications on interoperability i.e. including market blocking and

---

371 In lieu of such internal safeguards and more enhanced IPR protection, competition law tools are much more invoked in the EU, with a stronger role over the anti-competitive effects stemming from patent exploitation.

372 On the other hand, it is also argued that the US anti-circumvention laws i.e. DMCA, are not sufficient in view of a number of shortcomings (See Perzanowski (n 40) 141-142). Perzanowski elaborates the shortcomings as follows:

> § 1201(f) does note embrace all the interoperable technologies. Section 1201 (f) permits the circumvention of technological measures that protect computer programs, but not "works generally, such as music or audio-visual works … distributed in digital form" As a result, interoperable products that make use of technologically protected entertainment content or other works are open to attack under the DMCA. The disparity in the treatment of these two classes of interoperable technologies is the result of two problematic distinction. First, this inequality relies on a clear division between technological measures that protect computer programs and those that protect other copyrighted works. Second, it relies on a distinction between program interoperability and data interoperability. Both distinctions are the product of factual oversimplifications, and neither supports exempting one class of interoperable technologies while subjecting the other to DMCA liability (Perzanowski (n 40) 141-142).

foreclosure, particularly given the fact that patent protection of interfaces can hardly be justified by the purported goals i.e. promoting innovation and dissemination.[373]

4.3. Trade secrets

Trade secrets represent another major field of intellectual property protection when considering interfaces from the interoperability perspective. Given the fact that source code is considered to be the source of the originality as to the computer programs, authors/developers of computer programs tend to keep such code as trade secrets, as well as resting on copyrights and patents. Because of the difficulty of qualifying for patent protection and the thin scope offered by copyright protection, this represents a valuable and concrete opportunity for the software developers in terms of preventing interoperability.[374] At the international level, a number of requisites are laid down by the TRIPS Agreement, regarding the information to be covered by trade secrets. According to this Treaty's provisions, the presence of trade secrets is acknowledged so long as such information:

(1) 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;

(2) has commercial value because it is secret; and

[373] See Weston (n 13) 288.
[374] Zingales (n 62) 11.

(3) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret[375]

As could be seen above, trade secrets are meant to protect commercially valuable information which is kept as confidential via reasonable steps. In this scope of protection, the existence of intrinsic innovation is not sought in the software products covered by trade secrets. Under TRIPS, the very nature of trade secrets seems to have been regulated with no certainty regarding the prospect of the information obtained from reverse engineering, even though this process is considered not to be affected by trade secret protection.[376] Because trade secrets have acquired strong protection since codification in Article 39 of the TRIPS Agreement, demanding the protection of relevant technical information on software programs has thus far had the effect of adding another layer of protection to them, potentially with significant anti-competitive effects for the firms that need interoperability in order to compete in the same or an ancillary market.[377] Partially to respond to this as well as to ensure dissemination of knowledge and information, the European authorities recently enacted the Directive 2016/943.[378] The referred Directive (Trade Secrets Directive) has entered into force on 8th June 2018, to be transposed by the Member States within a two-year period, with the ultimate aim of harmonization of national trade secret laws.

375 TRIPS Agreement, art 39(2). Under the TRIPS provision, the protection of trade secrets against third parties' unauthorised disclosure, acquisition or use is bound up with such acts taking place "in a manner contrary to honest commercial practices."

376 Weston (n 13) 230-232.

377 Gustavo Ghidini and Emanuela Arezzo, 'One, none, or a hundred thousand: how many layers of protection for software innovations?' in J Drexl (eds), *Research Handbook on Intellectual Property and Competition* (Edward Elgar 2008) 363.

378 Directive (EU) 2016/943 of the European Parliament and of the Council on 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure ('Trade Secrets Directive').

First and foremost, the Trade Secrets Directive follows the three requirements set out by the TRIPS Agreement.[379] Notably, protection for trade secrets diverges from copyrights and patents in the sense that a trade secret is only protected against "unlawful acquisition, use and disclosure", which are specified under Article 4 of the Trade Secrets Directive. Notwithstanding, according to Article 3 of the Directive, "the acquisition of a trade secret shall be considered lawful when the trade secret is obtained by … (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".[380]

Having said that, alongside presumably the primary means of 'independent discovery or creation', 'reverse engineering' appears to be an alternative means to acquire the information to be covered by the trade secret.[381] Information obtained from reverse engineering should thus avail of a similar protection under the Trade Secrets Directive. However, this is bound with the stipulation that such a trade secret "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".[382] Having said this, once the acquisition or use has happened, a possible conflict of interests would arise under the Software

---

379 As per Trade Secrets Directive, all the following requirements should be met by the information as a 'trade secret':
1) 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;
2) it has commercial value because it is secret; and
3) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret (Trade Secrets Directive, art 2(1)).
Accordingly, commercially valuable business information or know-how may be protected as long as it is kept secret by the holder by way of, for example, non-disclosure or confidentiality agreements (Inge Graef, 'Data as Essential Facility Competition and Innovation on Online Platforms' (PhD Dissertation, KU Leuven Faculty of Law 2016) 144).

380 Trade Secrets Directive, art 3(1/b).

381 Trade Secrets Directive, art 3(1).

382 Trade Secrets Directive, art 3/1(b).

Directive as well as the Trade Secrets Directive which aims to strike a balance between dissemination and retaining of the information given the specified statutory rights.

In fact, a link could be established between the so called Directives on the proposition of "the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret".[383] The implicated requirement of "the free[dom] from any legally valid duty to limit the acquisition" would mean the ability to reverse engineer to the extent acknowledged and allowed under the Software Directive.[384] It is remarkable that the Trade Secrets Directive implicitly points to the limits of lawful reverse engineering, while explicitly acknowledging the legality of reverse engineering as well.[385] Given the fact that restrictions under Article 6 of the Software Directive could amount to such a "legally valid duty", decompiled codes would be deemed outside of the 'lawful acquisition, use and disclosure' enshrined under the Trade Secrets Directive should they exceed the limits of the Software Directive.[386]

Another limitation of the Trade Secrets Directive relates to the contractual rights and unfair competition laws, which are featured under this Directive in the sense that these safeguards would be pre-emptive over the lawful reverse engineering. In this respect, the Trade Secrets Directive clarifies that "reverse engineering of a lawfully acquired product should be considered as a lawful means of acquiring information, *except when otherwise contractually agreed*".[387] Also, it is noteworthy that national unfair

---

383 Trade Secrets Directive, art 3/1(b).

384 Remarkably, Article 6(2) of the Software Directive does not permit the information obtained through decompilation (a) to be used for goals other than to achieve the interoperability of the independently created computer program; (b) to be given to others, except when necessary for the interoperability of the independently created computer program; or (c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

385 Trade Secrets Directive, recital 16 and art 3/1(b).

386 Sally Weston, 'Improving interoperability by encouraging the sharing of interface specifications' [2017] 9(1) Law, Innovation and Technology 78, 85.

387 Trade Secrets Directive, recital 16.

competition laws could make it difficult to reverse engineer the information that would normally be kept under the trade secrets. This is expressed as follows:

> In some industry sectors, where creators and innovators cannot benefit from exclusive rights and where innovation has traditionally relied upon trade secrets, products can nowadays be easily reverse-engineered once in the market. In such cases, those creators and innovators can be victims of practices such as parasitic copying or slavish imitations that free-ride on their reputation and innovation efforts. Some national laws dealing with unfair competition address those practices.[388]

Considering that it is implied, both contract and unfair competition laws could offer some safe harbours for the trade secret holders, it is clear to say that reverse engineering of the related information could not be favourably treated under trade secret provisions. Although counter arguments would originate from the Software Directive which regards contractual provisions contrary to reverse engineering as "null and void",[389] the Trade Secrets Directive conferring an important role to unfair competition law rules, as well as contractual rights and obligations, would mean some potential conflicts yet to be resolved against lawful reverse engineering. Further to this, the possibility that Article 8(1) of the Software Directive would be interpreted as favourable to contractual clauses and unfair competition law rules[390] substantiates the potential conflicts referred to above.

---

388 Trade Secrets Directive, recital 17.

389 Permissibility of the contractual obligations contrary to the reverse engineering is challengeable, considering the fact that the Software Directive clearly bans "any contractual provisions contrary to" reverse engineering and acknowledging them as "null and void" (Software Directive, art 8/2).

390 See Software Directive, art 8(1) reading; "[T]he provisions of this Directive shall be without prejudice to any other legal provisions such as those concerning patent rights, trademarks, unfair competition, trade secrets, protection of semi-conductor products or the law of contract".

Under the light of the above information, attempts to reach to the APIs through reverse engineering could be doomed to failure against commercial practices e.g. license terms and contractual obligations, which might regard relevant information as trade secrets.[391] Article 6 of the Software Directive does not give any express right to use the reverse engineered information, so arguably a clause preventing its use may not fall foul of Article 8 of the Software Directive as well as the Trade Secrets Directive.[392] That is to say, the uncertainty as to the legitimacy of reverse engineering under the given statutory provisions of the EU law would be a grave risk for the competitive ICT players in effect.

4.4. Databases

Another form of intellectual property applicable to ICTs are databases, which are regulated by the EU Directive 96/9/EC ('Database Directive').[393] Under this Directive is created the *sui generis* database right, which differs from the conventional copyrights that build on the 'originality' criterion. When this criterion is met, copyright protection could be claimed along with the database right. Thus, a dual regime could be mentioned under the Database Directive whereby copyright is granted over the structure of the databases and the *sui generis* database right is provided to protect the content of the databases.

Article 4(1) of the Database Directive confers copyright protection to those databases, which, "by reason of the selection or arrangement of their contents" are considered to constitute the author's own intellectual creation. Therefore, the originality requirement

391 This does not prevent the reverse engineering of the interface, but purports to restrict the use of the resulting information even where there is no copyright protection (Weston (n 13) 231).
392 Weston (n 13) 231.
393 Directive 96/9/EC of the European Parliament and of the Council on 11 March 1996 on the legal protection of databases [1996] OJ L 77 ('Database Directive').

in this copyrightable material is comparably less demanding than the normal standards. On the other hand, while "the copyright protection of databases provided for by this Directive shall not extend to their contents",[394] reproduction of data stored in a database may constitute an infringement of the copyright of the data contained therein.[395] This result is bound with the pre-condition that the content is 'original' in representing the author's own intellectual creation within the meaning of normal/conventional standards.[396]

On top of the copyright granted for the databases themselves, a *sui generis* database right is conferred onto the same subject matter insofar as it involves "qualitatively and/or quantitatively substantial investment in either the obtaining, verification or presentation of the contents".[397] This right, which enables the author of the database "to prevent extraction and/or re-utilization of the whole or of a substantial part … of the contents of that database"[398] is enforceable even though the subject matter of the right is not copyrightable.[399] In any case, both the copyright and database right that are enshrined under the Database Directive do not affect any rights related to the data and

394 Database Directive, art 3(2). Notwithstanding, according to the same Directive provision, the copyright in question should be interpreted "without prejudice to any rights subsisting in those contents themselves".

395 Zingales (n 62) 13.

396 Such originality does not refer to the arrangement and selection of the data, which is the focus of the inquiry into the specific copyright protection for databases, but rather to their intrinsic nature as a "work of art" which may or may not belong to the database maker, depending on who created that data in the first place (Zingales (n 62) 13).

397 Database Directive, art 7(1).

398 For the purpose of the Database Directive, 'extraction' means "the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form" (Database Directive, art. 7/2(a)), whereas 're-utilization' means any "form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission" (Database Directive, art. 7/2(b)).

399 Besides, according to the Database Directive, "the repeated and systematic extraction and/or re-utilization of insubstantial parts of the contents of the database, implying acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database" is also protected on the part of the author of the database (See Database Directive, art 7/5).

the content that makes up the databases. Enforceability of the database right relies upon the investment done by the author of the database. In four related preliminary rulings delivered in November 2004, the CoJ made clear that the substantial investment required for a database to be protected under the sui generis right must relate to the creation of a database as such and that investment in creating the materials which make up the contents of the database cannot be taken into account.[400]

Given the breadth of the *sui generis* protection and the limited scope of the exceptions established or foreseen in the Directive,[401] it is apparent that database protection is broad enough to potentially cover a vast amount of data mining activities, yet with the potential to raise significant obstacles to the deployment of data mining techniques as well.[402] Since data access is not included within the *sui generis* database right, from the perspective of data mining and analytics, underlying elements of databases would pose important barriers for the third parties, even for the subscribers to the database. As these parties are banned from reaching out to the substantial parts of the contents of the database, their potential attempts to ensure interoperability would be ineffective.

From this point of view, should we deem access to databases an inner boundary for data miners, interoperability or access to interfaces would be considered as the outer boundary. The former (inner boundary) would have the effect of a legal barrier in the sense that cutting edge technologies including cloud computing and the IoT platforms would rest on a variety of IPRs including databases, and potential attempts to ensure interoperability would fail in the end. For instance, in the IoT context, data access or mining could not succeed even after the achievement of interoperability i.e. in the case

400 Graef (n 379) 139.
401 Database Directive, art 8 and 9.
402 Zingales (n 62) 14.

that interfaces that represent outer boundaries have been rendered available e.g. through reverse engineering.[403] That is to say, APIs being available does not mean transcending inner boundaries of IPR protection, namely databases, which are covered by copyright and the *sui generis* right.[404]

A similar situation could be mentioned about cloud computing, components of which are usually protected by the IPRs, including the *sui generis* database right. Whereas the Database Directive is cemented in the conventional paradigm that databases have a fixed structure and location where one accumulates and stores data, cloud computing would challenge this inherent understanding.[405] While this would augment the problems surrounding the cloud-based access and interoperability across different jurisdictions, the main problem across the EU appears to be the difficulty of the re-use of the datasets because of the so-called inner boundaries.[406] A report before the European Parliament points to this difficulty, qualifying the Database Directive "an impediment to the development of a European data-driven economy" whereby it is idealised that end-users have unrestricted data access, including re-use of the datasets covered by the databases.[407] While it seems uneasy to establish a strong link between a data-driven economy and database protection, it is possible to say that sui generis database rights creates another layer of IPR protection for running the widespread ICT services such as cloud computing and IoT, potentially making it difficult data mining and access, and rendering attempts to ensure interoperability meaningless.

---

403 Unver (n 30) 101-102.

404 Unver (n 30) 102.

405 Bartolini, Santos and Ullrich (n 332) 370.

406 Notwithstanding, there seems to be no statutory barrier against data flow across the EU, particularly following the entry into force of the Regulation 2018/1807, which sets out several measures to ensure that every business and user is able to process and store any data across the EU. See also infra note 775.

407 See Bartolini, Santos and Ullrich (n 332) 369, referring to the European Parliament, Committee on Industry, Research and Energy and Committee on the Internal Market and Consumer Protection, *Report on Towards a Digital Single Market Act*, 21.12.2015.

4.5. Assessment of intellectual property rights

IPRs, built upon different types, along with accompanying rights, bring out distinct layers of protection over the software and hardware components of ICTs. Copyright is meant to encourage and stimulate original creations, incorporating both source and object codes that underlie the expressive elements of computer programs. Patents aim to protect technical methods that are meant to be inventions which are acknowledged to include written codes. Trade secrets, rather narrowly fashioned in nature, are designed to protect the commercially valuable information that is kept as a secret on the part of the owner. Databases, adding another, fourth layer of protection, are subject to the *sui generis* database right based on "a substantial investment in either the obtaining, verification or presentation of the contents".

Remarkably, while each category of IPR is formulated to build on a distinct purpose and scope, they create distinctive layers of protection along with the potential to exclude rivals from copying, making or using the subject matter of the right. Against this background, it is remarkable that a type of exclusionary effect is embodied in the IPRs, although this is less persuasive regarding the trade secrets. Given this fact, a long-lasting debate is at stake with regard to the extent to what IPRs should have such an effect over the rival technologies and would-be products. For instance, while there is no serious debate over the copyrightability of hardware elements, against the complex and abstract nature of the software, distinguishing the literary and expressive parts of software from the non-literary ideas poses a difficult task, having direct implications for the interfaces. In fact, although reverse engineering and decompilation are allowed under copyright *acquis*, how to treat the APIs discerned through these lawful acts is yet to be settled under EU law and jurisprudence. Whilst the EU

copyright regime is acknowledged to cover the source and object codes, uncertainty still exists concerning the nature of APIs which are the key to interoperability.

Albeit with the uncertainty mentioned above, reverse engineering is permitted in the Software Directive, subject to certain restrictions. The effectiveness of this solution is however challengeable as not representing an unfettered right for access to the interfaces. There are, at least, three reasons why the reverse engineering exception may not go far enough to promote interoperability:

(1) Some kinds of computer programs may enjoy dual protection under both patent and copyright law in some countries,

(2) Copyright holders sometimes use TPMs to lock up their programs so that they may not be lawfully reverse engineered without breaking the lock to access them,

(3) Would-be second comers sometimes require access to more information than just the object code owned by the first-comer in order to design an interoperable software product.[408]

On top of these reasons, it should also be kept in mind that no one but the first intruder (access seeker) could benefit from this method of securing interoperability given the fact that dissemination of the decompiled information is prohibited by Article 6 of the Software Directive. Moreover, software interfaces could change frequently and pose a significant uncertainty for the competitors because of the emergent complexity and upfront costs. Thus, reverse engineering arises as an expensive, time-consuming and

[408] Eagles and Longdin (n 266) 52.

unsustainable option to be hardly deemed as a self-standing business model enabling interoperability in the ICT field.

While the abovementioned uncertainties are not directly relevant to patents, computer-enabled inventions that are protected by patents might be more restrictive than copyrights in terms of preventing third parties from re-using the protected software, including the APIs. Principally, when access to information contained in the APIs does not involve the "making" or the "using" of the patented invention, no patent infringement would take place. Given this fact, reverse engineering does not amount to patent infringement by itself; yet one could face up to an infringement claim by making use of the protected interfaces. While every interface could not benefit from the protection because of the threshold i.e. 'technical effect' within the meaning of invention, the position of the EPO has progressively moved, and more and more inventions related to computer programs have been successfully granted patent protection in the EU.[409]

In view of these facts, the patents' blocking power against the reusability of software, including the interfaces, could be significant. Essentially, patents may hinder interoperability information being discerned and reused by the third parties, and their cumulative effect would be augmented with other IPRs. In fact, proliferation of IPRs, particularly patents, often accompanies a situation where more parties have the right to exclude their rivals or opt to impose an excessive licence/royalty fee. Absent contractual commitments or licensing obligations i.e. which may be imposed by

[409] Bartolini, Santos and Ullrich (n 332) 370.

SSOs,[410] means firms can usually charge higher royalty rates for licensing interface patents than for licensing other patents, regardless of the degree of innovation the interface patents may embody.[411] This would mean a double-edged threat for the access seekers, having a deterrent effect on the dissemination of knowledge and innovation. Crucially, protection of IPRs come up with a remarkable cost as to information flows, as opposed to the very basis of the IPR regimes. Under a strict interoperability regime, the intended dissemination would not be realised, nor a diverse cultural production based on IPR-protected content. This is more persuasive for the EU legal system which does not have internal IPR safeguards, unlike the US framework, that enjoys a number of jurisprudential tools for mitigation of IPR-based anti-competitive effects i.e. patent misuse, fair use and merger doctrines.

From a broader viewpoint, a similar handicapping effect could arise out of trade secrets, which are also regulated under EU law. While the act of reverse engineering to reach certain information that is already protected by trade secrets is first and foremost legal,[412] unfair competition law and contract law regulations are acknowledged to take precedence over the copyright rules and the exceptions under the Software Directive.[413] By the same token, the wording of the Trade Secrets Directive enables restricting re-use of the interfaces even where no copyright exists, should the interfaces reflect the acquired information under certain limitations e.g. limits regarding decompilation, national unfair competition and contract law obligations.

---

410 Most SSOs encourage IPR owners involved in standardisation to disclose upfront i.e. prior to the adoption of a standard, the IPRs that they consider may be essential for its implementation (See the section '2.1.4. Standardisation').

411 Samuelson (n 4) 1963.

412 Trade Secrets Directive, art 3/1(b).

413 Software Directive, art 8.

Databases, subject to copyright protection as well as *sui generis* protection under certain circumstances, as set out under the Database Directive, would involve an added layer of protection, even though they do not pose a barrier to interoperability themselves. Notwithstanding, transcending the outer layers of protection, i.e. other IPRs than databases, by enabling interoperability does not warrant reusability of datasets included within the databases, as this means an infringement under the Database Directive. Therefore, reverse engineering and other attempts to ensure interoperability would enable data mining and access, yet not bring an effective result for the databases that are protected by the rights mentioned above, which represent the inner boundaries precluding access and/or copying.

From an overall perspective, while the IPRs aim to prevent infringement by limiting the user's ability to copy/lend/modify files and devices, their practical application often goes much further than this purpose, especially through preventing interoperability of file formats and devices.[414] This problem is also a result of and/or supported by the creation and use of TPMs going beyond their anti-circumvention purpose e.g. through preventing the use of copyrighted works that are legal, such as fair use/dealing or copyright for private/research purposes.[415] Given this fact, one could mention about an 'indirect effect' of implementing IPRs besides their directly attributable original purpose. Having said that, the effect of the IPRs embracing interfaces would entail 'over-protection' that goes beyond the very aim of the protection of the innovation, technical invention, commercial secret and valuable information by often displacing the rivals away from the potential competition.

414 Daly (n 23) 97.
415 Daly (n 23) 97.

Crucially, the indirect effect of controlling these interfaces impacts competition and innovation.[416] The increasing number of IPR types and layers would have significant anticompetitive effects for the firms which need interoperability to sell products that either work with or compete with the protected program.[417] The indirect effect of the protection of the interfaces via IPRs would emerge in the form of blocking the third parties from entering into the relevant market or competing effectively, at the expense of consumer benefits and choices being diminished. The indirect effects are extendable to the cultural production and participatory democracy given the major concerns and the inflexible legal regime regarding interoperability. While a fulfilling analysis of the negative impact of overzealous use of IPRs goes beyond the limits of this study, it is fair to say that IPR rules and safeguards including those related to interoperability at the EU level fail to adequately address the indirect effects of the control over interface specifications, on interoperability.[418]

Against this background, the pro-interoperability policy of the Software Directive could potentially be taken as a leverage to figure out and meet the needs surrounding 'information flows' and from a wider perspective, the 'global information infrastructure'.[419] Notwithstanding, the limited nature of the exceptional rights under Articles 5(3) and 6 of the Software Directive fall short of meeting these broadly minded information and interoperability needs as well as coping with the related concerns highlighted above. Given the wide range of underlying techno-social and competition concerns and the surrounding gatekeeping roles and functionalities,

416 Van Rooijen (n 40) 203.
417 See Ghidini and Arezzo (n 377) 363.
418 See also Weston (n 13) 257.
419 See Mansell and Steinmuller (n 263) 1.

existing tools and measures of the EU law, being not limited to the Software Directive, appear shortcoming to address the given concerns.

5. EU Competition Law

EU competition law is one of the areas where interoperability is regulated for the purpose of protecting, ensuring and restoring competition. In this regard, structural and/or behavioural measures are resorted to through a wide range of tools to deal with abuse of dominance, collaborative acts, i.e. agreements, concerted practices and market concentrations i.e. merger and acquisitions. These so-called situations are examined respectively under Article 101 and 102 of the TFEU and the 2004 Merger Regulation. Such instruments are invoked to investigate whether abusive behaviours e.g. refusal to supply, discrimination, tying; collaborative or concentrative undertakings under question pose any threat for competition over the relevant market(s). While the anti-competitive effects need not necessarily be actual or experienced, but exceed some thresholds in the sense that they create some risk and likelihood as to create unintended consequences e.g. reduced competition, lessened innovation, increased prices and/or deteriorated quality.

Under EU competition law, in almost all cases, ‘market definition’ is the first step that needs to be fulfilled to identify the competitive products which are substitutable (interchangeable) with each other. Once the market is defined, it should be ascertained whether market power is foreseen to arise or already present in the relevant market(s). This latter step means designation of dominant undertakings, which has a key effect particularly to reach any finding of abuse of dominant position. During the assessment of abusive behaviours, the scrutiny is focused on the actual or realised conducts to

analyse whether any anti-competitive behaviour has taken place, whereas other analyses, i.e. under Article 101 of the TFEU or merger controls, mostly depend on an ex-ante assessment of the undertakings in question. Below, the competition law tools and remedies available under EU competition law are analysed along with the case law. In this regard, 'market definition' is analysed first, to be followed by Articles 101 and 102 of the TFEU and merger controls. In so doing, the focus is intensified on interoperability-based concerns and remedies followed in the EU precedents, particularly CJ judgments.

5.1. Market definition

Structural and/or behavioural remedies to be invoked under EU competition law primarily depend on a 'market definition' that represents the first step. The relevant products market comprises all those products and/or services which are regarded as substitutable by the consumer by reason of the products' characteristics, prices and intended use.[420] The *relevant market* implies that "there can be effective competition between the products which form part of it",[421] revealing a dynamic concept in nature. Such dynamic features create a difficulty in demarcation of innovative i.e. ICT-based products, in a market.[422] Further to this dynamic nature, multi-sided markets e.g.

420 Commission Notice on the definition of relevant market for the purposes of Community competition law [1997] OJ C 372/03).

421 Case 85/76 *Hoffman- La Roche & Co AG v Commission* [1979] ECR 461, [1979] 3 CLR 211, para 28.

422 Particularly analysing 'competition in innovation' is acknowledged as a very difficult task, incorporating 'market definition', along with the requirement towards competition law enforcers to make predictions on future and often uncertain developments (See Josef Drexl, 'Anticompetitive Stumbling Stones on the Way to a Cleaner World: Protecting Competition in Innovation Without a Market' [2012] 8(3) Journal of Competition Law and Economics 507, 512).

online platforms similarly complicate the issue of market definition, which typically relies on one-sided approach based on a centralised product.[423]

The primary tool to define the markets is testing the price elasticities of the relevant products. If the cross-price elasticities denote a set of products that consumers are willing to have within the price limits that exclude other products, such products could be said to demonstrate a market within the meaning of competition law. This is and figured and shaped out mainly through the 'hypothetical monopoly test'. According to this test, the relevant products market includes all products to which consumers would most likely switch in response to a "small but significant and non-transitory increase in price" (SSNIP).[424] This test simply measures substitutability by asking whether a 'small but non-transitory increase in price' (usually 5-10%) of a one product will cause purchasers to purchase sufficient of another product instead to make the price increase unsustainable.[425] The Commission has thus far tended to favour demand-side tests partly because the exercise emphasizes products markets from the viewpoint of consumers and user preferences.[426] Therefore, supply-side substitutability, which means to evaluate capabilities of the undertakings to provide competing products, is of a subordinated role during the course of market definition.

---

423 These difficulties are also highlighted by a recent report prepared for the Commission (See Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition policy for the digital era* (2019) 44-46 <http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> accessed 9 October 2020.

424 The Hypothetical Monopoly Test is a standardised tool in antitrust analysis, according to which, the relevant market includes all products to which consumers would most likely switch in response to a "small but significant and non-transitory increase in price" (SSNIP). According to the US Horizontal Merger and Guidelines (US Department of Justice and Federal Trade Commission, 2010, para 4.1.1.), "…the test requires that a hypothetical profit-maximizing firm … that was the only present and future seller of those products ('hypothetical monopolist') likely would impose at least a 'small but significant and non-transitory' increase in price ('SSNIP')".

425 Alison Jones and Brenda Sufrin, *EU Competition Law: Text, Cases and Materials* (5th edn, OUP 2014) 63.

426 Steve Anderman and Hedvig Schmidt, *EU Competition Law and Intellectual Property Rights: The Regulation of Innovation* (2nd edn, OUP 2011) 39.

Not only the price elasticities of relevant products, but also consumers' inaction, particularly against the switching costs, might be a significant factor affecting their preferences. The Commission, in its 2002 Guidelines regarding market analysis in the electronic communications sector, points out this issue as follows:

> Consumers who have invested in technology or made any other necessary investments in order to receive a service, or use a product, may be unwilling to incur any additional costs involved in switching to an otherwise substitutable service or product (…) Accordingly, in a situation where end users face significant switching costs in order to substitute product A for product B, these two products should not be included in the same relevant market.[427]

From this point of view, 'lack of interoperability' between a dominant platform and complementary products e.g. apps and devices, might characterise the situation in the marketplace, so that the difficulty of switching across the platforms could be very determinant in market definition. A market power, usually a 'dominant position', could then be conferred onto the product in question, should the switching costs be dissuasive enough to deter end-users from opting for alternative products. This logic also represents the policy approach pursued by the Commission in many antitrust cases, including *Hugin*,[428] *Hilti*,[429] *Volvo*,[430] *Renault*[431] and *Tetra Pak II*.[432]

---

427 Commission guidelines on market analysis and the assessment of significant market power under the Community regulatory framework for electronic communications networks and services (2002/C 165/03) ('Commission's 2002 Guidelines'), para 50.

428 Case 22/78, *Hugin Kassaregister AB and Hugin Cash Registers Ltd v. EC Commission* [1979] ECR 1869.

429 Case C-53/92 P, *Hilti v. EC Commission* [1994] ECR I-667.

430 Case 238/87, *AB Volvo v. Erik Veng (UK) Ltd.* [1988] ECR 6211, [1989] 4 CMLR 122 ('*Volvo* judgement').

431 Case 53/87, *CICCRA v. Renault* [1988] ECR 6039 ('*Renault* judgement').

432 Case C-333/94 P, *Tetra Pak International SA v. EC Commission* [1996] ECR I-5951.

Lack of interoperability often comes up with the related IPRs upheld for the products that constitute the primary (upstream) market on which the secondary (downstream) competition relies. This much more reflects the *Hilti* case, whereby the Commission defined the relevant market for the cartridge strips to be used in Hilti nail guns. The main specific source of dominant position appears to have been the patent protection on these cartridge strips, which was Community-wide at the time.[433] By the same token, in *Volvo* and *Renault,* the relevant primary market was defined based on the products (car components) protected by IPRs. Arguably, this would not have been the case if the components, e.g. body panels protected by the design rights, were interoperable with those of competitors, although being IPR-protected.[434]

While the EU precedents do not mean that the IPRs under scrutiny are directly and automatically to be translated to market power (e.g. dominance),[435] there is an apparent risk that associated IPRs would cause definition of market(s) in a narrow fashion. Considering the Commission's decisional practice, this risk is remarkably high in the case where interoperability is absent between the competing products. On the other hand, if the primary market is competitive, an undertaking could hardly exploit its position over customers in a secondary market by raising prices.[436] That is to say, a correlation exists between definition of narrower markets and lack of interoperability, as being featured in IPR-protected dominant products.

---

433 Francis Fishwick, 'The Definition of the Relevant Market in the Competition Policy of the European Economic Community' [1993] 63 Revue D'économie Industrielle 174, 176.

434 Anderman and Schmidt (n 426) 46.

435 See Christopher R. Leslie, *Antitrust Law and Intellectual Property Rights: Cases and Materials* (OUP, 2011) 54, where it is established that the vast majority of academic literature recognizes that a patent does not confer market power. See also infra note 415.

436 Jones and Sufrin (n 425) 351.

5.2. Article 101 of the TFEU

5.2.1. General overview

Article 101 of the TFEU aims at determining whether any kind of collaboration between the undertakings is pro or anti-competitive. In this regard, Article 101(1) of the TFEU prohibits agreements and concerted practices between two or more undertakings "which may affect trade between Member States and which have as their object or effect, the prevention, restriction or distortion of competition within the internal market".[437] All vertical and horizontal agreements and concerted practices are encompassed by Article 101(1), which gives several non-exhaustive examples to illustrate anti-competitive collaborations. For Article 101(1) to be applied, there should be an 'appreciable' effect on interstate trade within the meaning of EU Competition Law.[438] Agreements or decisions that are found to have such effects are declared as "automatically void" as per the Article 101(2) of the TFEU.

As mentioned above, in an Article 101 case, it is sought to find out whether pro-competitive effects outweigh the restrictive (anti-competitive) effects. Article 101(3) is the legal means enlightening this comparative exercise. According to Article 101(3), Article 101(1) might not apply to acts of collaboration in the cases that they contribute to "improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit" and as long as such restrictions are "indispensable to the attainment of these objectives" and do not "eliminat[e] competition in respect of a substantial part of the products in

437 Consolidated Version of the TFEU [2012] OJ C 326/49 ('TFEU') art 101(1).
438 Anderman and Schmidt (n 426) 215.

question".[439] Following modernisation of the EU Competition Law tracing back to 1999, the EU Commission has issued Guidelines to clarify implementation of such conditions based on a more 'effects-based approach',[440] focusing on the concept of 'consumer welfare'.

Article 101 is invoked by the Commission to assess the horizontal and vertical agreements including licensing e.g. technology transfer agreements to ensure that they do not contain any clauses that would be anti-competitive by object or by effect. In this regard, restrictions agreed on by the parties are assessed by the Commission as to whether they would potentially exclude the rivals from the possible channels of competition e.g. distribution, sale, marketing. Whereas this assessment used to be done on a formalistic approach until the late 1990s, this approach was replaced by an effects-based approach in 1999 and 2004. A wide range of agreements potentially to be deemed as anti-competitive fall outside of Article 101(3) because of the more flexible and lenient rules adopted in time. The block exemptions[441] issued by the Commission, serving this effects-based approach, have a wide coverage as they exempt a great many vertical agreements potentially to be prohibited under Article 101(1). In particular, the block exemption applies so long as 30% market share threshold is met and the

439 TFEU, art 101(3).

440 Drawing from the influence of the Chicago School's antitrust analysis on US competition policy, the effects-based approach aims to avoid erroneous intervention against competitive and efficiency-increasing behaviour (avoiding type 1 errors or false positives) and to achieve an optimal level of enforcement of competition rules (Jones and Sufrin (n 425) 59).

441 Block exemptions operate as a safe harbour, exempting agreements even if they infringe Article 101 (Alison Jones and Brenda Sufrin, *EC Competition Law: Text, Cases and Materials* (4th edn, OUP 2011) 629), obviating individual assessment of the agreements that are covered by the block exemption regulations. Until May 2004, a notification system was in place, requiring individual notification of an agreement to the Commission, which was the only body with the power to grant an exemption under Article 101(3). However, since 1 May 2004 when Regulation 1/2003 came into force, the prohibition contained in Article 101(1) is automatically inapplicable *ab initio* to agreements and concerted practices that satisfy the conditions set out in Article 101(3), without the need for any decision to that effect (Joanna Goyder and Matthew O'Regan, 'Market Conduct' in L. Garzaniti and M. O'Regan (eds), *Telecommunications, Broadcasting and the Internet: EU Competition Law and Regulation* (3rd edn, Sweet & Maxwell 2010) 4).

agreement does not contain any hardcore restraints i.e. imposing price or territorial restraints.[442]

5.2.2. Standardisation agreements

In the context of horizontal agreements, standardisation agreements have a significant stake, representing an important playing field for the market actors and incorporating significant interplay between IPRs, openness and interoperability. In principle, a rather positive stance is adopted by the EU Competition Law towards standard-setting agreements. According to the Commission's Guidelines on the applicability of Article 101 of the TFEU to horizontal co-operation agreements, it is affirmed that standardisation agreements are usually pro-competitive as they tend to promote the internal market, encourage development of new and improved products or markets and ensure interoperability and compatibility to the benefit of consumers.[443] However, a partially cautious approach is reflected in the way standardisation takes place, particularly in view of the far-reaching implications on how competition and follow on innovation would be impacted by would-be standards. It is acknowledged that:

> Where participation in standard-setting is unrestricted and the procedure for adopting the standard in question is transparent, standardisation agreements which contain no obligation to comply with the standard and provide access to the standard on fair, reasonable and

442 Jones and Sufrin (n 441) 629.

443 European Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements (2011/C 11/01) ('Commission's 2011 Guidelines'), para 263.

non-discriminatory terms will normally not restrict competition within the meaning of Article 101(1).[444]

From the viewpoint of the Commission Guidelines it is possible to derive that SSOs might pose some risks because of; the followed procedures, the degree of openness and transparency and possible restrictions to participation. Likewise, standards might incorporate a number of IPRs,[445] which are naturally infringed until and unless rights holders accede not to claim as such. As a matter of fact, IPRs which represent the Achilles heel of the SSOs would affect not only the viability of would-be standards but also the interoperability of the potential products to be forged in the relevant market(s). Thus, interoperability is closely linked to and would be significantly affected by, the extent to which SSO processes are open and inclusive.

The problem arises that the natural monopoly created via standardisation on the technology for interoperability, may have IPRs associated with it, and these rights may be owned by one market player or a consortium.[446] In fact, interoperability related problems might arise should the IPRs embedded into a standard be hidden by the rights holder and kept outside of the SSO procedure - usually for extraction of larger royalty fees (the "hold-up" problem). Furthermore, rights holders can use their licensing policies to control further development of the standard, and to influence the market of products and services around the standardisation.[447] Such problems are closely related

444 Commission's 2011 Guidelines, para 280.

445 An analysis of the IPR databases of 11 of the most important SSOs by a group of scholars revealed that approximately 250 distinct standards include technologies that are covered by one or more declared IPR, and many of these standards are successful and widely employed (Pierre Larouche and Geertrui Van Overwalle, 'Interoperability standards, patents and competition policy', (2014) TILEC Discussion Paper DP 2014-050, December 2014, 6).

446 Ghosh (n 81) 77.

447 Ghosh (n 81) 77.

to the intellectual property incorporated into the standardisation processes, without access to which relevant standards could not be implemented.

Such IPRs that are essential to using the standards i.e. standard essential patents (SEPs),[448] are thus central to the standardisation process and could affect interoperability indirectly, but also significantly. Given the fact that exclusionary impact would come up with the closed standards, lack of interoperability would be an indirect result of the standardisation process. Having said that, lack of interoperability does not directly trigger enforcement of Article 101 by itself, yet this would happen through other factors such as limited openness and hampered innovation.

5.3. Article 102 of the TFEU

5.3.1. Abuse of dominant position: Main thrusts, types and conducts

Whereas Article 101 of the TFEU deals with the agreements and concerted practices, Article 102 of the TFEU focuses on the unilateral and joint abusive behaviours, the latter being encountered quite rarely. Article 102 aims to prevent dominant undertakings from driving out their competitors from the marketplace and/or using their market power to make consumers' conditions worse. Such conducts, which are deemed to have a commercially excessive nature and anti-competitive effect, are regarded as legally void insofar as that they meet the threshold of 'abuse of dominant position' under Article 102.[449] Abuse of dominant position, as contemplated by Article

[448] Once a patented technology has been selected and implemented in the standard, the use of the patent covering that technology becomes essential – a SEP (Urška Petrovčič, *Competition Law and Standard Essential Patents: A Transatlantic Perspective* (Kluwer Law International BV 2014) 29).

[449] Article 102 of the TFEU articulates the most common (non-exhaustive) examples of abuse of dominance. According to that article, "[s]uch abuse may, in particular, consist in:

102, encompasses both 'exclusionary' and 'exploitative' conducts. While the former category means conducts attempting to exclude competitors i.e. refusal to supply, discrimination, tying, the former covers misuse of market power to obtain extra gains from consumers i.e. unfair pricing and limiting supply to markets.[450] Article 102 of the TFEU exemplifies abusive behaviours by giving a non-exhaustive list of conducts.[451]

Article 102 covers exclusionary and exploitative type abusive conducts that are also based on the lack of interoperability. Stretching from de jure or de facto standards to non-standardised products, lack of interoperability could thus be the source of antitrust concerns that could warrant the application of Article 102. Broadly speaking, Article 102 is considered to be an important last resort to prevent the worst excesses of a lack of interoperability, but only available where there is dominance.[452] Practices of dominant undertakings, which aggravate the conditions of interoperability but also have not got a correcting response from either the market itself or coercive legal tools, could be challenged under Article 102 of the TFEU. However, interoperability is not an end goal of competition law tools itself; yet it could be considered as such where consumer harm emerges because of the dominant undertaking's practices.

This rule of thumb, first and foremost, is based on the presumption that ICT companies can freely decide on the degree to which their products and services would interoperate

(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;
(b) limiting production, markets or technical development to the prejudice of consumers;
(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts." (TFEU, art 102).

450 See Anderman and Schmidt (n 426) 34.

451 In this context, 'unfair pricing' and 'limiting supply to markets' are enshrined under Article 102(a) and Article 102(b) respectively, whereas 'discrimination' and 'tying' are put forth under Article 102(c) and Article 102(d).

452 Weston (n 13) 166.

with those of their rivals.[453] Secondly, there might be some points at which lack of interoperability is likely to have anti-competitive effect, because of the likelihood that competitors might be driven out of the market, along with actual or potential consumer harm e.g. increased prices, reduced innovation. Against such circumstances, Article 102 is the primary legal means to deter, and where necessary penalize, the so-called abusive behaviours. In ICT markets, signs of abuses would particularly come out with the gatekeeper positions created by network effects and/or de facto standards, which are typified by exclusionary behaviours targeting the foreclosure of competitors and incorporating 'refusal to supply', 'tying' and 'discrimination'.

In particular, 'refusal to supply' signifies so-called gatekeeper positions and foreclosure attempts based on hindering or restricting interoperability. For instance, in the case of a dominant product i.e. an operating system whose interfaces are kept closed after a long-lasting disclosure strategy, competitors might be seriously disadvantaged and/or face the risk of exiting the market. In such cases, risk of market foreclosure is usually followed by the consumers being locked into the dominant product. Given this fact, refusal to deal or supply, which also embodies discrimination to an extent, represents the most remarkable abusive conduct in relation to 'interoperability'. The focal point behind this proposition is that lack of interoperability mainly stems from restricted or withdrawn interfaces, also revealing an area of intersection between the exploitation of IPRs and antitrust interventions.[454]

---

453 See Wolfgang Kerber and Heike Schweitzer, 'Interoperability in the Digital Economy' [2011] 8(1) JIPITEC 39, 43.

454 'Tying' and 'exclusive dealing' pose comparable anti-competitive effects. However, through these acts foreclosure happens by means of the existing contracts and their exclusionary terms and conditions, rather than the absence of interoperability. Furthermore, these two acts do not have a direct relationship with the usage and boundaries of IPRs.

As far as exploitative abuses are concerned, the most remarkable scenario would be consumers being worse off in terms of quality and price indicators. In such a marketplace, consumers do suffer from the absence of competitive restraints, often resulting in excessive prices and/or deteriorated quality. In such cases, market failures are by and large depicted by more structural problems, mostly requiring ex-ante measures such as open access requirements and price regulation, i.e. cost oriented prices, in the first place. Given this fact, Article 102 of the TFEU has so far been, and is still, predominantly used against 'exclusionary' abuses.[455] From this point of view, 'refusal to supply' is examined in this thesis as representing the typical exclusionary conduct mirroring interoperability-based abuses.[456] In this context, firstly, 'refusal to supply' is elaborated under the light of EU precedents, comprising the most relevant case law i.e. 'essential facility' and 'refusal to license' cases. In so doing, 'refusal to supply interoperability information' is also dealt with as a subcategory of the 'refusal to license' cases under EU competition law.

5.3.1.1. Refusal to supply

5.3.1.1.1. Historical and jurisprudential background

'Refusal to supply' is an old antitrust problem, built on precedents from the early years of the US Sherman Act. Evolving from *U.S. v. Terminal Railroad Association*,[457] refusal cases were brought before the antitrust courts, drawing on an evolutionary jurisprudence echoing the 'essential facilities doctrine'.[458] Following a nearly century-

455 Jones and Sufrin (n 425) 371.
456 While in some other scholarly works (see Perzanowski (n 40) 152-154) are examined other abusive behaviours including 'tying', this is not found to be useful given the reasons in supra note 454.
457 *U.S. v. Terminal Railroad Association* 224 US 383 (1912).
458 Regarding the evolution and usage of the doctrine, particularly under EU law, see Unver (n 100).

long collection of case law ending up with the US Supreme Court's *Trinko*[459] judgement, remedying 'refusal to supply' by a monopolist firm was considered to be very exceptional. Since then, under US antitrust law, it is acknowledged this problem could be solved by antitrust mechanisms, provided that the specific problem has arisen from the withdrawal of a contract, namely when a dominant actor has decided to reverse away from dealing with its competitors.[460] On the other hand, 'refusal to supply' has greater repercussions under EU competition law, involving not only cessation of supplies but also denial of new offers.

Within the EU framework, Article 102 has been widely used to remedy dominant undertakings' refusals to deal with their competitors, unless this is justified by an objective reasoning. This abusive behaviour, involving wide-ranging relationships consisting of competitors, customers and distributors, has been affirmed to potentially affect competitive functioning of the markets, under EU jurisprudence. Marking a contrast to the US law, the 'essential facilities doctrine' was more clearly acknowledged by the EU Courts, as having evolved through the case law based on 'refusal to deal', which traces back to the *Commercial Solvents*[461] case in the 1970s.

In *Commercial Solvents*, which represents the leading 'refusal to supply' case under EU competition law, the condemned behaviour was a dominant company's refusal to

---

459 *Trinko* judgement (supra note 36) dismissing the application of the widely known essential facilities doctrine to already regulated industries, symbolizes a sharp end to the claims of mandatory access obligations under section 2 of the Sherman Act. In *Trinko*, the Supreme Court held that:

> One factor of particular importance is the existence of a regulatory structure designed to deter and remedy competition harm. Where such a structure exists, the additional benefits to competition provided by antitrust enforcement will tend to be small and it will be less plausible that the antitrust laws contemplate such additional scrutiny (*Trinko* judgement, para 412).

460 See *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 US 585 (1985).

461 Joined Cases 6, 7/73, *Commercial Solvents v. Commission* [1974] ECR 223 ('*Commercial Solvents* judgement').

supply the raw material of amino-butanol, used for manufacturing ethambutol, which is an anti-tuberculosis drug. Commercial Solvents, a dominant company in the (upstream) market for amino-butanol, after having cut its supplies to its competitor Zoja, was found to have abused their dominant position, particularly as this happened following its subsidiary ICI starting to manufacture ethambutol. The CoJ's judgement was based on the finding that:

> An undertaking which has a dominant position in the market in raw materials and which, with the object of reserving such raw material for manufacturing its own derivatives, refuses to supply a customer, which is itself a manufacturer of these derivatives, and therefore risks eliminating all competition on the part of customer, is abusing its dominant position within the meaning of Article 86 [ex-102].[462]

Commercial Solvents was followed by further judgments with similar revelations in different contexts. In *United Brands*,[463] a dominant company's (United Brands) cutting off the deliveries of Chiquita branded bananas to its customer, Olesen, subsequent to its decision to promote and advertise a rival brand, was found as abusive under Article 102.[464] By the same token, in *Telemarketing*, the General Court (GC) condemned a dominant TV broadcaster's tying up would-be telemarketing advertisements to the condition that its subsidiary was to be the contractor to answer the calls coming from

---

462 Ibid, para 25.

463 Case 27/76, *United Brands v. Commission*, [1978] ECR 207 ('*United Brands* judgement').

464 The CoJ reached the following conclusion in finding an 'abuse of dominance':

> In view of these conflicting arguments it is advisable to assert positively from the outset that an undertaking in a dominant position for the purpose of marketing a product ... cannot stop supplying *a long standing customer* who abides by regular commercial practice, if the orders placed by that customer are in no way out of the ordinary (*United Brands* judgement, para 182).

the viewers. Considering this as a "refusal to supply the services of that [TV] station to any other telemarketing undertaking", the European Court upheld the following:

> If, further, that refusal is not justified by technical or commercial requirements relating to the nature of the television, but is intended to reserve to the agent any telemarketing operation broadcast by the said station, with the possibility of eliminating all competition from another undertaking, such conduct amounts to an abuse prohibited by Article 86 [now 102], provided that the other conditions of that article are satisfied.[465]

As seen above, 'refusal to deal' was found to be abusive based on some behavioural elements seen in many EU precedents. In this regard, 'termination of contract while entering into the downstream market' (*Commercial Solvents*), 'refusal to provide services to the customers who decide not to cooperate any more' (*United Brands*) and 'reserving an ancillary market by tying up purchases to buying an ancillary product' (*Telemarketing*) come to the fore in the antitrust liability arising from a dominant firm's refusal to deal. Additionally, it is noticeable that the European Courts ruling on antitrust liability sought that 'elimination of *all* competition' be risked following such a behaviour. Such case law infused the subsequent litigations based on 'refusal to deal' with wider implications, which are detailed below.

5.3.1.1.2. Essential facilities doctrine and related cases

While the mainstream 'refusal to deal' cases could be matched with common features that depend on 'behavioural' elements, another stream of cases emerge alongside these cases

[465] Case 311/84, *Cenbtre belge d'études du marché*, [1985] ECR 3261 ('*Telemarketing* judgement').

with more 'structural' aspects. The notion of 'essential facilities' and the need to open up such facilities to competition portrayed these cases, which have been mostly resolved by the Commission in the early 1990s, during the years when liberalisation figured on the EU agenda. In this emerging part of case law, Article 102 has been construed as containing an obligation for dominant undertakings to share access where a facility under their control is necessary for the exercise of activities in an adjacent market.[466]

Signifying this approach, the *London European/Sabena*[467] and *British Midland/Aer Lingus*[468] decisions came up, laying down the milestones for a competition law 'duty to deal' by dominant companies. The former case originates from a dominant undertaking's refusal to allow access to its computerised reservation system by another undertaking, which the Commission found abusive for it "could have resulted in London European [applicant] abandoning its plan to open a route between Brussels and Luton". In the latter, the Commission found a dominant undertaking's (Aer Lingus) refusal to interline[469] with another undertaking (British Midland) on a certain route as an infringement of Article 102. In this latter case, as a matter of fact, Aer Lingus's strategy had not resulted in British Midland's departure from the route, and it is difficult to see that the interlining could be classified as an 'indispensable' input, or an 'essential facility'.[470] Moreover, it was not clear in both cases that the denial of access towards the new entrants threatened their survival as opposed to merely creating a competitive disadvantage.[471]

---

466 Paul Nihoul and Peter Rodford, *EU Electronic Communications Law: Competition and Regulation in the European Telecommunications Market* (OUP 2004) 470.

467 Decision 88/589 of 4 November 1988, *London European/Sabena* [1988] OJ L 317/47.

468 Decision 92/213 of 26 February 1992, *British Midland/Aer Lingus* [1992] OJ L 96/34.

469 'Interlining' is a standard facility based on an international (IATA) agreement pursuant to which airline companies authorise each other, as well as travel agents, to offer their services via a single ticket.

470 Jones and Sufrin (n 441) 487.

471 Steven D. Anderman, *EC Competition Law and Intellectual Property Rights: The Regulation of Innovation* (Clarendon Press 1998) 201.

Subsequently, two interim Commission decisions; *Sealink Harbours Ltd/B&I Line plc*[472]and *Sea Containers/Stena Sealink,*[473] could be said to have developed along the same lines. In these cases, which originated from the complaints of ferry operators who were not allowed, or allowed under onerous conditions, to use the port, the Commission found the dominant port owners liable for their actions, and concluded as follows:

> An undertaking which occupies a dominant position in the provision of an *essential facility* and itself uses that facility (i.e., a facility or infrastructure, without access to which competitors cannot provide services to their customers), and which refuses other companies access to that facility *without objective justification* or grants access to competitors only *on terms less favourable than those which it gives its own services*, infringes Article 86 [ex-102] if the other conditions of that Article are met.[474]

One of the most peculiar characteristics of these harbour cases is the implicit 'special responsibility' resulting merely from controlling bottleneck-type facilities, which are by and large attributed to a 'duty to deal', without any behavioural considerations.[475] Behavioural elements, framing the 'refusal to deal' cases i.e. *Commercial Solvents,*[476] are far less emphasized in this continuum of case law. In contrast to the previous case law, risks over 'elimination of all competition' do not constitute a subject matter of the analysis conducted. While a number of related cases were handled by the European

---

472 Case IV/34.174, *B&I Line plc/Sealink Harbours Ltd.* [1992] 5 CMLR 255.

473 Case IV/34.689, *Sea Containers/Stena Sealink* [1994] OJ L 15/8.

474 Ibid, para 66.

475 See Pierre Larouche, *Competition Law and Regulation in European Telecommunications* (Hart Publishing, 2000) 204-211. See also Richard Whish, Competition Law (5th edn, Butterworths 2003), 670, reading; "[U]ndertakings controlling a bottleneck might be considered to be 'super-dominant', implying that they have a higher responsibility than the obligations attaching to 'merely' dominant firms".

476 Joined Cases 6,7/73, *Commercial Solvents v. Commission* [1974] ECR 223 ('*Commercial Solvents* judgement').

Courts in the 1990s, i.e. *Magill*[477]*, Tiercé Ladbroke*,[478] *Oscar Bronner*[479]*,* the latter is widely acknowledged as the most remarkable EU case for drawing the scope and constraining the limits of the essential facilities doctrine, particularly for the tangible (physical) assets.

Oscar Bronner originated from an attempt by a publisher of an Austrian daily newspaper, Oscar Bronner, to get access to the only existing nationwide delivery scheme which was run by another publisher, Mediaprint, who held dominance in the Austrian daily newspaper market. Having faced a refusal from Mediaprint, Oscar Bronner took legal action before the Austrian Court, which then applied to the CoJ with a preliminary question. The CoJ focused on the economic viability of access seeker(s) in the relevant market, and concluded that the following cumulative conditions need to be met for a refusal to grant access to an allegedly essential facility to be unlawful:[480]

1) The refusal must be *likely to eliminate all competition* in the relevant market on the requesting party,

2) The refusal must be incapable of being *objectively justified*,

3) The facility in question must be *indispensable* in order for the business of the requesting person to be carried on (inasmuch as there is *"no actual or potential substitute in existence"*).

---

477 See *supra* note 227.

478 Case T-504/93, *Tiercé Ladbroke SA v. Commission* [1997] ECR II-923, [1997] ECR II-923, [1997] 5 CMLR 309 ('*Tiercé Ladbroke* judgement').

479 Case C-7/97, *Oscar Bronner GmBH & Co KG and Others v. Mediaprint Zeitungs-und Zeischiftverlag GmbH & Co KG and Others* [1998] ECR I-7791, [1999] 4 CMLR 112 ('*Oscar Bronner* judgement').

480 Ibid, para 41.

According to the *Oscar Bronner* case, a primary source, i.e. critical physical infrastructure, which is economically non-substitutable, is sought for a mandatory sharing, signifying a much higher ('natural monopoly' type) *indispensability* threshold. In fact, there arises an economics-based formulation of the 'essential facilities doctrine' comparable to the 'natural monopoly' theory. Although considerable as a context-specific ruling, *Oscar Bronner* is noteworthy for drawing up the jurisprudential lines, not only for 'essential facilities' type cases, but also, much more broadly speaking, 'refusal to deal' cases. On its own facts, i.e. based on a privately owned physical infrastructure, *Oscar Bronner* appears as a perfectly justifiable decision, revealing a salutary reminder that the redress for refusals to supply under Article 102 is limited to those affecting the 'process of competition', not individual competitors.[481]

5.3.1.2. Refusal to licence

'Refusal to license' by a dominant undertaking represents an exclusionary abuse having unique features as well as building on the course of the 'refusal to deal' cases. Under EU competition law, 'refusal to license' ignites a more comprehensive scrutiny, when compared with conventional 'refusal to deal' cases. This stems from the very nature of the IPRs, which ban non-authorized use of the protected subject matter, which often consists of original (intellectual) creations or inventions based on some qualitative and/or quantitative work. Notably, a dominant undertaking holding an IPR, which is normally of an exclusionary nature, can not be considered as an abusive practice itself, as acknowledged by the CoJ.[482] CoJ jurisprudence, while prepared to allow that even

[481] Eagles and Longdin (n 266) 169.

[482] In the *IMS Health* judgment, the CoJ held:

> According to settled case-law, the exclusive right of reproduction forms part of the owner's rights, so that the refusal to grant a licence, even if it is the act of an undertaking holding a dominant position, cannot in itself constitute an abuse of a dominant position (*IMS Health* judgment, para 34).

dominant intellectual property owning firms should be free to choose their licensees, also concedes that 'exceptional circumstances' might nevertheless exist in which a refusal to license IPRs might constitute an abuse of dominant position.[483]

Magill, a landmark judgement on 'refusal to license', for the first time set out the so-called 'exceptional circumstances' that warrant sharing of dominant IPR-protected products. In the *Magill* case, three European television companies (RTE, BBC, and ITP) refused to disclose their weekly programme listings which a publisher (Magill) needed in order to create a weekly guide compiling all the programme listings at the time. Refusal to disclose such information was justified by the three television companies on the basis that their programme listings had been protected with copyright according to UK and Irish laws. The Commission held that the television companies abused their dominant position on the (downstream) market for weekly television magazines and regarded the non-disclosure as a prohibited conduct under Article 102 since they hindered the creation of a *new product,* as well as retaining the downstream market to themselves. On appeal, both the GC and CoJ rejected the arguments related to copyright protection, upholding the Commission's decision.

The CoJ specified three reasons, naming them as the "exceptional circumstances" which render the television companies' refusal to license unlawful. First, the television companies' refusal prevented the *appearance of a new product*, a comprehensive weekly guide to television programs for which there was a potential consumer demand. Second, there was *no objective justification* for their refusal. Third, "the appellants, by

---

For similar findings under US antitrust law, see Leslie's (n 435) 167-176, reading;

> While exclusionary conduct can include a monopolist's unilateral refusal to license a copyright, an author's desire to exclude others from use of their copyrighted work is a presumptively valid business justification for any immediate harm to consumers (Leslie (n 435) 175). As well, this fact is upheld both in the *Magill* and *Volvo* judgments (*Magill* judgment, para 49; *Volvo* judgment, para 8).

483 Eagles and Longdin (n 266) 161.

their conduct, reserved to themselves the secondary market of the weekly television guides by *excluding all competition* in that market [with reference to *Commercial Solvents*], since they denied access to the basic information which is the raw material *indispensable* for the compilation of such a guide.[484]

The *Magill* judgement clearly builds on the previous case law regarding 'refusal to deal', such as in *Commercial Solvents*, incorporating the key elements such as 'objective justification', 'elimination of all competition' and 'indispensability',[485] which reflect the baseline of 'exceptional circumstances' that is also applicable to IPR-protected dominant products. Further to these elements, the *Magill* judgement created the 'new product' test, a new element, to investigate 'refusal to license' cases within the context of 'exceptional circumstances'. That is to say, the 'refusal to license' analysis has been taken up a notch by the CoJ, which went beyond the 'refusal to deal' analysis.

The *Magill* judgment has had its repercussions in the subsequent Court decisions, including in *Tierce Ladbroke*[486] and *IMS Health*, where *Magill* criteria were elaborated and reinforced. Particularly, *IMS Health* represents a landmark judgement, whereby the 'exceptional circumstances' test was revisited and demystified. In *IMS Health*, the conflict between the parties began after a new entrant PII, afterwards acquired by NDC, initiated to use a copyrighted database concerning pharmaceutical sales in Germany[487] for its market sales' services. During the judicial proceedings before the

---

484 Magill *judgement*, paras 54-56. It is argued that by approving the holding of the GC on this point, the CoJ has effectively endorsed the basis of the 'essential facilities' doctrine promoted by the Commission, albeit under certain conditions (Anderman and Schmidt (n 426) 209).

485 The last reason in the *Magill* ruling not only underlines 'elimination of all competition' in the downstream market but also points out that in order for a 'refusal to license' to be considered abusive, the IPR-protected facility to which access was denied should be an 'indispensable' input for carrying out an activity in the downstream market.

486 *Tiercé Ladbroke* judgement, para 309.

487 Such a database was called an 1860 'brick structure' containing information gathered from pharmacies located in 1860 different geographical areas all over Germany.

national German court, a preliminary question as to whether the claimant's (IMS) refusal to license could amount to an abuse was referred to the CoJ. Meanwhile, NDC applied to the Commission with the allegation that IMS breached Article 102. Despite the Commission's finding as to the existence of 'exceptional circumstances' by mentioning that the so-called copyrighted database has been a *de facto* industrial standard,[488] the GC suspended the Commission's interim decision.[489]

Rendering a preliminary ruling under Article 267 (formerly Article 234) of the TFEU, the CoJ stated that the 'exceptional circumstances' of *Magill* were to be applied *cumulatively*. According to the CoJ, in order for a dominant firm's refusal to licence a competitor who is carrying out a business dependent on the former's *indispensable* IPR to be an abuse, all the following three conditions have to be fulfilled:[490]

1. the undertaking which requests the licence intends to offer, on the market for the supply of data in question, *new products or services not offered by the copyright owner and for which there is potential consumer demand*;

2. the refusal is *not justified by objective considerations*;

3. the refusal is such as to reserve to the copyright owner the market for the supply of data on sales of pharmaceutical products in the Member State concerned by *eliminating all competition on that market*.

---

488 In finding abuse, the Commission interpreted the 'exceptional circumstances' of *Magill* as *alternative* (not cumulative) sets of conditions (Commission Decision 2002/165/EC, 2002 O.J. (L 59) 18 relating to a proceeding pursuant to Article 82 of the EC Treaty (Case COMP D3/38.044-NDC Health/IMS: Interim Measure, para 180)).

489 Case C-184/01 R, *IMS Health* v. *Commission* [2001] ECR II-3193, [2002] 4 CMLR 58 (26 October 2001). On appeal, the CoJ upheld the suspension of the GC (See Case C-481/01 P(R), *IMS Health* v. *Commission* [2002] ECR I-3401, [2002] 5 CMLR 44) (11 April 2002).

490 *IMS Health* judgement, para 52.

The EU Court seems to have carefully crafted the 'exceptional circumstances' within the specific context of the *IMS Health* case. First of all, 'exceptional circumstances' originating from *Magill* with regard to mandatory licensing were acknowledged to be applied 'cumulatively', not on an alternative basis. It was thereby affirmed that the 'new product test' needs to be applied as an inseparable component of the so-called *Magill*-origin test. Secondly, well-established cumulative conditions of *Magill* were construed to be not exhaustive, but 'sufficient' for a mandatory licensing under Article 102.[491] That proposition seems to follow the purpose of Article 102(b), which is to prohibit abusive conducts by dominant firms where such conduct limits *technical development of markets* to the detriment of consumers.[492] Last but not least, the Court has taken a wider perspective entailing horizontal competition along with no necessity of two market structures,[493] which typically characterises the refusal to deal cases. Within the light of the Court's interpretation, *IMS Health* could be said to have broadened the legal playing ground of the 'exceptional circumstances' test.

5.3.1.3. Refusal to license/supply interoperability information

Interoperability based antitrust problems are often visible with the exclusionary conducts of dominant undertakings, as typified with refusal to deal or license. While 'interoperability' would be the subject matter of a great many conflicts between rivals e.g. quality degradation and security, the antitrust lens to be taken under Article 102 would mainly look to the likelihood of market foreclosure and consumer harm. In the absence of any likelihood regarding exclusion of competitors and consumer harm, e.g.

---

491 *IMS Health* judgement, para 38.

492 Steve D. Anderman and John Kallaugher, *Techonology Transfer and The New EU Competition Rules - Intellectual Property Licensing after Modernisation* (OUP 2006) 286.

493 Notably, the CoJ establishes that, "… for the purposes of the application of the earlier case-law, it is sufficient that a potential market, or even hypothetical market, can be identified" (*IMS Health* judgement, para 44).

risk of heightened switching cost, non-disclosure of interoperability information would not be considered as a competition law problem by itself. EU competition law and precedents, on this basis, reveal a case law concerning antitrust treatment from the refusal to disclose interoperability information.

The first antitrust investigation took place in the *IBM*[494] case, which was related to IBM's "failing to supply other manufacturers in sufficient time with the technical information needed to permit competitive products to be used with System/370 (interface information)".[495]As this would deprive competing manufacturers of the related software and their updates, leading to potential competition problems, the Commission sent its statement to IBM, seeking a solution based on the disclosure of interfaces. After several rounds of negotiations, IBM committed to disclose the interface information under "reasonable and non-discriminatory" (RAND) charges to ensure the competing manufacturers would attach their hardware and software designs to IBM System/370 during a 5-year period. The case was resolved following IBM's commitment being accepted by the Commission as to be enforced by 1 August 1984 until the end of 1989. Throughout the process, the Commission aimed not only to ensure that "non-IBM suppliers would be able to remain System/370-compatible into the foreseeable future", but also not to "have a negative effect on IBM's interests in

494 Case No IV/29.479 – IBM [1984].

495 The Commission alleged that IBM held a dominant position in the Member States at that time for the supply of the key products for its most powerful range of computers, the IBM System/370, and had abused that position contrary to Article 86 (ex-102), which in addition to the refusal to supply interface information, consisted of the following:

(i) not offering System/370 central processing units ("CPUs") without a capacity for main memory included in the price ("memory bundling")

(ii) not offering System/370 CPUs without the basic software included in the price ("software bundling"), and

(iii) discriminating between users of IBM software in refusing to supply certain software installation services ("Installation Productivity Options" = IPOs) to users of non-IBM CPUs. (See EC Competition Policy Newsletter, 1998, No. 3, <http://ec.europa.eu./competition/publications/cpn/cpn19983.pdf> accessed 9 October 2020).

developing new products".[496] Later on, the settlement, or undertaking, as agreed by the Commission, was earmarked to have had positive effects as follows:

> The U/T [undertaking] therefore not only stimulated competition in that it removed a major obstacle for IBM's competitors to offer innovative System/370 products at an earlier moment in time than they could have done in the absence of the U/T, if at all, but also because of this reinforced competition it put pressure on IBM to innovate and improve upon its own products.[497]

In the subsequent period, interoperability again figured on the agenda of EU competition law with the *Microsoft* case, which relates to both 'refusal to supply' and 'tying' practices of Microsoft.[498] The case originated in December 1998 from Sun Microsystems's (now 'Oracle') allegations based on Microsoft's abuse of its dominant position. Sun, in their application, claimed that Microsoft had been leveraging its dominant position in the client PC OS market to work in the group server OS market, by refusing to supply the interface information (that serves interoperability between Windows PC OS and non-Microsoft work group servers) to them. The Commission opened up two investigations and sent three statements of objection, and at the end of a nearly 5-year scrutiny period, found a breach of Article 102 in April 2004, and ordered Microsoft to disclose the access-cut (withdrawn) interface information and with a fine of 479 million Euros. On appeal, the GC upheld the Commission's decision along the same line of reasoning, arriving at the conclusion that Microsoft abused its

496 Ibid.
497 Ibid.
498 While both Microsoft's refusal to supply interoperability information and tying the purchase of Windows OS with that of Windows Media Player was at issue, this thesis focuses on the former practice within the meaning of Article 102.

dominant position by not disclosing its interfaces that would enable competitors to have interoperability with Windows OS architecture.[499]

The Commission's legal and economic assessment mostly depends on the indirect network effects,[500] which were presumed to pose a 'structural' entry barrier.[501] According to the Commission, such barriers to entry, when combined with Microsoft's refusal to *continue to* supply, namely withdrawal of interoperability information,[502] resulted in an abuse of dominance.[503] This behaviour of Microsoft, in the Commission's view, was found to be detrimental to the consumers, who would otherwise benefit from innovative products to be introduced by competing vendors.[504] In the *Microsoft* case, which marks a stark distinction from previous case law, an imminent risk of exclusion of competitor(s) and directly attributable consumer harm were not sought to reach to an antitrust liability.[505] Relying on and giving an emphasis

---

499 See supra note 15.

500 While the direct network effects relate to the number of Windows based PC users and the value attributed to the network itself, the indirect network effects relate to the indirectly generated benefits via using the Windows OS, e.g. increase of software developers to write applications for the Microsoft Windows OS. The Commission explains the importance of the latter as follows:

> In essence, the dynamic between the Windows client PC operating system and the large body of applications that are written to it are *self-reinforcing*. In other words, applications developers have a *compelling economic incentive* to continue writing applications for the dominant client PC operating system platform (that is to say, Windows) because they know that the potential market will be larger (Commission's *Microsoft* decision, para 458).

501 McMahon describes the Commission's approach as a *structural* one, underlining accompanying unpredictable consequences. She enunciates her view as follows:

> While structure can clearly affect outcomes, a focus on this issue alone without a closer examination of the impact of conduct on consumer welfare (and efficiency) is problematic in network environments and in competition law more generally (McMahon (n 16) 143).

502 See the Commission's *Microsoft* decision, para 524.

503 See the Commission's *Microsoft* decision, para 546.

504 More explicitly, Microsoft's denial of access to the interface information was characterised as '*limit[ing] the prospect for such competitors to successfully market their innovation and […] discouraging them from developing new products* and therefore *limit[ing] technical development to the prejudice of consumers*'. In fact, the Commission's analytical approach that radiates with establishing eliminatory risks on competitive structures and focuses on their indirect effects regarding future innovations, is linked to *limiting technical development to the prejudice of consumers* (within the meaning of Article 102(b) of the TFEU).

505 This point of view is divulged by the Commission as follows:

> Furthermore, it is established in case law that Article 82 of the Treaty covers not only abuse which may directly prejudice consumers but also abuse which *indirectly*

to the wording of Article 102(b), the Commission was satisfied with the foreseeability of possible harms towards follow-on innovation rather than the hindrance of new product(s) in the particular case.[506]

The Commission, not strictly confining itself to the already set rules of case law[507], underscored the need to "analyse *the entirety of the circumstances* surrounding a specific instance of a refusal to supply".[508] Having particular concerns about the potential risk of 'market tipping' in the downstream (work group OS) market, the Commission seems to have developed a distinct 'theory of harm', getting away from the four-partite 'exceptional circumstances' test. The Commission's deviation from the previous case law is however worth being criticised for the social and legal costs to be attached to it.[509]

From a broader point of view, the *Microsoft* formula could be considered to reveal an uneven interoperability policy design towards strategically optimised competition law

---

> prejudices them by impairing the effective competitive structure as envisaged by Article 3 (f) of the Treaty (Commission's *Microsoft* decision, para 704).

Also see the GC's *Microsoft* judgment, para 643.

506 This approach is more visible in the abandonment of the 'new product test', if not fully, but within the context of *Microsoft*. According to the Commission;

> A detailed examination of the scope of the disclosure at stake leads to the conclusion that, on balance, *the possible negative impact of an order to supply on Microsoft's incentives to innovate is outweighed by its positive impact on the level of innovation of the whole industry (including Microsoft)*. As such, the need to protect Microsoft's incentives to innovate cannot constitute an *objective justification* so as to offset the exceptional circumstances identified (Commission's *Microsoft* decision, para 783).

507 The Commission's view on to what extent the established rules of case law must be taken into account in the decision making process could be seen in its following prescription:

> On a general note, there is no persuasiveness to an approach that would advocate the existence of an exhaustive checklist of *exceptional circumstances* and would have the Commission disregard a *limine* and other circumstances of exceptional character that may deserve to be taken into account when assessing a refusal to supply (Commission's *Microsoft* decision, para 555).

508 Commission's *Microsoft* decision, para 558. See also the GC's *Microsoft* judgment, paras 312-336.

509 For similar views see Christian Ahlborn, David S. Evans and A. Jorge Padilla, 'The Logic & Limits of the "Exceptional Circumstances Test" in Magill and IMS Health' [2005] 28 Fordham International Law Journal 1009, 1110.

goals. The optimised character of the interoperability solution of *Microsoft* is rationalised by the absence of substitutable tools to ensure interoperability. The Commission, in its comparative analysis refers to three categories of technical tools; the use of open industry standards supported in Windows; the distribution of client-side software on the client PC; and the reverse engineering of Microsoft's products, and concludes that none of them is a viable solution for the companies willing to compete with Microsoft on the work group server OS market.[510] The GC's analysis draws a similar and comparably clearer framework regarding Windows work group server OS interfaces. The Court considers 'indispensability' as a phenomenon having varying degrees and that the ideal level of interoperability is the one by which a server running a non-Microsoft work group server OS is able to act as a domain controller within a Windows domain using Active Directory and is capable of participating in the multimaster replication mechanism with the other domain controllers.[511] Across this picture, it is fair to say that although the instruments invoked by the Commission originate from and subsist within the EU competition law, the idealised market structure and theory of harm behind this finding suggest a semi-regulatory policy for software interoperability.

5.3.2. Commission Guidance on Article 102: Filtered criteria and effects-based approach

The Commission initiated a soft law making process to demarcate the lines concerning the exclusionary abuses under Article 102 and ended up with the issuance of 'Guidance on the Commission's Enforcement Priorities in Applying Article 102 of the EC Treaty

510 See the Commission's *Microsoft* decision, paras 667-691.
511 GC's *Microsoft* judgment, para 390.

to Abusive Exclusionary Conduct by Dominant Undertakings'[512] i.e. 'Commission Guidance', in 2009. Reflecting the mainstream dynamic in the modernisation of EU competition law, the effects-based approach finds its expression regarding exclusionary type abusive behaviours within the 'Commission Guidance'. The leading aim for adoption of this Guidance could be described as filtering the previous case law through a lens of an economics-based approach, rather than a formalistic approach based on the ordoliberal principles which were predominantly pursued throughout the decades since the first adoption of TEEC competition rules. Having said that, of more significance than the attempt in the Guidance to incorporate the prior case law into its methodology, is its emphasis on the integration of more econometric analysis into abuse cases, including refusals, through the adoption of an 'effects-based approach', an approach the Commission supposes to be more in tune with that of the United States and considered less prone to 'type' errors.[513]

As a result of the effects-based approach being taken, 'consumer welfare' is conferred a more crucial role under the Guidance. Consumers are put at the centre, as it is affirmed that they need to be protected from the adverse effects stemming from a dominant undertakings' exclusionary behaviours. Not in all cases of exclusion, but when a competitor who is as *equally efficient* as a dominant undertakings is excluded, a potential grounds for intervention will be relevant following the enforcement

---

512 Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, C(2009) 864 final, OJ C 45 ('Commission Guidance').

513 Eagles and Longdin (n 266) 177-178. There are two types of errors, false positives or negatives, mainly characterised by form-based approaches. Type 1 errors (false positive) and type 2 (false negative), representing over and early, or pre-mature, enforcement. Either situation (type errors) has potential to give way to social harms. While there might be instances of type 2 errors, where competition law fails to intervene despite the fact that consumer harm is very likely or has happened, the likeliness and would-be harms of type 1 errors are found more critical in general (See Peter Alexiadis, 'Forging a European Competition Policy Response to Online Platforms' [2017] 18(2) Business Law International 91, 94).

priorities enshrined under the Guidance.[514] Furthermore, the Guidance acknowledges that 'efficiencies' would be put forth so as to justify the exclusionary behaviour and their constraints on competition, insofar as overweighing benefits are established to pass on to the consumers with no or minimised harm to competition. In this context, the dominant undertakings are required to demonstrate, with a sufficient degree of probability and on the basis of verifiable evidence, that the following cumulative conditions are fulfilled:

- the efficiencies have been, or are likely to be, realised as a result of the conduct.
- the conduct is indispensable to the realisation of those efficiencies.
- the likely efficiencies brought about by the conduct outweigh any likely negative effects on competition and consumer welfare in the affected markets.
- the conduct does not eliminate effective competition, by removing all or most existing sources of actual or potential competition.[515]

Despite the acknowledgement of an efficiency defence, a pro-competitive stance built on the ordoliberal roots could still be inferred from the Commission's Guidance. In this regard, the idea of the 'protection of competitors' is discernibly injected into the Commission's effects-based approach that targets both 'protection of competition' and 'consumer welfare'.[516] Particularly in the context of non-price based exclusionary

---

514 See the Commission Guidance, para 23, reading as follows:

> With a view to preventing anticompetitive foreclosure, the Commission will normally only intervene where the conduct concerned has already been, or is capable of, hampering competition from competitors which are considered to be as efficient as the dominant undertaking.

515 Commission Guidance, para 30.

516 The paragraph below of the Guidance illustrates to what degree the Commission will take into account efficiency-based arguments, while considering the exclusionary conducts towards inefficient, or less efficient, competitors:

> However, the Commission recognises that in certain circumstances a less efficient competitor may also exert a constraint which should be taken into account when

conducts, the given ambiguity is much more visible, and is also reflected in the context of 'refusal to supply' behaviours.

According to the Guidance, if a dominant undertaking has refused to supply or license to his competitors, this is considered as a significant reason to presume an existent 'consumer harm' under certain circumstances.[517] Should the so-called circumstances be proven to have existed, the dominant undertakings could be held liable for effective competition being eliminated owing to their refusal to deal with their downstream competitors regardless of the negative effects to the consumers.[518] To cover all the relevant scenarios, the Guidance seems to have filtered the exceptional circumstances under which refusal to deal is to be regarded as an 'abuse of dominance'. According to this consolidated formula, for a dominant undertaking's refusal to supply to amount to an abuse the following conditions need to be met cumulatively:[519]

1. the refusal relates to a product or service that is *objectively necessary to be able to compete effectively* on a downstream market;

2. the refusal is *likely to lead to the elimination of effective competition* on the downstream market; and

3. the refusal is *likely to lead to consumer harm*.

considering whether particular price-based conduct leads to anticompetitive foreclosure (Commission Guidance, para 24).

It is argued that the Commission Guidance seeks to blur this distinction between efficient and inefficient competitors by suggesting that the assessment of inefficiency is a dynamic concept, and that a rival firm that appears inefficient today might expect to become as efficient as its dominant rival over time (Derek Ridyard, 'The Commission's Article 82 Guidelines: some reflections on the economic issues' [2009] 30(5) European Competition Law Review 230, 232).

517 Commission Guidance, paras 87-88.

518 Commission Guidance, para 85.

519 See the Commission Guidance, para 81.

Under this comprehensive and generic formula, a divergence from the original strand of 'exceptional circumstances' must be noted whereby the conditions have a less sharpened and more simplified character. In addition, after a careful reading, it could be found that this tripartite test has remarkable traces leading out from the stand-alone formulation of *Microsoft*. For instance, for a finding of an abusive refusal to supply, 'indispensability' is no longer required to be a featured aspect of the access denied asset.[520] Instead, 'objectively necessary' is created as a comparably less bold requirement, reminiscent of *Microsoft*, where there was no reference to 'indispensability' as opposed to previous case law i.e. *Magill, IMS health* or *Oscar Bronner*. Likewise, 'elimination of effective competition'[521] seems to be opted for instead of 'elimination of all competition' as the pre-requisite, demonstrating a loosening of grounds for finding an abuse, just like in the *Microsoft* formula. Along the same lines, 'consumer harm' is presupposed to arise "where the competitors that the dominant undertaking forecloses are, as a result of the refusal, prevented from bringing innovative goods or services to market and/or where follow-on innovation is likely to be stifled".[522] This point of view draws on the *Microsoft* judgement, where the main focus was on the 'follow-on innovation' rather than the 'new product test', and the burden of proof was imposed onto the dominant firm for proving that mandatory sharing harmed its innovation incentives.[523] It seems that the Guidance, without deeply questioning, seems to acknowledge this presumptive approach as the

---

520 Commission Guidance, para 83.
521 Commission Guidance, para 85.
522 Commission Guidance, para 87.
523 GC's *Microsoft* judgement, paras 696-7, reading as follows:

> The Court finds that, as the Commission correctly submits, Microsoft, which bore the initial burden of proof, did not sufficiently establish that if it were required to disclose the interoperability information that this would have a significant negative impact on its incentives to innovate.

baseline for efficiency claims,[524] whilst also bearing some risks of having a unilateral and formalistic approach.

From an overall perspective and reading of the Guidance, a looser characterisation of the 'exceptional circumstances' to warrant mandatory sharing and interoperability suggests more discretion being left to the Commission, marking a contrast to the effects-based approach. The Commission, in assuming more discretionary power, particularly concerning the refusal cases, might have considered the possibility of having to deal with cases similar to *Microsoft*, which cut across EU case law with uneven criteria. This however does not disperse the uncertainty, even potentially increasing it concerning the antitrust treatment of prospective refusal cases. Against the uncertainty as to what extent the effects-based approach is applicable in the analysis of abusive conducts, harmful consequences would emerge, along with irrevocable outcomes regarding the dominant undertakings' incentives towards innovation and efficiency.[525]

5.4. Merger regulation

5.4.1. General overview

Mergers and acquisitions (M&As), or broadly speaking 'concentrations', have since the mid-1980s been subject to the Commission's scrutiny because of their potential to

[524] See the Commission Guidance, para 90, reading; "In particular, it falls on the dominant undertaking to demonstrate any negative impact which an obligation to supply is likely to have on its own level of innovation". See also Philip Marsden, 'Some Outstanding Issues from the European Commission's Guidance on Article 102 of the TFEU: Not-so-faint Echoes of Ordoliberalism' in Federico Etro and Ioannis Kokkoris (eds), *Competition Law and the Enforcement of Article 102* (OUP 2010) 69.

[525] See also Yannis Katsoulacos and David Ulph, Optimal Enforcement and Decision Structures for Competition Policy: Economic Considerations in Federico Etro and Ioannis Kokkoris, *Competition Law and the Enforcement of Article 102* (OUP 2010) 77.

affect both the structure and functioning of the relevant markets.[526] However, this monitoring was limited due to the lack of a particular provision tailored for controlling M&As under the TFEU. Uncertainty could not be resolved fully despite the Commission's efforts to use Article 101 and 102, albeit with the preference to use the latter. This preference did not help so much as the pre-requisite to apply Article 102 to the existence of a dominant position in the relevant market. In the light of such restraints, a Merger Control Regulation (MCR) was issued by the European Council and Parliament in late 1989.[527]

The so-called first Regulation (MCR) has set out procedural and substantive tests to evaluate the changes of control on a lasting basis by means of M&As and structural type (concentrative) joint ventures. With regards to the jurisdictional thresholds, it was set out that all concentrations with an EU (Community) dimension were required to be notified to and approved by the Commission.[528] Regarding the appraisal of the concentrations, the 'dominance test' was adopted under the MCR.[529] This rule

---

526 Broadly speaking, while horizontal mergers would potentially have anti-competitive effects when they lead to concentration through a lessened number of players and reduced competition between them; the vertical mergers may raise competition concerns should there be a risk of foreclosing downstream competitors. For detailed legal and economic analysis through case-law see Nicolas Petit, 'Innovation, Competition, Unilateral Effects and Merger Control Policy' (*SSRN*, 29 January 2018) <https://ssrn.com/abstract=3113077> accessed 9 October 2020; Mrudul Dadhich, 'Regulation of vertical mergers under European Union Law: Lessons to be Learnt by Other Jurisdictions' (2015), Europea Colleg Hamburg, Study Paper No. 3/15 <https://europa-kolleg-hamburg.de/wp-content/uploads/2015/11/Study-Paper_Dadhich.pdf> accessed 9 October 2020.

527 Council Regulation (EEC) No 4064/89 of 21 December 1989 on the control of concentrations between undertakings, OJ L 395, 30/12/1989 ('Merger Control Regulation' or 'MCR').

528 A concentration is considered to have a Community dimension where;

a) the aggregate worldwide turnover of all the undertakings concerned is more than ECU 5000 million, and
b) the aggregate Community-wide turnover of each of at least two of the undertakings concerned is more than ECU 250 million, unless each of the undertakings concerned achieves more than two-thirds of its aggregate Community-wide turnover within one and the same Member State (MCR, art 1(2)).

529 Under MCR it was set out as follows:

> A concentration which creates or strengthens a dominant position as a result of which effective competition would be significantly impeded in the common market, or in a substantial part of it, shall be declared incompatible with the common market (MCR, art 2(3)).

(dominance test) had not been changed until the introduction of the new regulation, namely the 'European Union Merger Regulation' (EUMR).[530] A new substantive test called the 'Significant Impediment of Effective Competition' (SIEC) has been adopted as the new rule for appraisal of the concentrations. This test is reflected in the Article 2(3) of the EUMR as follows:

> A concentration which would *significantly impede effective competition*, in the common market or in a substantial part of it, in particular as a result of the creation or strengthening of a dominant position, shall be declared incompatible with the common market.[531]

The new test focuses on the effects of notified concentration on competition, in combination with the structure of the market, and prohibits mergers that "significantly impede effective competition", not necessarily but "in particular as a result of the creation or strengthening of a dominant position". This latter emphasis on 'dominance' still incorporates consideration of the market structure; yet it apparently leaves room for a divergent interpretation based on the SIEC test.[532] While representing a compromise solution between the dominance test and the new SIEC; the EUMR included many other improvements, i.e. facilitation of the referral procedures, increased flexibility concerning the filing date and the commitment procedures, which all together earmarked the modernization of EU competition law based on the so-called 'effects-based approach'.

---

530 See supra note 223.
531 EU Merger Regulation, art 2(3).
532 Regarding the details of this new test (SIEC), see Petit (n 526).

Having said that, the Commission's approach in dealing with the concentrations is by and large focused on assessment of potential anti-competitive outcomes from the would-be M&As, investigating whether there is a risk of market tipping towards potential products to be created, or creation or strengthening of a dominant position with the concentration. Such concentrations, either horizontal or vertical, are assessed usually against the counter-factual scenarios, in order to establish and analyze the potential outcomes that would arise out of M&As. Because EU merger control normally takes place prior to the implementation of the merger, the counterfactual in merger cases is usually the status quo ante, i.e. the situation that exists at the time when the Commission reviews the merger.[533] This approach would sometimes come up with some costs such as disregarding the counter-functioning efficiencies, i.e. given the potential short-term anti-competitive effects.[534] Remarkably, the theoretical presumptions along with hypothetical scenarios have been noticeably leading the decision-making processes with regard to the possible consequences of the concentrations at the EU level.[535]

In this context, the achievement of interoperability does not constitute an aim of EU merger control policies and mechanisms, just like other competition law tools i.e. Article 101 and 102. Nevertheless, interoperability-centric M&A concerns and remedies find a significant place to themselves within the broader context of EU competition law aims, incorporating follow-on innovation, amelioration of network effects and enhancing competition. Having said that, the most significant and relevant M&A cases are examined below.

---

533 Competition Policy International, 'The Counterfactual Analysis in EU Merger Control' (21 November 2013) <https://www.competitionpolicyinternational.com/the-counterfactual-analysis-in-eu-merger-control/> accessed 9 October 2020.

534 See also supra note 526.

535 See Competition Policy International (n 533).

5.4.2. Interoperability related merger cases

5.4.2.1. First set of case law

Cisco/Tandberg[536] represents a merger case between two entities i.e. Cisco and Tandberg horizontally competing in the market for video communications solutions (VCSs). The relevant markets regarding VCSs were found to consist of 'dedicated room' and 'multi-purpose room' and 'executive office/desktop solutions' as three separate downstream markets, while an upstream market regarding multi-point control units (MCUs) was also included into the investigation. The Commission did not find any serious doubt that the vertical link between upstream MCUs and downstream VCSs would give rise to foreclosure concerns because of the proposed merger.[537] However, Commission's investigation revealed potential entry barriers in the VCS space in relation to the dedicated room solutions market, in particular regarding the absence of multi-screen to multi-screen interoperability.[538] The Commission's concerns surrounded the risk that interoperability between the VCS products of the merging parties and those of their competitors would be degraded in a post-merger period. This horizontal concern was also accompanied by the fact that market shares of the merged entity in the relevant markets would be approximately double of that of its next competitor.

In order to respond such concerns, Cisco proposed a set of commitments, including divestment of its IPRs on the Telepresence Interoperability Protocol (TIP) to be

536 Case COMP/M.5669 - *Cisco/Tandberg* [2010] ('*Cisco/Tandberg* decision').
537 *Cisco/Tandberg* decision, paras 114 and 124.
538 *Cisco/Tandberg* decision, para 53. According to Commission, "interoperability for VCS can refer both to the possibility for different endpoints (different brands or models belonging to different segments) to communicate with each other, and to the possibility for an endpoint to function correctly on a given network infrastructure" (*Cisco/Tandberg* decision, para 55).

assigned to an independent industrial body.[539] By this means, other manufacturers were permitted to participate in the process of updates over the TIP, which was credited as the essential standard to be applied to videoconference communication services. Until the divestiture was to be completed, royalty-free third-party licenses were committed to by the merging parties, concerning the current and future patents that would be essential during implementation of the Protocol. More crucially, according to the commitments which were conceded by the Commission, competitive endpoint vendors and their customers would be able to interoperate with virtually all the merged entity's installed base of multi-screen systems.[540] *Cisco/Tandberg* reveals an interesting example since the case involved the divestment of intangible assets as well as an extensive set of complex commitments in order to ensure interoperability in the market for videoconferencing solutions.[541]

In *Intel/McAfee*,[542] the Commission's review was regarding a conglomerate merger between Intel and McAfee which were active in the markets, respectively, for the x86 central processing units (CPUs) and chipsets and for the security software products. Intel consistently held very high market shares in excess of or around 80% in an overall x86 CPU market, while security software market was found to be more competitive whereby McAfee was the second ranking software security vendor (SSV) following Symantec.[543] While conglomerate mergers mostly do not give rise to competition problems, Commission has had concerns about the risk of preferential treatment or

539 *Cisco/Tandberg* decision, para 147.
540 *Cisco/Tandberg* decision, para 147.
541 See Thomas Hoehn and Alex Lewis, 'Interoperability Remedies, FRAND Licensing and Innovation: A Review of Recent Case Law' (2013) 34(2) European Competition Law Review 101, 109.
542 Case COMP/M.5984 - *Intel/McAfee* [2011] ('*Intel/McAfee* decision').
543 *Intel/McAfee* decision, paras 69-82.

positive discrimination within across the merged entities' products in contrast to the pre-merger period.[544]

One of the Commission's concerns was regarding degradability of cross-interoperability between the merging parties' products with those of their rivals, while possibility of the products of Intel and McAfee being technically tied was also raised as another reason for serious doubts as to the compatibility of the transaction with the internal market. In order to meet these concerns, Intel committed to ensure that instructions and interoperability information for new functionalities in Intel CPUs and chipsets were documented and available for use by independent SSVs on a royalty-free basis.[545] This ensured competing SSVs to be able to compete on a level playing field against the endpoint security services to be offered by Intel in the post-merger period. With regards to the interoperability of Intel endpoint security solutions with hardware developed by Intel competitors, Intel committed not to take affirmative steps to degrade its software performance when operating on a personal computer containing a non-Intel CPU.[546] Thereby, independently developed security solutions by SSVs would interact with the CPUs manufactured by Intel's competitors under the same conditions that they were already working with Intel chipsets and CPUs. As regards the technical tying concerns, in the case where Intel would add any endpoint security software e.g. malware detection engine to Intel CPUs and chipsets, Intel would offer to license independent SSVs to

544 Commission particularised that "Intel could optimise the APIs between its chipsets/CPUs and McAfee's security solutions, its compilers or its software development kits ("SDKs") according to McAfee's design preferences, while the integration with the solutions of competing SSVs would be altered. This would result in McAfee's security solutions running better on Intel's CPUs than the endpoint security of the other vendors" (*Intel/McAfee* decision, para 131).

545 *Intel/McAfee* decision, para 298.

546 *Intel/McAfee* decision, para 300.

interoperate with such software such that the subscription services offered by them would be able to utilize Intel's underlying software.[547]

Intel's commitments covered future products to be jointly developed by the merging parties for a five-year period, during which other original equipment manufacturers would replace Intel's tied security products (switch-off mechanism).[548] These remedies committed on a royalty-free basis are argued to go beyond previous case law e.g. *Microsoft*, whereby the related undertakings were required to update information for new versions of relevant products created by the individual undertakings, but not of the joint products.[549]

The abovementioned case law demonstrates the Commission's readiness to intervene into the proposed mergers with the view to create sufficiently competitive ICT markets along with pro-interoperability measures. If the findings denote a likelihood of effective competition being significantly impeded subsequent to a merger/acquisition, a variety of remedies including enhancement of interoperability could be at the disposal of the Commission, as happened in the given merger clearances. As long as potential degradability of interoperability is at stake in the post-merger period, this might be considered as an anti-competitive risk so as to be deterred with some remedies. Such remedies would include divesting IPRs, e.g. attached to a proprietary protocol set, to an independent industry body such as in *Cisco/Tandberg* and making the interface specifications, including those of future products, available to competitors such as in *Intel/McAfee*.

---

547 *Intel/McAfee* decision, para 301.
548 *Intel/McAfee* decision, para 341.
549 Hoehn and Lewis (n 541) 110.

In view of *Cisco/Tandberg* and *Intel/McAfee*, competition law tools such as demand-side substitutability and the SIEC test seem to have been used in combination, if not from a long-term perspective. Post-merger market concerns usually stem from an intra-platform point of view, appearing to have had a significant role during the course of investigations conducted. From this viewpoint, both in *Cisco/Tandberg* and *Intel/McAfee*, the services and products focused on by the Commission did not embrace the whole marketplace, but those of the merging parties. In this regard, judging whether an effects-based approach or the SIEC-based evaluation was pursued for the above cases would not dismiss the overall concerns. Albeit with the intent of enhancing interoperability, intra-platform perspective being held in such decisions brings these M&A decisions closer to the case law in the pre-modernisation period, i.e. when the Commission's interventions shaped the ground for the mergers between technical platform providers, e.g. CAS owners, and multimedia (pay TV) companies.

In the referred to earlier cases,[550] which mostly related to vertical concerns, the EU Commission intervened into the notified mergers and joint ventures mainly with a view to deter exclusion of competitors via exclusively controlled technical platforms, premium content or through comprehensive multi-media service packages. Considering the market foreclosure risks, the EU Commission defined narrow markets, and made the clearances with a variety of conditions, particularly mandated interoperability at the level of intra and inter platform - predominantly with an

[550] See Case COMP/M.2876, *Newscorp/Telepiù*, Commission decision of 2 April 2003, OJ L 110 of 16 April 2004; Case No.IV/M.2050, *Vivendi/Canal+Seagram*, Commission decision of 13 October 2000, OJ C311/3; Case IV/M. 0037, *BSkyB/KirchPayTV*, Commission decision of 21 March 2000, OJ C 100, 15 April 2000; Case IV/M.0048, *Vodafone/Vivendi/Canal+*, Commission decision of 20 July 2000, OJJ C 11, 20 May 2003; Case IV/M. 993, *Bertelsman/Kirch/Premiere*, Commission decision of 27 May 1998, OJ L 53, 27 February 1999; Case IV/M. 1027, *Deutsche Telekom/Beta Research*, Commission decision of 27 May 1998, OJ L 53, 27 February 1999; Case IV/M. 469, *MSG Media Service,* Commission Decision of 9 November 1994, OJ L 364, 31 December 1994.

emphasis on the former because of the would-be vertically integrated multimedia firms. Facing the risk of double control by the same undertaking which would potentially have digital gatekeeper positions, led the Commission to make the related facilities, i.e. set-top boxes/CASs, available to downstream competitors, stimulate the adoption of common interfaces and bring limitation to the "first windows rights"[551] as well as to the duration of premium content transmission rights. Thereby, not only vertical and horizontal interoperability but also transmission of premium content was secured to be in an open, transparent and non-discriminatory manner. What is more, providing fair and non-discriminatory CAS access to competing companies was acknowledged as crucial for 'media diversity and pluralism', as reflected in the EU sector-specific regulation as well.[552]

As the first set of case law reveals the similar aspects of the earlier cases, it could be argued that presumed competitive and pro-interoperability concerns continued to lead the decision-making processes for the concentrations later on. This also means considering merger controls as an implicit tool or leverage for market regulation, if not precluding the so-called effects-based approach under the EUMR. Under this mixed approach, interoperability was reflected in a large number of the Commission's M&A decisions, having significant implications such as in the first set of case-law i.e. *Cisco/Tandberg* and *Intel/McAfee* decisions.

---

551 Rights holders try to extract maximum value from their programming rights by a variety of commercial practices. One of the referred practices is selling movies several times, being called the 'windows system' in common business language (See Geradin and Layne-Farrar (n 91) 70).

552 See the section '6.2.1.2. Conditional access obligations'.

5.4.2.2. Second set of case law

While EU merger controls demonstrate similar consequences regarding interoperability, a more lenient approach and less stringent conditions could be identified in post-modernization period. Reflecting these features, the Commission's two landmark decisions responding interoperability needs, i.e. *Microsoft/Skype*,[553] and *Facebook/WhatsApp*,[554] could be featured as the second set of case law, as analysed below.

In *Microsoft/Skype*, the notified transaction was related to Skype being acquired by Microsoft, with the conglomerate and horizontal effects under scrutiny. The Commission assessed post-merger effects on the relevant markets, namely 'consumer' and 'enterprise' communications markets, including the related services like voice and video calls, instant messaging messages, and found no serious doubts regarding the so-called effects. Marking a contrast to the previous case law, the Commission's findings revolved around the ephemeral character of large market shares, which were reaching to 80-90%,[555] a stark dominance in the rapidly growing consumer communications market. The Commission found the notified merger would cause no harm based on the acknowledgement that "consumer communications services are a nascent and dynamic sector and market shares can change quickly within a short period of time".[556] Likewise, consumers were found to be "sensitive to innovative services or products" and would be able to switch to new services/applications if the service

553 Case COMP/M.6281 - *Microsoft/Skype* [2011] ('*Microsoft/Skype* decision').
554 Case No COMP/M.7217 - *Facebook/WhatsApp* [2014] ('*Facebook/WhatsApp* decision').
555 The Commission concluded that, albeit with a large market share (80-90%) in the scenario of the narrowest market definition, namely in the Windows based PC market, different scenarios in case of broader markets would not affect the ultimate assessment (See *Facebook/WhatsApp* decision, para 110).
556 *Microsoft/Skype* decision, para 78.

providers "are unable to offer users new and innovative functionality", implicating that 'consumer lock-in' should not be deemed as a matter of concern.[557]

Under the assessment of horizontal effects, interoperability was highlighted concerning the 'enterprise communications market', where Microsoft's Lyn product being merged with Skype was questioned in terms of preferential interoperability. However, it was stressed by the Commission that Skype was already interoperable with Lyn (for instant messaging and voice calls). Even in the case of full integration, preferential interoperability was not featured as a problem since Skype's services were not suitable for the entities that use call centres, which was considered as a key factor.[558] Furthermore, no negative effect was found likely in the subsequent three years, considering Lyn's small percentage of market share in the enterprise communications market.[559] Based on given counter-balancing facts, no condition was imposed on the parties, and the proposed merger was approved by the Commission.

Facebook/WhatsApp represents another concentration unconditionally approved by the Commission. The Commission dismissed the competition concerns regarding relevant markets, namely the markets for 'consumer communication services', 'social networking services' and 'online advertising services' that would be affected by the proposed acquisition. In finding no harm, analysis was devoted to the potential horizontal overlaps within the market for the consumer communication services as well as to the vertical effects in relation to the other two markets. In the former market, both of the merging parties, namely Facebook and WhatsApp were found active with their apps respectively called "Facebook Messenger" and "WhatsApp". On the other

557 *Microsoft/Skype* decision, paras 121-122.
558 *Microsoft/Skype* decision, paras 215-216.
559 *Microsoft/Skype* decision, para 221.

hand, in the latter two markets, just Facebook was found to have been providing relevant services e.g. social networking, photo/video sharing, online advertising.

In relation to the market for consumer communication services, no competition concern was raised, based on the findings similar to those in *Microsoft/Skype*. In this regard, large market shares and network effects were not considered to create a barrier to market entry or expansion in the presence of disruptive innovations,[560] multi-homing[561] and freely downloadable apps that occupy little space on devices.[562] These factors, according to the Commission, would eliminate the switching costs and lock-in risk, even though both of the merging parties were active in the market for consumer communication services. Likewise, no competition concern was raised with regard to the markets for 'social networking services' and 'online advertising services', as the merging parties were regarded as 'distant competitors' in the former[563] and 'non-competitors' in the latter.[564] In terms of targeted advertising, the existence of many service providers competing with Facebook, with them having access to internet user data through alternative means, seems to have had weight within the Commission's assessment.[565]

---

560 According to the Commission, "Consumer communications apps are a fast-moving sector, where customers' switching costs and barriers to entry/expansion are low. In this market any leading market position even if assisted by network effects is unlikely to be incontestable. (…) Also, competing consumer communications apps are able to grow despite network effects, both over time and following disruptions in the market (*Facebook/WhatsApp* decision, para 132).

561 [T]his means that, when customer try new consumer communications apps, users do not generally stop using the consumer communications apps they were previously using (*Facebook/WhatsApp* decision, para 110). In other words, "the use of one consumer communications app (for example, of the merged entity) does not exclude the use of competing consumer communications apps by the same user (*Facebook/WhatsApp* decision, para 133).

562 [M]ulti-homing is facilitated by the ease of downloading a consumer communications app, which is generally free, easy to access and does not take up much capacity on a smartphone (*Facebook/WhatsApp* decision, para 133).

563 *Facebook/WhatsApp* decision, para 158.

564 *Facebook/WhatsApp* decision, para 165.

565 See *Facebook/WhatsApp* decision, para 189, reading; "The Commission notes that, regardless of whether the merged entity will start using WhatsApp user data to improve targeted advertising on Facebook's social network, there will continue to be a large amount of Internet user data that is valuable for advertising purposes and that are not within Facebook's exclusive control."

Although interoperability has been the subject matter of scrutiny from the views of third parties, no critical concern was raised on that. The Commission firstly noted that interoperability was not available on the part of merging parties' main competitors on smartphones, and in particular it was not an element that sustained the entry and expansion of WhatsApp, Facebook Messenger or other popular consumer communications apps.[566] Crucially, in the Commission's view, interoperability would not be considered to be a matter of concern "unless Facebook decide to merge two platforms or to allow cross-platform communication".[567] Notably, technical hurdles against such an integration, i.e. automated matching between Facebook and WhatsApp user accounts, seems to have reduced possible post-merger emergences in the Commission's eyes.[568]

However, strikingly, in August 2016 WhatsApp announced updates to its terms of service and privacy policy, including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities as opposed to the notification by the parties in 2014.[569] Finding this was an issue which Facebook was aware of at the time of notification, The Commission imposed a fine of €110 million on Facebook for providing incorrect or misleading information during the 2014 investigation.[570] The Commission has not reversed back or launched a reassessment for the 2014 merger

566 *Facebook/WhatsApp* decision, para 122.
567 See *Facebook/WhatsApp* decision, para 123.
568 See *Facebook/WhatsApp* decision, paras 159-162. See also Vicente Bagnoli, 'The big data relevant market as a tool: For a case by case analysis at the digital market' (12th Ascola Conference (Competition Law for the Digital Economy) 12 June 2017), 29-34 <https://ssrn.com/abstract=3064795> accessed 9 October 2020.
569 European Commission, Press Release, 'Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover', 18 May 2017 <https://europa.eu/rapid/press-release_IP-17-1369_en.htm> accessed 9 October 2020.
570 Ibid.

clearance, saying that the "clearance decision was based on a number of elements going beyond automated user matching".[571]

Considering the developments following the *Facebook/WhatsApp* decision, data protection aspects seem to have an impact in the future decision making processes of the Commission. From a broader perspective, while the interoperability and integration aspects were found not to have crucial impact in the post-merger period, this rather flexible approach should not be taken as a permanent basis particularly in the light of the subsequent decisions made by the national authorities.[572] As a matter of fact, the opportunity cost of hindered (or limited) interoperability would bear more complicated results and tensions, reaching out to data protection laws and rules. This situation would suggest a more intrusive approach regarding interoperability and related issues, i.e. integration of merging parties' apps, in prospective M&A decisions.

Regardless of the data protection aspect, it is worth noting that horizontal relationships do not seem to have created a significant tension for the Commission in this second set of case law. Had the post-merger interoperability been put under risk because of market power and/or network effects as to be not mitigated by counter-balancing facts, this would have been deemed as a reason for a possible intervention. Besides, the Commission not emphasizing network effects in this caselaw demonstrates that it is considered that many emerging ICT markets do not reveal serious concerns regarding

571 Ibid.

572 Since the closure of the *Facebook/WhatsApp* case with unconditional approval, the relationship between competition law and data protection re-emerged in three cases at the national level. In Italy the Autoria Grante della Concorrenza e del Mercato (AGCM) in May 2017 considered WhatsApp guilty for having forced its users to share their personal data with Facebook. Whereas in Germany, Bundeskartellamt, after an investigation launched in March 2016, found that Facebook abused its dominant position in the social networks market, infringing data protection legislation via imposition of unfair unlawful terms and conditions towards users (Bagnoli (n 501) 30).

market foreclosure, and with reduced vertical concerns. Summing up, a remarkable change in the decision making processes over time is note-worthy, given the *Microsoft/Skype* and previous Microsoft cases i.e. *Microsoft, Microsoft Tying*.[573]

5.4.2.3. *Microsoft/LinkedIn*: Revisiting the interoperability concerns

Microsoft/LinkedIn[574] represents one of the few conglomerate merger cases that were assessed on the basis of various aspects including Big Data, as well as the interoperability relationships. While Microsoft was found to have a strong market position in the markets for 'PC operating system (OS)' and 'productivity software', LinkedIn was found to exist in a number of markets including 'social networking', 'online advertising' and 'recruiting tools'. Relevant markets that would be impacted were defined as the markets for 'professional social networking (PSN) services', 'customer relationship management (CRM) software solutions' and 'online advertising services'. After the Commission's evaluation, a number of conditions were attached to the merger clearance after the finding of potential anti-competitive effects i.e. market foreclosure, seen as likely to happen in the markets where LinkedIn was active.

The proposed acquisition was assessed not only for the conglomerate effects, but also horizontal and vertical effects. In this regard, markets for 'online advertising' and 'CRM software solutions' were reviewed by the Commission through an investigation of potential anti-competitive effects including Big Data related aspects. The assessment

---

573 See also Zhang (n 148) 92, reading; "A real distinguishing feature the Commission could have focused on is that due to the rapidly changing nature of technology enabled markets, the way that consumers use personal computing technology has changed from what it was when WMP and IE were being considered". As rightfully said by the author, consumers are increasingly using their tablets and smartphones and Windows is not the dominant operating systems on tablets and phones, that market instead belongs to Android and iOS, so even if Microsoft were incentivised to tie Skype to Windows and with the action of network effects, the competitive effect of this tie may be different to the tying of WMP and IE to Windows (Zhang (n 148) 92).

574 Case M.8124 - *Microsoft/LinkedIn* [2016] ('*Microsoft/LinkedIn* decision').

relating to the so-called two markets was focused on a likelihood of a *combination of user datasets* for online advertising and *bundling of data access or restriction* of them to the CRM software solutions. These concerns were dismissed as the merging parties were found not to have sufficient market power and the ability to foreclose their competitors in the relevant markets.[575] In fact, both of the merging parties were not active in any of the relevant markets except for the market regarding 'online non-search advertising services', and unilateral post-merger effects were not seen likely because all investigated markets were considered as exposed to competitive forces.

While anti-competitive effects were found unlikely in the markets for 'online advertising services' and 'CRM software solutions', some concerns were raised for the market regarding PSN services. Concerning this market, a number of scenarios were assessed with regards to potential conglomerate and vertical anti-competitive effects. Such scenarios were refined as; the 'pre-installation of LinkedIn into the PC OS', 'integrating LinkedIn features into the Microsoft productivity software i.e. Outlook and other Office products and the refusal to have access to Microsoft's APIs' and 'bundling/tying LinkedIn applications with Microsoft's productivity software'. The main questions marks were put on the queries of whether 'pre-installation' and 'integration' scenarios would hamper effective competition in the market for PSN services.[576] Following the counter-factual analysis, the scenario of 'bundling/tying LinkedIn applications with Microsoft's productivity software' was found unlikely given the presumption that tying was not revealed as a plan through Microsoft's internal documents. Furthermore, it was highlighted that any anti-competitive tying to be done by Microsoft would be challenged under Article 102.[577]

---

575 *Microsoft/LinkedIn* decision, paras 179-180 and 192-193.
576 *Microsoft/LinkedIn* decision, para 302.
577 *Microsoft/LinkedIn* decision, para 304.

On the other hand, in relation to the 'pre-installation' scenario, the Commission found that this strategy would give LinkedIn a greater visibility along with an increased membership base and user activity.[578] Furthermore, Microsoft would easily agree with the manufacturers for pre-installation, and they might not have an incentive to install a second PSN application.[579] According to the Commission, competing PSN service providers were likely to face a potential market tipping and foreclosure, as consumers would have difficulty switching to competing providers.[580] Similar concerns were also raised for the 'integration' scenario, which would enable LinkedIn to have access to the contacts in Outlook, resulting in an expanded network.[581] Moreover, in this scenario, third party access to the Microsoft Office software suite, particularly Outlook, would be risked and access to relevant APIs would be denied to the competing PSN suppliers.[582] This possibility would discredit rival PSN services and put them in a disadvantaged position against the more advanced features of LinkedIn being integrated into Microsoft productivity software, particularly Microsoft Outlook or the Office suite.[583]

Across these scenarios, 'multi-homing' was not acknowledged by the Commission as counter-balancing the foreseen competition concerns. What is more, the Commission considers the given post-merger scenarios "can require significant time on the part of PSN users, [and] can in some cases act as a disincentive to multi-homing between PSN platforms".[584] This feature of the analysis underlies the Commission's 'tipping' concerns in *Microsoft/LinkedIn*, as opposed to *Microsoft/Skype* and

578 *Microsoft/LinkedIn* decision, paras 315-316.
579 *Microsoft/LinkedIn* decision, para 320.
580 See *Microsoft/LinkedIn* decision, para 320.
581 *Microsoft/LinkedIn* decision, para 328.
582 *Microsoft/LinkedIn* decision, para 329.
583 See *Microsoft/LinkedIn* decision, para 330.
584 *Microsoft/LinkedIn* decision, para 345.

Facebook/WhatsApp. At this point, it is noteworthy that market tipping was found unlikely for the consumer communications services in the context of *Microsoft/Skype* and *Facebook/WhatsApp*. According to these decisions, competition concerns were dispelled not only for multi-homing but also because of the presumption that a wider audience were sought by the applicants, respectively Microsoft and Facebook. Conversely, in the *Microsoft/LinkedIn* case, the Commission was concerned that the market for PSN services would be irremediably "tipped" in favour of LinkedIn, ultimately carrying the risk of foreclosure of other PSN providers in that market, such as Xing, GoldenLine and Viadeo, which are LinkedIn's main competitors in Poland, Germany and France, respectively.[585] With regard to the Commission's concerns, Microsoft proposed a number of commitments, specifically responding to the concerns related to the 'integration' and 'pre-installation' scenarios which are given below.

Integration commitments include;

(i) access to all APIs for all core Office products, along with a unified gateway enabling developers to build applications and services that can access data from Microsoft's cloud services,

(ii) making available the Office Store for distribution and downloading of Outlook add-ins for third-party PSN Services,

(iii) ensuring that the so-called Outlook add-ins are run independently of LinkedIn features to be included in Office,

(iv) allowing EEC users to disable LinkedIn features for the entire Office suite.[586]

---

585 Federico Marini-Balestra and Riccardo Tremolada, 'Digital markets and merger control: balancing big data and privacy against competition law – a comment on the European Commission's decision in the *Microsoft/LinkedIn* merger' [2017] 38(7) European Competition Law Review 337, 341. See also *Microsoft/LinkedIn* decision, para 343.

586 *Microsoft/LinkedIn* decision, paras 414-417, 437.

Pre-installation commitments include;

(i) ensuring that PC OEMs and distributors are free not to install any LinkedIn branded application, Start tile or Taskbar button for Windows OS on their PCs that are distributed in the European Economic Area,

(ii) allowing users to remove LinkedIn from Windows if PC OEMs and distributors decide to pre-install it,

(iii) not reiterating in any way against PC OEMs and distributors for developing, using, distributing, promoting or supporting a Windows PC application and/or a Windows PC tile for third-party PSN providers,

(iv) granting users the ability to remove the LinkedIn from their Windows PC OS,

(v) not offering or prompting users to install or including LinkedIn through Windows PC OS or its updates.[587]

With an overall assessment, it is possible to conclude that both sets of commitments not only respond to the relevant scenarios but also aim to ensure a level playing field in the post-merger PSN market. The Commission demonstrates it can use merger control mechanisms to the extent that relevant markets are revisited and revitalized with none or the minimized possibility of competition problems. *Microsoft/LinkedIn*, representing this very end-target, unwraps a package of commitments, revealing a semi-regulatory vision. Intervening in the area of behavioural economics, the Commission opted for a remedy that encouraged users to make a choice as to which PSN to use,[588] and aimed to create equal footing amongst the rival companies.

---

587 *Microsoft/LinkedIn* decision, paras 419-421, 438.

588 Michele Giannino, 'The appraisal of mergers in high technology markets under the EU merger control regulation: from *Microsoft/Skype* to *Facebook/WhatsApp*' (*SSRN*, 12 January 2015) 14-15 <https://ssrn.com/abstract=2548560> accessed 9 October 2020.

Remarkably, the Commission's interventions in several antitrust and merger cases pose a divergence, if not an inconsistency overall. For instance, while tying up Windows Media Player with Windows OS was challenged under Article 102 in *Microsoft*,[589] Microsoft's tying Internet Explorer with its OS did not receive the same reaction later on.[590] On the other hand, scenarios apart from tying e.g. based on integration and pre-installation, clearly appear to have raised concerns on the part of the Commission.

From this viewpoint, interoperability-based behavioural remedies inspired by *Microsoft* seem to have been drawn on in *Microsoft/LinkedIn*. Yet, the *Microsoft/LinkedIn* decision did not specify a unique obligation, e.g. disclosure of interface specifications, and contended with the maintenance of the former level of interoperability between Microsoft's products and those of competitors. Also, remarkably, while interoperability concerns were met and responded to, other concerns such as tying/bundling were dismissed under *Microsoft/LinkedIn*. Given this fact, the antitrust and M&A interventions of the Commission could be said to complement each other, including from the interoperability perspective.

However, this does not reflect the case at all. Interestingly, in *Cisco/Tanberg*, Cisco has already been licensing its essential patents (SEPs) on a royalty-free basis and permitting its competitors to implement TIP in their products, namely videoconferencing solutions. The Commission nevertheless opted to clear the acquisition with the structural and behavioural conditions to ensure the interoperability

589 See supra note 498.

590 In December 2009, the Commission accepted the commitments offered by Microsoft finding them capable to address competition concerns related to the tying of its web browser, IE, to Windows. In this regard, the Commission considered Microsoft's screen choice acceptable, as opposed to its previous decision in 2004. See Case COMP/39530, *Microsoft* [2009] OJ C 45 ('*Microsoft Tying*' decision).

between its products and those of competitors is not impaired.[591] Not only in *Cisco/Tandberg*, even throughout EU history, creating a pro-interoperability environment on the basis of equal footing among the players has functioned as a subordinate goal of merger control mechanisms. Except in circumstances when the interoperability concerns are mitigated via multi-homing and other factors, e.g. the ephemeral nature of market power, the Commission's interventionist approach should be noted against the potential risks of impaired interoperability, as the *Microsoft/LinkedIn* decision signifies clearly.

5.5. Assessment of EU competition law

EU competition law offers a variety of tools to cope with the anti-competitive behaviours and accompanying risks that would accompany different market settings, including via collaborations, concentrations and abuse of dominant position. In this context, ensuring vertical and/or horizontal interoperability stands out as an important objective, usually subordinated to broadly set competition law goals. From this point of view, in the absence of vertical and/or horizontal competition concerns, remedial tools are not invoked to enhance the level of interoperability under EU competition law. Nonetheless, many EU precedents demonstrate the readiness of the Commission to intervene in the case of potentially impaired or absent interoperability.

First and foremost, the *Microsoft* judgement demonstrates that the Commission could enforce Article 102 with a view not only to restore but also to further the level of interoperability, even sometimes going beyond the established lines of case law, i.e.

[591] It should however be noted that this scenario of any impairment or degradability of 'interoperability' could hardly realise, as a dominant company's withdrawal of interface information that was already supplied to third parties would easily be challenged by the European Courts as happened previously in the *Microsoft case*.

regarding ‘exceptional circumstances’. It is undeniable that *Microsoft* caused some erosion of the legal standards applicable to ‘refusal to license’ behaviours, leaving an open and unsecure area for intervention based on the lack of interoperability. The absence of a well-established ‘theory of harm’ albeit with the elaboration of the underlying facts in *Microsoft*[592] would mean future cases could be dealt with on a looser ground that is supposedly to be directly linked to the TFEU rules i.e. Article 102(b) on the basis of literal reading instead of a meticulous interpretation invoking the substantiated consumer welfare criteria for intervention, i.e. through the lens of the effects-based approach, as opposed to the Commission Guidance.

Having said that, competition law tools seem to be stretched to ensure interoperability, even at the expense of consumer welfare. Thus, it is remarkable to add that pro-interoperability competition law remedies would pose uncertainty as to how to implement the applicable tools, particularly the ‘exceptional circumstances’ test. Under this unpredictable environment, competition law practitioners would be expected to act more flexibly, whereas the market players could then face up to risks of infringement and punishment easily. On this note, it should also be emphasized that narrowing the room for the market players in terms of the refusal to supply e.g. interoperability information to third parties, would suggest an expanded duty to deal, resulting in chilled innovation and investment motives. Closely related to this, boundaries between competition law and sector-specific regulation would seem to be

592 See Valentine Korah, *Intellectual Property Rights and the EC Competition Rules* (Hart Publishing 2006) 166, reading; “I would have liked to see a longer discussion of the earlier cases on refusal to supply or license and more economic theory. I would have liked the decision to have been based more clearly on the danger of the adjacent markets tipping in favour of Windows”. For the contrary views see Michele Messina, ‘Article 82 and the New Economy: Need for Modernisation?’ [2006] 2(2) The Competition Law Review 73, 95.

blurrier following *Microsoft* and comparable interventions, which favour a formalistic and pro-competitive approach regardless of proven consumer harms.

As far as Article 101 is concerned, a similar set of consequences could not simply be reached since a more rule-based, technical and detailed proceeding is followed for the scrutiny of agreements and concerted practices. Moreover, a 30% market threshold in this context means a safe harbour that does not exist in antitrust and/or merger cases. Particularly from the perspective of horizontal concerns, market collaborations are often found to be pro-competitive when the market players tend to reach out to an industry-wide solution that would reinforce openness and interoperability. Standardisation agreements illustrate this as they often force their members to share their IPRs when they are essential to the standards to be adopted in the end. Notwithstanding, from a wider viewpoint, many standards do not necessarily reflect on the industry-wide needs for interoperability and innovation, given the fact the SSOs are often strategically used by the stakeholders to stimulate their ecosystem-centric viewpoint incorporating complementary markets.[593] Thus, post-SSO scenarios would incur conflated long-term consequences involving a possibility of market tipping towards certain products, appealing to potential interventions based on Article 102. Such situations would result in a market landscape which might have already gone through a competition law scrutiny yet still posing interoperability problems because of the isolated digital gateways and semi-structural entry barriers, which might fall outside of the reach of both Article 101 and 102.[594] Such digital gateways could be

[593] For a discussion on how and why ICT firms participate in standardisation processes and how different standards are forged based upon various tools and tactical factors pursued by the participants, see Kai Jacobs, 'Corporate standardization, management and innovation' in Richard Hawkins, Knut Blind, Robert Page (eds), *Handbook on Innovation and standards* (Edward Elgar 2017) 377-397.

[594] See also the section '7.2.4.2. Interoperability in the IoT ecosystems'.

illustrated by the IoT based examples like Google (Brillo), Microsoft (Azure), Samsung (SmartThings), Apple (HomeKit), Amazon (Alexa) as well as technical (CAS) platforms which authenticate and transmit the digital signals to TV screens.

Going beyond the economics-based understanding from competition policy perspective, interoperability has a social value which remains difficult to measure.[595] Surfacing particularly in hindrance of information flows, cultural productions and democratic culture for the access and interoperability gaps and related problems e.g. often based on proprietary models that occupy public domain, this social value is not easily recognisable and does exceed the outer limits of the competition law tools and analysis. As highlighted at the outset of this study, major interoperability concerns are not limited to the consumer welfare, and are closely related to civic virtue embedded in the so called social value which would require a broader perspective.

The above snapshot signifies both a dilemma and shortcoming of EU competition law, which increasingly has a regulatory tendency as opposed to its original roots and principles. As implied by a recent report, EU competition law tools are not capable enough to cope with the digital era problems,[596] as particularly surfacing in conjunction with the gatekeeping roles and functionalities. This is more visible in interoperability related cases, whereby the Commission wishes to exceed the established case law and not to confine itself with the concept of 'consumer welfare' having to find consumer harm by weighing up benefits and costs.

Alongside these deficiencies, the lengthy and complicated enforcement procedures should particularly be underlined. While M&A and Article 101 assessments look to

595 Perzanowski (n 40) 113.
596 See supra note 500.

the future with no requirement of retrospectively evidencing the findings, antitrust assessment under Article 102 differs since it relies on qualitative/quantitative evidence demonstrating likely anti-competitive effects as well as scanning through the previous case law to find out the most appropriate rule. This situation does not promise a stable and predictable pathway, as could be implicated from the *Microsoft* decision, which sorted the encountered interoperability problem with uneven criteria and tests, i.e. the incentive balancing test, after a five-year period following the claimant's application.

The expense and complexity of an order to disclose interface information was remarkably high in *Microsoft*, rendering a striking example for the regulatory costs of an antitrust intervention of this kind.[597] In *Microsoft* which first came up with a Commission decision in 2004 that covered an investigation based on a five-year period, the GC has rendered its judgement in 2007, being followed by further conflicts and statements of objectives including a non-compliance decision issued by the Commission in 2008. The enforcement process has been complicated by a great many issues, i.e. royalty rates, (in)sufficiency of interoperability information, which ended up with another GC's decision dated 27 June 2012 upholding the Commission's non-compliance decision.[598] Such a lengthy process, while compromising the credibility of the antitrust investigations, does not result in an effective solution against the time-sensitive, imminent and sometimes structural/architectural interoperability problems.[599] Besides, *Microsoft* type foreclosure-based findings might not stimulate,

---

597 Unver (n 30) 113; Weston (n 13) 189.

598 Hoehn and Lewis (n 541) 107-9.

599 This is particularly convincing as structural and behavioural aspects increasingly meet in ICT markets and behavioural solutions tend to have more structural characteristics in effect (See also A. Van Rooijen, 'Devising Ex ante Interoperability Rules: Lessons from the Court of First Instance's Microsoft Judgment' [2011] 14 International Journal of Communications Law & Policy 1, 2-3, reading; "Although all the specific facts of a case can be taken into account under Article 102 TFEU procedure and it is thus very flexible, a more structural regime may be welcome to ensure that the benefits of interoperability are reaped on a broader scale".

even maintain, the innovation and dynamic efficiency, given the short-cut formulations running short of a well-advanced 'theory of harm'. In this vein, there arises a discrepancy and gap between the EU competition law goals and the formulas pursued in implementation i.e. particularly under Article 102 of the TFEU.

6. Sector-specific regulations: Electronic communications law

6.1. Main elements of the ECRF

6.1.1. Main pillars and evolution of the ECRF

While IPR and competition law measures have a horizontal or generic nature and applicability over any industry or sector, sector-specific rules are industry-oriented characteristically. Among EU sector-specific rules, those governing the telecommunications industry reveal the most prominent and established set of regulations, including interoperability rules and principles. Whereas the main concern of this study is the analysis of ICT-centric interoperability concerns, 'telecommunications', or more broadly speaking 'electronic communications', needs to be paid particular attention since it underlies a great many ICT services, including cloud computing, the IoT, etc. Crucially, electronic communications networks and services constitute the backbone infrastructure upon which not only ICTs but also a globalizing digital economy thrive. Regulations related to the electronic communications sector therefore go beyond a simple sector-specific framework, extending to other ICT spheres along with significant spill-over effects for the economy and society.

From the beginning, the liberalization and regulation of the electronic communications sector have been underscored by European policy makers, with an emphasis on the

'natural monopoly'[600] characteristics of the sector. Avoiding duplication of facilities, particularly duplication of the fixed costs of the network system, has been an important component of the 'natural monopoly' argument for access regulation under the philosophy of sector-specific rules.[601] Not only in telecommunications but also in other network industries, many industry segments were considered non-competitive and opened to third parties' access for similar reasons. For instance, in the rail transportation sector, tracks and stations were found to be non-competitive or a natural monopoly, in contrast to passenger and freight services, as with considering electricity and transmission grids as non-rivalry bottlenecks along with an access regulation. Remarkably, policy makers considered liberalization of the state monopolies insufficient to ensure a competitive market running free from any legal, infrastructural and economic constraints,[602] and made extra effort to pursue open access and interconnection policies towards enabling effective competition and consumer benefits.

Hence, the idea of opening up the network industries to competition has driven the regulatory policies in this area for over two decades across the EU and globe. The Commission's 1987 Green Paper[603] represented the baseline towards this end, setting

---

600 'Natural monopoly' means a situation in which any amount of output is always produced more cheaply by a single firm: the cost of production is lowest when one firm serves the entire market (Daniel F. Spulber, 'Competition Policy in Telecommunications' in M. Cave, Sumit K. Majumdar and I. Vogelsang (eds), *Handbook of Telecommunications Economics* (Elsevier Science B. V. 2002) 486-7). It is acknowledged that in natural monopoly industries that denote scale and scope economies, a firm is presumed to construct and operate the underlying networks more efficiently, e.g. with lower costs, than it would be with more than one firm.

601 Ibid.

602 This fact is enunciated as follows under the Commission's 1998 Access Notice:

> The mere ending of legal monopolies does not put an end to dominance. Indeed, notwithstanding the liberalisation Directives, the development of effective competition from alternative network providers with adequate capacity and geographic reach will take time (Commission Notice on Application of Competition Rules to Access Agreements in the Telecommunications Sector [1998] OJ C 265/02, recital 64).

603 European Commission, Towards a Dynamic European Economy: Green Paper on the development of a Common Market for Telecommunications Services and Equipment [1987] COM (87)290 ('1987 Green Paper').

out an EU-level program incorporating 'liberalization' and 'harmonization' of the telecommunications markets. While the former aimed at fully liberalized markets with no special or exclusive rights, the latter meant adoption of regulatory standards in terms of access, interconnection and ensuring competition. Not only liberalization and harmonization of the relevant markets, but also the co-application of competition law to the telecommunications sector was also acknowledged as one of the principles underlying the 1987 Green Paper. Within the framework of these goals, a Resolution[604] was agreed by the European Council and published on 30 June 1988. Since then, European legislative authorities have responded to both hard law i.e. regulations and directives, and soft law i.e. recommendations and guidelines, in order to realize the articulated policy objectives.

Such legislative measures aimed to transform the telecommunications sector from a state-led monopoly to a competitive marketplace. To that end, liberalization directives were first put into force to ensure removal of all the exclusive and special rights in relevant areas of services, e.g. terminal equipment, wireless and wired services and fixed voice telephony, in a gradual manner. The first step on this pathway was the Terminal Equipment Directive[605] that entered into force in 1988, being followed by 1990 Services Directive.[606] While the former was aiming at withdrawal of legal monopolies in the terminal equipment markets, the latter liberalized provision of telecommunications services, apart from 'voice telephony', in the Member States.

---

604 Council Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 [1988] OJ C 257/1.

605 European Commission, Commission Directive (EU) 88/301 of 16 May 1988 on competition in the markets in telecommunications terminal equipment [1988] OJ 1988 L 131/73.

606 European Commission, Commission Directive (EU) 90/388 of 28 June 1990 on competition in the markets for telecommunications services [1990] OJ 1990 L 192/10.

The Commission took the initiative under Article 106 (formerly 90(3)) of the TFEU, which facilitated the liberalisation process with no requirement to submit these directives before the approval of the European Council and Parliament, as opposed to the procedure under Article 116 (formerly 96) of the TFEU. The CoJ upheld in two respective judgements[607] in 1991 and 1992 that the Commission was entitled to directly enact and implement such directives. Being backed by the CoJ's judgements, the Commission adopted a series of directives amending the 1990 Services Directive to encompass a broader range of telecommunications services: satellite communications, use of cable television networks, mobile and personal communications.[608] The final step was the enactment of the Full Competition Directive, which required Member States to remove all exclusive and special rights for the supply of telecommunications services, including voice fixed telephony, by the 1st January 1998, at the latest.

Liberalization directives were accompanied by the harmonization directives which constituted and laid out an Open Network Provision (ONP)[609] programme that essentially aimed at harmonization of the national measures regarding access to and use of public telecommunication networks and services. The scope of the ONP programme was initially limited to issues of access to the network infrastructure and

---

607 Court of Justice, Judgement of the Court of 19 March 1991 in *Case C-202/88: French Republic v Commission of the European Communities – Competition in the markets in telecommunications terminal equipment*, [1991] ECR-I-01223; Court of Justice, Judgement of the Court on 17 November 1992 in Joined *Cases C-271, C-281/90 and C-289/90: Kingdom of Spain, Kingdom of Belgium and Italian Republic v Commission of the European Communities – Competition in the markets for telecommunications services*, [1992] ECR I-05833.

608 Athanasios Psygkas, *From the "Democratic Deficit" to a "Democratic Surplus": Constructing Administrative Democracy in Europe* (OUP 2017) 37.

609 ONP was defined in the ONP Framework Directive as "the harmonisation of conditions for open and efficient access to and use of public telecommunications networks and, where applicable, public telecommunications services and the efficient use of those networks and services" (Council Directive (EU) 90/387 of 27 June 1990 on the establishment of the internal market for telecommunications services through the implementation of open network provision [1990] OJ L 192/1, art. 2).

'reserved services' provided by the incumbent operators,[610] including postal, telegraph and telephone (PTT) agencies. However, along with gradual liberalization, the idea has been expanded to cover the privately governed networks and services as they succeeded the public incumbents (monopolies). To ensure that such markets thrive in a competitive manner, EU authorities spread the ex-ante regulation to many network components, including the local network or local loop which represents the "end mile" before the end-users. This would be considered as a final step to allow new entrants to compete with incumbent operators under the same or comparable conditions, with no sunk costs to be met by the former.[611]

Following the abovementioned steps being taken, market players were confronted by diverse and wide-ranging measures. Regulatory measures incorporating the ONP Directives during the 1990s, usually called the '1998 regulatory framework', were far from giving a clear signal towards a dynamic, competitive and convergent marketplace. Given this fact, the Commission lauched a review process in 1999, aiming at consolidating and revising the existing directives. Lack of an effective and flexible legal framework that is adaptable to the changing needs of the global information society motivated the review process. Ultimately in 2002, EU legislators adopted a comprehensive and technology-neutral framework, by which all transmission networks and services are covered under the same concept of 'electronic communications'. The 2002 regulatory framework had five aims: (i) to react to

610 Ian Walden, 'Access and Interconnection' in Ian Walden and John Angel (eds), *Telecommunications Law and Regulation* (2nd edn, OUP 2005) 126.

611 By this means of not incurring capital expenditures for building a new infrastructure, new entrants would be able to compete with the incumbents and reach out to the same customer base. Not only such micro, company level benefits, but also macro, EU-wide benefits, including global competitiveness, had a driving force behind such policies, ending up with local loop unbundling (LLU) in each Member State. The Commission, following the Lisbon Summit in 2000, issued a Regulation (2000/2887) mandating LLU across the EU.

technological and market developments; (ii) to promote more effective competition; (iii) to remove unnecessary regulation and simplify associated administrative procedures; (iv) to strengthen the internal market and (v) to protect consumers.[612]

Introduction of the 2002 regulatory framework enabled a more stable and consolidated regulatory structure, which has so far been kept up albeit with necessary modifications and overhauls. Given this fact, while a number of hard and soft laws have been issued by the EU legislature in the following years, the 2002 framework has set the main pillars for the 'ECRF', up until now. Having said that, for the purpose of this study, the concept of the 'ECRF' is preferred because a number of additional regulations and directives have been put into force further to the 2002 regulatory framework. An important and recent development happened with the enactment of the 2018 European Electronic Communications Code (EECC)[613], which signifies an overhaul for the ECRF. Under the EECC Directive, or simply the EECC, is incorporated an expanded set of regulatory mechanisms, procedures and remedies, based on a more forward-looking blueprint.

As far as the historical background is concerned, it should be remembered that the EECC is a part of the Digital Single Market (DSM) process which was initiated by the Commission in 2015.[614] At that time, EU authorities considered that a more consistent and harmonized regulatory structure across the Member States was a pressing need for

---

612 Arnold Porter, European Telecommunications Practice Group, 'Introduction to the New EU Regulatory Framework for Electronic Communications' (2002) 6.

613 See supra note 239.

614 The Digital Single Market traces back to the initiative of the Digital Agenda (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Digital Agenda for Europe', COM (2010) 245 final/2). The so-called Agenda specified 101 specific policy actions across 7 domains: the digital single market; interoperability and standards; trust and security; fast and ultra-fast internet access; research and innovation; digital literacy, skills and inclusion and ICT-enabled benefits for the EU.

the creation of a fully-fledged digital single market. Given this fact, the DSM initiative was launched in May 2015,[615] incorporating electronic communications regulations as well as copyright, standardisation, data privacy, taxation and consumer protection rules. A review process was initiated in September 2015, ending up with a proposal published in September 2016[616] and finally the EECC Directive put into force in December 2018. Targeting a wider and deeper harmonization across the EU, the EECC has streamlined and consolidated the applicable regulatory framework, as explained below.

6.1.2. Regulatory structure and policy objectives

The 2002 regulatory framework, which underlies the so-called ECRF, originated from the five main directives given below:[617]

1- Framework Directive (2002/21/EC), OJ L 108, 24.4.2002.[618]

2- Access Directive (2002/19/EC), OJ L 108, 24.4.2002.[619]

3- Authorisation Directive (2002/20/EC), OJ L 108, 24.4.2002.[620]

---

615 European Commission, 'Digital Single Market: Bringing down barriers to unlock online opportunities' <http://ec.europa.eu/priorities/digital-single-market_en> accessed 9 October 2020.

616 It was set out by the Commission that the review of ECRF would focus on measures that aim to;
- provide incentives for investment in high-speed broadband networks,
- bring a more consistent internal market approach to radio spectrum policy and management,
- deliver conditions for a true internal market by tackling regulatory fragmentation,
- ensure effective protection of consumers, a level playing field for all market players and consistent application of the rules, as well as
- provide a more effective regulatory institutional framework (EECC Directive, recital 3).

617 For more detailed information see European Commission, 'Digital Single Market: Electronic Communications Laws' <https://ec.europa.eu/digital-single-market/en/telecoms-rules> accessed 9 October 2020.

618 Amended by the Better Regulation Directive (2009/140/EC) OJ L 337, 18.12.2009; repealed by the EECC Directive (2018/1972) OJ L 321, 17.12.2018.

619 Amended by the Better Regulation Directive (2009/140/EC) OJ L 337, 18.12.2009; repealed by the EECC Directive (2018/1972) OJ L 321, 17.12.2018.

620 Amended by the Better Regulation Directive (2009/140/EC) OJ L 337, 18.12.2009; repealed by the EECC Directive (2018/1972) OJ L 321, 17.12.2018.

4- Universal Service Directive (2002/22/EC), OJ L 108, 24.4.2002.[621]

5- E-Privacy Directive (2002/58/EC), OJ L 201/37, 31.07.2002.[622]

These Directive were maintained with some modifications until the adoption of the EECC in December 2018. The EECC made a consolidation of these directives, except for the E-Privacy Directive, which was put into another review process.[623] So far, a number of regulations have also been issued that should be comprehended within the context of the ECRF. Among these, the three regulations given below are note-worthy as having a key role with regards to regulatory governance of electronic communications networks and services.

1- Regulation on the Body of European Regulators of Electronic Communications (BEREC), OJ L 321, 17.12.2018.

2- Regulation 2015/2120 on open internet access and net neutrality, OJ L 310, 26.11.2015 (EU Net Neutrality Regulation).

3- Regulation on roaming on public mobile communications networks, OJ L 172, 30.6.2012.

Built on the above directives and regulations, the ECRF means a comprehensive set of rules, rights and obligations which need to be transposed by the Member States.[624] While the EU Directives usually address Member States for the transposition,

---

621 Amended by the Citizens' Rights Directive (2009/136/EC) OJ L 337, 18.12.2009; repealed by the EECC Directive (2018/1972) OJ L 321, 17.12.2018.

622 Amended by the Citizens' Rights Directive (2009/136/EC) OJ L 337, 18.12.2009; repealed by the EECC Directive (2018/1972) OJ L 321, 17.12.2018.

623 See the European Parliament, 'Review of the ePrivacy Directive' (Think Tank, 03/02/2017), <http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2017)587347> accessed 9 October 2020.

624 However, the EU Regulations constitute an exception to this rule as they are directly applicable in the Member States with no requirement for transposition.

enforcement of the transposed rules rests on the independent NRAs in each country. While Member States, in practice the NRAs, enjoy the primary responsibility of implementing the ECRF, the Commission has the role of guiding, updating and monitoring implementation.[625] This means a 'decentralized' system, being managed by means of a number of tools and mechanisms, i.e. market review, spectrum allocation and dispute resolution, which require interaction and collaboration between the parties, i.e. the Commission and NRAs.[626] Also, an increasing number of soft laws, i.e. guidelines, recommendations and decisions, have thus far been issued by the Commission, shedding light on how to enforce the ECRF.[627]

Within the regulatory structure of the ECRF, 'convergence' is the key and leading concept to be taken into account.[628] Convergence is a more important compass for policy making in Europe and in Asia than in the US, where a broader view prevails that recognizes that there are several other trajectories of change, e.g. divergence, differentiation and fusion.[629] According to the notion of convergence, all the transmission networks and services need to be treated in an equal and same manner for regulatory purposes. That is to say, the ECRF is designed to apply to all telecommunications networks, fixed or wireless, as well as broadcast networks i.e. terrestrial, satellite and cable, so that equivalent rules will apply to all these networks.[630]

---

625 See also Psygkas (n 608) 38.

626 For detailed information regarding the check and balances between the NRAs and the Commission, particularly under the market review process, see the section '6.1.3. SMP regime and market remedies'.

627 See the 2002 Guidelines; Commission Recommendations on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC.

628 See the EECC Directive, recital 7.

629 Johannes M. Bauer, 'The Evolution of the European Regulatory Framework for Electronic Communications' (2013) IBEI Working Papers Telefonica Chair Series, 2013/41, 14.

630 Porter (n 612) 11.

Following the spirit of 'convergence', the 'electronic communications service' (ECS) was originally defined under the 2002 Framework Directive to mean "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks".[631] Repealing this Directive, the EECC defines the 'ECS' as a "service normally provided for remuneration via electronic communications networks, which encompasses, (⋯): (a) 'internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120; (b) 'interpersonal communications service'; (c) and services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting".[632]

The abovementioned change by the EECC, responds to the intensifying convergence between the ICT networks and services. Although not covering a great many ICT networks and services, the EECC included some of the online communications services (OCSs) within the definition of the ECS, as detailed below.[633] In this revised structure, convergence still represents the backdrop for the regulation of the ECSs, yet more enhanced objectives and remedies are added to the existing framework, making the ECRF more streamlined and responsive to the digital era.

631 Framework Directive, art 2(c).

632 EECC Directive, art 2(4). 'Electronic communications networks' is also a related key concept in implementation of the ECRF. Under the EECC, 'electronic communications network' is defined as "transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit and packet-switched, including the internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed." (EECC Directive, art 2(1)).

633 See the section the section '6.2.2.2. Introduction of new ECS categories'.

Crucially, policy objectives of the ECRF have also been expanded with the enactment of the EECC, which stipulates that the competent authorities, e.g. NRAs and the Commission, shall:

1) promote connectivity and access to, and take-up of, very high capacity networks,

2) promote competition in the provision of electronic communications networks and associated facilities,

3) contribute to the development of the internal market, and

4) promote the interests of the citizens of the Union.[634]

Notably, "promot[ion of] connectivity and access to, and take-up of, very high capacity networks" was not stated as a policy principle under the Framework Directive (2002/21/EC). This principle has been included by the EECC, which underscores the deployment of and access to high speed and quality broadband networks by bringing about a comprehensive set of access remedies, incorporating both access related obligations and certain incentives for the deployment of high capacity networks.[635]

Against this background, it should be noted that the policy objectives to be pursued under the ECRF, in general, are comprehensive and multi-dimensional. While regulatory obligations concerning connectivity and competition denote the main path of the ECRF, underlying rules and remedies should be fulfilled in conjunction with two other objectives, namely protection of consumers and contribution to the development of the internal market, which incorporate subordinate objectives such as

634 EECC Directive, art 3(2).
635 EECC Directive, Part II, Title II (Access), art 59-83.

ensuring end-to-end connectivity, universal service, protection of personal data and privacy, media diversity and pluralism.

6.1.3. SMP Regime and market remedies

The ECRF, from the beginning, builds upon the co-existence of sector-specific and competition law rules. According to the ECRF, ex-ante regulation should exist where generic competition law measures do not suffice for the policy goals. From this point of view, sector-specific rules are of a complementary and ideally temporary nature. On the other hand, sector-specific rules having an ex-ante character makes these rules directly applicable, e.g. without the need to await any anti-competitive effect, and are implicitly pre-emptive over the competition law rules. This enables wider room for ex-ante regulatory intervention, compared to competition law.[636]

Albeit with potential conflicts, implementation of each body of law is bound up with certain pre-conditions and requirements, resulting in a 'complementary' relationship between the two. EU case law, as manifested in the *Deutsche Telekom*[637] judgment dated 14 October 2010, demonstrates that regulated sectors, such as electronic communications, are not legally immune from competition law, even in the case that

---

636 Arguably, regulatory authorities have wider control rights than competition authorities, because competition law rules challenge the lawfulness of conduct, while regulatory authorities engage in detailed regulation of wholesale and retail prices, profit sharing, investments, etc. (Jean-Jacques Laffont and Jean Tirole, *Competition in Telecommunications* (4th edn, The MIT Press 2002) 277).

637 See Judgment of the Court of Justice of 14 October 2010 in case C-280/08 *Deutsche Telekom v Commission.* Deutsche Telekom (DT) judgment concerns DT's leaving a disproportionate margin between wholesale charges and retail charges for access to the local network. Although wholesale and retail prices were subject to sector-specific regulation, DT has had the commercial discretion allowing itself to restructure the tariffs by reducing the so-called margin. Considering this fact, the Commission concluded that Deutsche Telekom has abused its dominant position in the market for the provision of local access to fixed telecommunications networks via margin squeeze between the wholesale local access (LLU) prices and retail access prices, with the unfair selling prices within the meaning of Article 102(a) of the Treaty. The CoJ upheld the Commission's decision, affirming that such conducts might be subject both to the competition rules and to national or European sector-specific measures (co-existence principle).

an ex-ante approval mechanism is in place. As this judgement demonstrates, despite the similarities between each other, competition law and the ECRF measures have remarkably different natures and functionalities.[638]

Primarily, the part played by sector regulation that deals with market power mainly aims to ensure efficiency by favouring a competitive market structure or by mimicking the results of a competitive market structure.[639] On the other hand, in order to guide the regulators with regards to remedying market failures, the necessary steps to be taken, i.e. from the market definition to the remedies, are set out under the ECRF and related guidelines, recommendations, etc.[640] From a broader point of view, application of the ECRF is envisaged only in cases when there is no effective competition in the relevant market. This is expounded in the EECC as follows:

> Considering that the markets for electronic communications have shown strong competitive dynamics in recent years, it is essential that ex ante regulatory obligations are imposed only where there is no effective and sustainable competition in the markets concerned.[641]

To formulate this in a rather simplified manner, it was acknowledged by the 2002 Framework Directive that the presence of "significant market power" (SMP) in an electronic communications market would mean a lack of effective competition with the requirement of imposing a set of access remedies, e.g. access, non-discrimination,

---

638 Regarding the similarities and differences between the two legal bodies of EU law, see Alexiadis (n 237).

639 Alexandre De Streel, 'The Relationship between Competition Law and Sector Specific Regulation: The case of electronic communications' [2008] 1 Reflets et perspectives de la vie économique 53, 56.

640 See also infra note 651.

641 EECC Directive, recital 29. See also EECC Directive, art 3/4(f).

cost orientation and accounting separation, on the SMP undertakings.[642] While this is not phrased in the same way, the SMP is still conferred a key role in the determination of the appropriate level of ex-ante regulation, under the EECC.[643] It could thus be said that the SMP-based access remedies constitute the backdrop of the ECRF in pursuing the goal of promoting competition.

Through the SMP regime under the ECRF, it is intended that "overall analysis of the economic characteristics of the relevant market" is conducted on the basis of competition law terms and criteria.[644] Crucially, the concept of SMP defined under the EECC is equivalent to 'dominance' as defined in the case law of the CoJ.[645] Not only in designating SMP undertakings but also in imposing access remedies on such undertakings, namely in all steps of 'market analysis' defined under the EECC, competition law terms and methods are invoked. Nonetheless, hybridisation of the SMP regime with competition law methodologies should not be understood as allowing antitrust to be stretched beyond its reasonable limits and replacing sectoral regulation.[646] This approximation is just an attempt to ensure that regulatory decisions are more flexible and closer to the economic reality of the market,[647] as well as responding to the more complex and dynamic markets.[648]

---

642 Framework Directive, recital 27. See also the Framework Directive, art 8/5(f).

643 See the EECC Directive, recital 163 and art 67-68.

644 2002 Guidelines, para 78.

645 See the EECC Directive, recital 161. See also the EECC Directive, art 63(1) reading as follows:

> An undertaking shall be deemed to have significant market power if, either individually or jointly with others, it enjoys a position equivalent to dominance, namely a position of economic strength affording it the power to behave to an appreciable extent independently of competitors, customers and ultimately consumers.

646 Alexandre De Streel, 'The New Concept of "Significant Market Power" in Electronic Communications: The Hybridisation of the Sectoral Regulation by Competition Law' [2003] 24(10) European Competition Law Review 535, 542.

647 Ibid.

648 See the Framework Directive, recital 25.

The steps to be followed under the SMP regime are respectively prescribed as 'market definition', the 'SMP assessment' (identifying SMP operators) and 'market remedies' (selecting and imposing appropriate remedies in order to eliminate market failures). As specified in Article 67 of the EECC Directive (formerly Article 16 of the Framework Directive), which sets out procedure for 'market analysis', NRAs shall take the utmost account of the Commission Recommendation and the Guidelines when applying the prescribed 3 step-procedure.[649] On top of these three more apparent steps, should be added a further step, the 'evaluation of market remedies', which is implicitly recognized under the ECRF,[650] as reflected below.

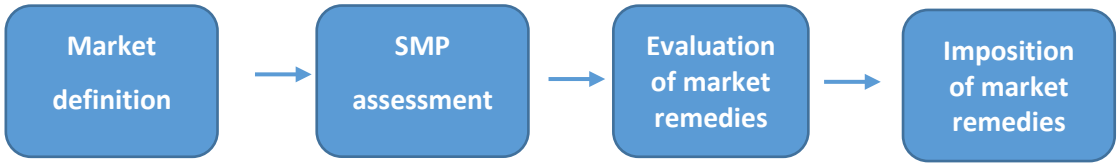

Figure 6: SMP regime

Source: Constructed by the author

Regarding the first step, namely market definition, the Commission's recommendations have a key role in guiding NRAs in their decisions. Notably, the Commission has so far issued three Recommendations, respectively in 2003, 2007 and 2014, distinguishing certain markets that are susceptible to ex-ante regulation.[651] To

649 See De Streel (n 646) 537.
650 EECC Directive, art 68-74 and 76-81.
651 Commission Recommendation of 9 October 2014 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (2014/710/EU) [2014] OJ L 295; Commission Recommendation of 17 December 2007 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (2007/879/EC) [2007] OJ L 344; Commission Recommendation of 11 February 2003 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (2003/311/EC) [2003] OJ L 114.

remove such a market from ex-ante regulation, or to add a new market on top of those enlisted by the Commission, the relevant NRA has to fulfill the 'three criteria test'.[652] Under this test, the conditions of (i) the 'presence of high and non-transitory barriers to entry', (ii) 'absent market structure tending towards effective competition' and (iii) the 'insufficiency of competition law to address market failures' should exist to justify ex-ante regulation for the relevant market.[653]

In any case, demand and supply substitution of the relevant products e.g. networks and services, as well as potential competition, need to be evaluated for each market being defined. When price elasticities point to a set of products that are non-substitutable with others, a separate market could be mentioned to exist. To arrive at such a conclusion, NRAs often invoke the hypothetical monopolist (SSNIP) test,[654] which represents a widely acknowledged competition law tool. Market definition which needs to be recurring every five years for the purpose of sector-specific regulation[655] always needs to be done on a forward-looking basis,[656] depending on the existing market data.[657]

Following market definition, NRAs are charged to assess SMP (dominance) to evaluate whether any undertaking has a dominant position (SMP) in the relevant market. In so doing, market shares are taken into utmost account as the primary factor

---

652 See the EECC Directive, art 67(1).

653 Ibid. The three-criteria test being met simply gives way to an NRA imposing a number of remedies on the SMP undertaking(s), including modification and/or withdrawal of the remedies already imposed. However, the three criteria test does not directly conclude with this result, but allows the NRA to carry out the market analysis with the next step(s), namely designation of the SMP undertakings and the appropriate remedies.

654 Regarding details of the hypothetical monopolist test, see the section '5.1. Market Definition'.

655 According to the ECRF rules, NRAs are required to carry out analyses of the relevant markets at least every five years (See the EECC Directive, Article 67(5/a)).

656 2002 Guidelines, para 27.

657 NRAs should determine whether the market is prospectively competitive, and thus whether any lack of effective competition is durable, by taking into account expected or foreseeable market developments over the course of a reasonable period (2002 Guidelines, para 20).

to determine whether there exist SMP undertaking(s) in the relevant markets.[658] Being not solely based on the market shares, any SMP assessment should build on "a thorough and overall analysis of the economic characteristics of the relevant market" reflecting on further criteria such as; 'overall size of the undertaking', 'control of infrastructure not easily duplicated', 'technological advantages or superiority', 'economies of scale', etc.[659]

Following determination of the SMP undertakings, market analysis should carry on with the designation of remedies. According to Articles 67 and 68 of the EECC Directive, NRAs should impose appropriate remedies on SMP operators at the end of the market analysis procedure. In this regard, if the relevant market is found not to be effectively competitive, e.g. signifying potential anti-competitive behaviours, those SMP players should then be subject to ex-ante obligations. The key point here is that the NRAs should select the remedies in view of the potential market failures, "based on the nature of the problem" and complying with the 'proportionality' principle.[660] Imposition of the most appropriate remedies thus entails analyzing whether and to what extent SMP players could affect potential competition through various factors, i.e. retail prices and availability of services.

From this point of view, 'evaluation of market remedies' is as important as other steps given the fact that NRAs should not react to every potential anti-competitive effect in the same manner. While the toolbox in the hands of NRAs is comprised of wide-ranging access obligations, including structural remedies i.e. functional separation,

658 According to the 2002 Guidelines, single dominance concerns normally arise in the case of undertakings with market shares of over 40%, although very large market shares - in excess of 50% - are in themselves, save in exceptional circumstances, evidence of the existence of a dominant position (2002 Guidelines, para 75).

659 2002 Guidelines, para 78.

660 EECC Directive, art 68(4).

such remedies are supposed to be selected against the market structure, price levels and potential abusive behaviours in the relevant market. It seems that, according to 73(1) of the EECC, access remedies could be imposed in case a consumer harm is likely to attend a potential anti-competitive threat. More explicitly, when "emergence of a sustainable competitive market at the retail level" is at risk of hindrance due to a SMP firm's potential denial of access, that firm may be subject to ex-ante access remedies should the NRA consider such a denial "would not be in the end-user's interest".[661] It is noticeable that the network component or service in question should not necessarily be 'indispensable' or 'essential' for the third parties to compete in the relevant market. Therefore, the threshold for intervention under the ECRF seems to be easier and more accessible when compared to EU competition law.

6.1.4. A deeper look at the ECRF: Critical review of the regulatory mind-set

Electronic communications' regulations both at the EU and national level aim at eliminating monopolies and building up competitive markets through access and pricing obligations mainly directed at dominant players. Hence, the SMP regime and underlying EU regulatory system envisages that access to the bottleneck, essential facility type network components e.g. local loop, or services e.g. interconnections, will ensure the achievement of the targeted policy objectives. Behind this regulatory system lies the notions of 'sunk costs' and 'entry barriers' which are conceived to support each other,[662] warranting coercive regulations. Barriers to entry in the

661 EECC Directive, art 73(1).

662 When interconnection is at stake, the notion of 'sunk costs' is by and large replaced with the notion of 'network externalities', which is considered to be harmful unless mitigated by an interconnection obligation. Indeed, the presence of an externality may lead to under-consumption in the case of a positive externality and over-consumption in the case of a negative externality (De Streel (n 571) 66). For instance, less than the optimal number of customers may decide to join a network if new customers are not compensated, when joining the network, for the increase of welfare they create to the already existing customers (Ibid).

telecommunications sector are related to both size and lack of flexibility in investments,[663] which are often echoed by a 'natural monopoly'.[664]

Although sunk costs, as well as natural monopoly features, pave the way to access remedies to a certain degree, sector-specific regulations particularly in the field of electronic communications would need to be dealt with from a deeper and broader perspective. First of all, it is worth criticizing those ECRF rules and measures targeted at, or mainly invoked to, eliminate structural barriers so as to stimulate new entries to the market. So often, regardless of the behavioural aspects, network components run by the incumbents are considered to threaten would-be competitive services and consumer welfare unless they are made available to third party access. Despite the plausibility of this approach, the infrastructure-intensive narrative would be challenged for it lacks an in-depth analysis with respect to the behavioural aspects,[665] from a broader ICT viewpoint.

The implicated need for a broader ICT perspective should be considered in parallel with IP convergence and accompanying developments. IP convergence has long been driving the development of communication means, demand and network structures. Innovations such as fibre optics, digitalisation and packet-switching changed completely not only the technical, but also the economic environment of telecommunications.[666] Consumer demand, stimulated by technological advances,

---

663 William H. Melody, *Telecom Reform: Principles, Policies and Regulatory Practices*, (Private Ingeniørfond, Technical University of Denmark 1997) 114.

664 See also Unver (n 100) 74.

665 Remarkably, since the decline of the Structure-Conduct-Performance paradigm in industrial economics, it is now recognized that non-strategic and strategic market failures are closely linked together and that structure influences conduct as much as conduct influences structure (Alexandre De Streel, 'Efficient Regulation of Dynamic Telecommunications Markets and the New Regulatory Framework in Europe' in Ralf Dewenter and Justus Haucap (eds), *Access Pricing: Theory and Practice* (Elsevier B.V 2007) 359).

666 Larouche (n 475) Introduction.

leads the way to how electronic communications networks are governed and services consumed, and at this point IP convergence functions as the catalyst of both the demand and supply of ICT networks and services. The locus where demand and supply meet each other is moving from the legacy telecommunications networks to 'digital platforms' that are run based on the internet and wide-ranging ICTs.

Here, two focal points need to be elaborated. First and foremost, the legacy networks have extensively been, and are still currently being, replaced with next generation networks (NGNs), which mean software-governed and fibre-equipped networks capable of meeting ever-increasing ICT-based needs. As the proliferation of NGNs come about within certain quality parameters, e.g. regarding high speed and reduced latency, they require enhanced investment and returns from the employed sunk cost, though the same does not work equally for the software companies running over these networks. Given also the shifting locus mentioned above, the legacy ECRF regulations which are heavily focused on fixed/mobile/broadband network access are controversial and possibly with negative consequences because of their unpredictable effect over NGN investment and long-term consumer benefit.[667]

It is important to note that interactions among ICT players increase and spread across the technological layers of an IP stack, being not limited to the telecom operators. As the digital platforms have an extra-territorial reach, along with a globalising digital economy, firms and individuals increasingly need to communicate with other firms and individuals. In this context, electronic communications' operators increasingly collaborate with the upper layer e.g. software management and content players and the

[667] See Mehmet Bilal Unver, 'Is a fine-tuning approach sufficient for EU NGA policy? A global review around the long-lasting debate' [2015] 11(39) Telecommunications Policy 957, 970-972.

lower layer e.g. terminal equipment players, in order to maintain and reinforce their controlling power over the users with diversified and enriched products. This tendency largely stems from the fact that the distance between conventional telecommunications companies (telcoes) and consumers vanishes and turns into a fast-track direct link when the latter have a relationship with the upper layer companies. Not only these companies e.g. Google and Facebook type software companies, but also cloud and IoT providers get closer to the consumers by providing substitutive as well as complementary services alongside the so-called telcoes.[668] These developments surrounding IP convergence pose some legal and regulatory challenges particularly for the ECRF.

From a broader point of view, the increasing synergies between the internet; TCP/IP, the IoT, the transition from IPv4 to IPv6 and cloud computing, and the revolutionary changes in other technological and social arenas are leading to a new era of global development with the use of NGNs, EDGE technology and the move to store local content nearer to the consumer, can all be seen as constituting a 'fourth industrial revolution'. Having said that, it is also visible that the abovementioned shift of locus, while taking place from the bottom to the upper layers, entrusts more controlling power to the consumers. At the same time, computing and computer networks contributed heavily to the splintering of network infrastructures, by permitting fine-grained, swifter and more sophisticated management of large enterprises.[669]

---

668 Regarding the technical and economic characteristics of cloud computing and IoT services, see the section '7. Case studies: Internet of Things and Cloud Computing'.

669 Jean-Christophe Plantin, Carl Lagoze, Paul N. Edwards and Christian Sandvig, 'Infrastructure studies meet platform studies in the age of Google and Facebook', [2018] 20(1) New media & society 293, 301, referring to Manuel Castells, *The Rise of the Network Society* (Blackwell Publisher 2000).

However, for the time being, sector-specific regulations in the field of electronic communications have an increasing pace and density at the EU level. EU regulatory policies, largely putting aside the natural monopoly and related considerations, pursue a pro-competitive approach and contemplating the short-term benefits to be derived from network access regulations. Proliferation of NGNs and the landscape enabling the provision of equivalent services through a myriad of converging networks do not appear to pre-empt the Commission from pursuing legacy rules for ex-ante regulation. As implied above, the burden of proof for sector regulation to intervene in the selected markets is already lower than in antitrust law,[670] and the Commission endeavours to further lower the threshold to intervene.[671] However, this would mean a regulatory policy that fails to explicitly consider the investment effects of regulation,[672] also having the potential to affect consumer welfare contrary to expectations.

Crucially, if the technology is dynamically evolving and where both interdependencies and indirect effects are important, then a more dynamic and systemic approach will need to be adopted, taking direct and indirect effects of an intervention into account.[673] Lacking this perspective, the EU system, while elaborating on the potential market failures and entry barriers in the designated electronic communications' markets, does

---

670 De Streel (n 639) 68.

671 While the EECC gives some hints on this i.e. through a double lock system as envisaged under Article 33(5/c) regarding inconsistent market remedies, the Commission's 2013 Proposal for the Telecom Single Market (TSM) Regulation in its original draft was far more overbearing. Under the TSM Proposal was placed a number of new issues, such as veto power on spectrum management decisions, as well as market remedies, single authorization and mandatory virtual broadband access, which all denoted a more centralized yet less substantiated decision-making process at the EU level (See Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent', COM(2013) 627 final, (COD) <https://ec.europa.eu/digital-agenda/en/news/regulation-european-parliament-and-council-laying-down-measures-concerning-european-single> accessed 9 October 2020.

672 Bauer (n 629) 15.

673 Johannes M. Bauer, 'Governing the Mobile Broadband Ecosystem' [2015] 22(2) International Telecommunications Policy Review 1, 16.

not look at cross-market relationships from an overall ICT viewpoint. Hence, the ECRF's limited remit and focus on regulatory micromanagement over electronic communications' networks and services risks interdependencies and indirect effects being overlooked.

To sum up, the ECRF, albeit with its early emphasis on convergence, over-emphasizes the regulation of electronic communications i.e. fixed and mobile networks and broadband, leased line and voice) services, by excluding other ICT services from the regulatory scope. While the so-called networks and services are covered by the ECRF, a great many software governed services and underlying networks, including digital platforms, are not comprehended, despite the strong and dynamic interplays between them. Regardless of this approach's shortcomings, it is fair to say that interdependencies between the bottom and upper layers, which reveal new formations of digital ecosystems e.g. surrounding the IoT and cloud networks, appear to be an absent part of the EU regulatory approach. In this context of the so-called regulatory micromanagement focused on the lower layers, it should be reminded that software-governed ICT networks and services are given an advantageous leeway from the regulatory viewpoint. Overall speaking, pursuit of a multi-layered and holistic perspective is likely to reduce the potential legal and social costs that would come about with over or early regulation i.e. reduced investment.

6.2. Interoperability under the ECRF

6.2.1. Interoperability concerns and obligations

ICT markets characterise well 'network industry' features, particularly network effects. The absence or presence of interoperability impacts the extent to which

network effects are influential over the market players. As explained above, the degree of interoperability prevailing in an ICT market has an influence on the competitive dynamics of the marketplace. As far as electronic communications' markets are concerned, 'end-to-end connectivity' and other interoperability-based concerns accompany network effects in shaping the regulatory solutions. Having said that, interoperability is meant to be a self-evident public policy goal of the ECRF, so often independent from competition related concerns and remedies. Below, it is examined whether and to what extent interoperability is instrumentalised and regulated ex-ante, with a focus on specific areas of ECRF.

6.2.1.1.Interconnection

'Interconnection' means "the *physical and logical linking of public electronic communications networks* used by the same or a different undertaking in order to

- allow the users of one undertaking to communicate with users of the same or another undertaking, or
- to access services provided by another undertaking where such services are provided by the parties involved or other parties who have access to the network".[674]

Not only the physical and logical connection of networks but also consumers using such networks to communicate with each other is encompassed by interconnection, which is illustrated in the Figure 7. As shown in this figure, the disparate network users

[674] EECC Directive, art 2(28). For detailed information regarding definition, types and functioning of interconnection (agreements), including related competition law precedents and sector specific rules, see Kariyawasam (n 131) 136-223.

become able to communicate with each other and benefit from joining a more valuable network by means of interconnection, which is represented by the dashed line.

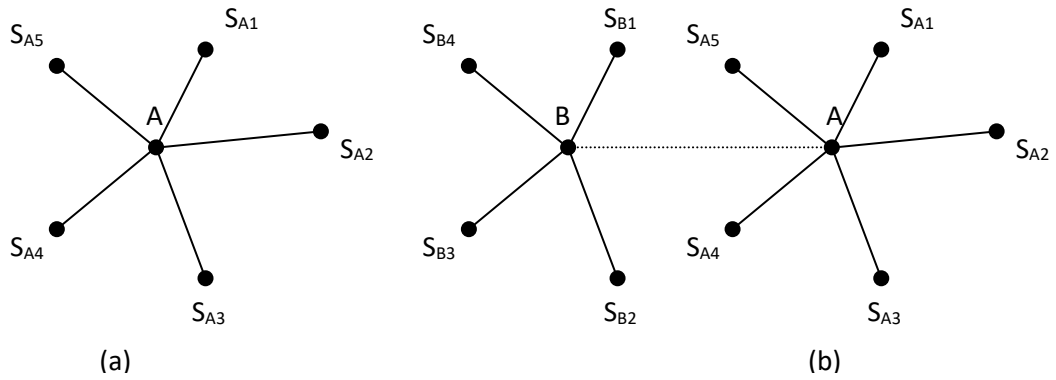

Figure 7: Interconnection

Source: Jonas Holm, 'Regulating Network Access Prices under Uncertainty and Increasing Competition: The Case of Telecommunications and Local Loop Unbundling in the EU' (MSc Thesis, University of Copenhagen 2000) 4.

Lying at the heart of liberalization and open access policies, 'interconnection' ensures 'network externalities'[675] are spread across the networks connected to each other, instead of internalizing them. As a matter of fact, network industries may have a "start-up" problem in that the initial networks may be so small that they are not sufficiently attractive to potential customers, so competing firms may have an incentive to interconnect so that the industry as a whole is more attractive to customers.[676] In order to prevent network externalities from being internalized by the incumbents and pre-empt anti-competitive behaviours, interconnection is usually mandated as a remedy for SMP undertakings.[677] Alongside this, non-SMP operators could also be subject to

675 Network externalities represent direct network effects, in that consumer utility directly depends on the market size, independently of the price system (John-Hee Hahn, 'Nonlinear Pricing of Telecommunications with Call and Network Externalities' (2002) 2 <https://krannert.purdue.edu/centers/ijio/Accepted/1720.pdf> accessed 9 October 2020).

676 Gerald R. Faulhaber, 'Access ≠ Access1 + Access2' [2002] 3 Law Review of Michigan State University, Detroit College of Law 677, 689.

677 See the EECC Directive, art 73(1/i).

the interconnection obligation in certain cases, if this is necessary to ensure end-to-end connectivity, namely any-to-any communication.

For end-users to communicate with each other, not only physical but also logical, software-level interconnections need to be secured, to which 'interoperability' is key. Having said that, interconnecting parties need to use the same protocols with each other to ensure 'end-to-end connectivity'. At this point, 'interoperability' meets 'interconnection' and 'end-to-end connectivity' which also relates to and enables the achievement of other goals, i.e. the 'contribution to development of the internal market'. Here it is important to state that, regardless of the policy objective of 'promotion of competition', interoperability of the networks and services needs to be secured, within the broader context of the ECRF. Reflecting this, a number of provisions are covered in the EECC, as explained below.

First and foremost, the EECC Directive establishes the basic rule that anyone operating a communications network available to the public has both a right to negotiate interconnection with other operators, and when requested, an obligation to enter into such negotiations with other network providers "in order to ensure provision and interoperability of services throughout the Union".[678] This link between interconnection and interoperability could be discerned from Article 61(2/a) of the EECC Directive, according to which NRAs shall be able to impose:

> to the extent necessary to ensure end-to-end connectivity, obligations on undertakings subject to general authorisation that control access to

[678] EECC Directive, art 60(1).

end-users, including, in justified cases, the obligation to interconnect their networks where this is not already the case.[679]

Given this fact, 'interconnection', whilst inhering as one of the key SMP remedies, could also be the subject matter of basic, generic, or non-SMP ECRF obligations, when this is necessary *to ensure end-to-end connectivity.* The vision of ensuring interoperability in this context, aims at ensuring 'interconnection' incorporating end-to-end connectivity. Overall, it could be argued that a subordinate place is conferred to ICT 'interoperability' within the context of the ECRF.

6.2.1.2. Conditional access obligations

Conditional access systems (CASs) are used to mean set-top boxes which function to translate digital signals into analogue signals for television sets, adding intelligence to them and allowing them to have some interactive capabilities.[680] Set-top boxes, with underlying elements of hardware e.g. a smart card and software e.g. an encryption system and subscriber management functions, constitute CASs[681] that enable authorised end-users to receive and view the content delivered to the users' terminals e.g. TV sets. For over two decades, CASs have become so popular and influential over the behaviours of consumers by enabling them to select their choice of TV

679 EECC Directive, art 60(1). According to the EECC Directive, control of means of access may entail ownership or control of the physical link to the end-user (either fixed or mobile), and/or the ability to change or withdraw the national number or numbers needed to access an end-user's network termination point. This would be the case for example if network operators were to restrict unreasonably end-user choice for access to internet portals and services" (EECC Directive, recital 144).

680 Nikos Nikolinakos 'The New Legal Framework for Digital Gateways - The Complementary Nature of Competition Law and Sector-Specific Regulation' [2000] 9 European Competition Law Review 408, 409.

681 Natali Helberger, 'Access to technical bottleneck facilities: the new European approach' [2002] 46 2nd Q Communications & Strategies 33, 34.

programmes, use their TV sets as computerised devices to browse and surf through the internet, as well as viewing specialised content e.g. video on demand.

As the content flows through CASs and related components, including APIs and electronic programming guides (EPGs), CAS platforms have long been considered to function as one of the gatekeepers to control access to the end-users. This consideration was driven by two main points: Firstly, as proprietary technologies are chosen by the platform owners with regard to APIs and EPGs, consumers could be locked into the platforms because of the network effects and switching costs. Secondly, the potential limitation or denial of access to alternative content resulting from such control mechanisms would cause the monopolisation of the consumer base(s) along with public policy problems, in particular 'media diversity and pluralism'.

In response to the abovementioned problems, European policy makers followed a mid-way approach through which proprietary solutions are allowed with an intensive ex-ante and ex-post scrutiny over the relationship between the upstream i.e. pay-TV and downstream i.e. CAS, markets. Whilst enabling faster development of the industry on the basis of proprietary platforms, EU authorities did not allow the relevant parties to collaborate on an anti-competitive basis and/or to exclude potential competitors from the market(s). On the one hand, the EU Commission closely monitored concentrative i.e. merger and acquisition based and collaborative i.e. joint venture based actions, by means of imposing conditions for clearances, including mandated third party access to technical platforms and/or premium content. On the other hand, CAS providers are obliged to grant all broadcasters access to their technical platforms through FRAND terms, under the ECRF (formerly 2002/19/EC Access Directive, now under the EECC).[682]

[682] See the EECC Directive, art 62(1), with reference to Annex II, Part I of the Directive which requires "all undertakings providing conditional access services" to:

While the first type of conditions under the merger clearances represent regulatory actions promoting both inter and intra-platform competition, the latter generic, ex-ante conditional access obligation mainly aims at intra-platform competition.[683] Crucially, all the related remedies embody ensuring interoperability as the key requirement. In M&A cases,[684] the Commission investigated whether comprehensive service packages and deals between the parties would foreclose effective competition in emerging and traditional markets, as well as whether notified concentrations or joint ventures would exclude competitors via either exclusively controlled technical platforms or privileged access to premium content. When compared to the generic CAS obligation enshrined under the EECC, this means a broadened viewpoint incorporating both intra and inter platform competition.

Nonetheless, the CAS obligation set out under the EECC specifies a unique regulatory path by which all broadcasters are enabled to have their content received and viewed by the analogue TV users who rely on set-top boxes, namely the CASs. This ECRF obligation contemplates a remedy with no burden of proof for anti-competitive effects. Notably, this generic and symmetric obligation is applicable to all transmission providers, the technical platform, irrespective of their market powers.[685] The CAS obligation is a remarkable example of an interoperability-centric remedy within the

> (…) offer to all broadcasters, on a fair, reasonable and non-discriminatory basis compatible with Union competition law, technical services enabling the broadcasters' digitally-transmitted services to be received by viewers or listeners authorised by means of decoders administered by the service operators, and comply with Union competition law (EECC Directive, Annex II, Part I).

683 See also Natali Helberger, *Controlling Access to Content - Regulating Conditional Access in Digital Broadcasting* (Kluwer Law International 2005) 153.

684 See supra note 550.

685 Non-SMP operators being covered by this obligation signifies the key role attributed to the CASs under the EECC, which explicitly acknowledges "Competition rules alone may not be sufficient to ensure cultural diversity and media pluralism in the area of digital television" (EECC Directive, recital 159).

intersected area of the telecommunications and media industries, also featuring CAS providers out of the two industries' convergence.[686]

While transmission through a CAS platform, as well as broadcasting, is managed usually by content providers, this dual role position being assumed by the same stakeholder potentially poses a strain over media diversity and pluralism, as well as potential competition. The CAS obligation enshrined under the EECC is conceivable as a response to eliminate this by offering an intra-platform interoperability-based solution. Besides, APIs and EPGs are also covered within the additional obligations that are envisaged to be imposed by the NRAs under certain, limited circumstances.[687] Last but not least, while the Commission is empowered to determine a common API across the EU, this last-resort regulatory step would be unnecessary in the absence of horizontal concerns and risks threatening a competitive marketplace.[688]

6.2.1.3. NGN based implications

As mentioned above, there exist certain areas where interoperability constitutes a subject matter of regulation under the ECRF. Considering no distinction could be mentioned as to the underlying networks and services from the interoperability viewpoint, NGN interoperability could be said to be embodied within conventional areas of regulation. Notwithstanding, the transition from legacy networks to NGNs undoubtedly brings about new issues and requirements which need to be paid

686 On the other hand, it is remarkable that the envisaged obligations are limited to the CAS technical platforms, but not to other interactive service applications, devices and platforms.

687 According to Article 61(2/d) of the EECC Directive [with reference to Annex II, Part II of the Directive], NRAs shall be able to impose obligations on CAS providers to provide access to APIs and EPGs on fair, reasonable and non-discriminatory terms "to the extent necessary to ensure accessibility for end-users to digital radio and television broadcasting and related complementary services specified by the Member State".

688 Unver (n 27) 166.

particular attention to. Below, starting with the generic interoperability provisions, the EECC is examined with a focus on the NGN related challenges.

As formulated under various articles of the EECC, i.e. Articles 61, 62, 72 and 73, access and interconnection remedies lie at the centre of the ECRF. Under Article 61(2/b) of the EECC, which represents a generic and symmetric provision, it is stipulated that NRAs be able to impose "in justified cases and to the extent that is necessary, obligations on undertakings that control access to end users to make their services interoperable".[689] As opposed to this rather widely formulated measure, Article 73(1) of the EECC entails a set of remedies focused on SMP undertakings. Within this framework, it is established that SMP undertakings might be subject to a number of interoperability-centric remedies, as given below:

> "(f) to grant open access to technical interfaces, protocols or other key technologies that are indispensable for the interoperability of services or virtual network services;
>
> (…)
>
> (h) to provide specific services needed to ensure interoperability of end-to-end services to users, or roaming on mobile networks;
>
> (i) to provide access to operational support systems or similar software systems necessary to ensure fair competition in the provision of services"

The SMP remedies stated above might be argued to cover NGN-based intelligence and functionalities, as featured via a service-neutral network design. Although not

[689] It is note-worthy that this remedy addresses all "undertakings that control access to end-users" regardless of the market power of the undertakings in question.

reflected in the finalised version, a stronger NGN-based implication could be derived from the EECC Proposal, which envisaged that SMP undertakings could be required:

> "to provide specified services needed to ensure interoperability of end-to-end services to users, including facilities for *software emulated networks intelligent network services* or roaming on mobile networks."[690]

As 'software emulated networks' have a self-standing nature and outreach the *virtual network services* or *software systems* referred to under the EECC, one could interpret the Commission proposal not being reflected in the EECC as a missed opportunity. This is particularly true as prospective NGN players would no longer act just as a telecom operator, but potentially as the controller of an IP ecosystem embodying software-governed service layers e.g. access, cloud and CDN, and in collaborations with content providers. Hence, intelligence in this context relates to a privately governed IP network, going beyond the conventional wisdom of interoperability or 'end-to-end connectivity' which the ECRF is primarily focused on.

On the other hand, the regulatory focus in the NGN context, would mean sharing of the SMP operators' proprietary protocols that govern their network functionalities. As a globally standardized IP-based multimedia communications system replacing circuit-switched networks seems to be a far-fetched possibility, it is important to both stimulate the development of NGNs and have some safeguards to pre-empt the anti-competitive effects that would result from market imbalances. Incorporating NGN interoperability within this broader context emerges to be a part of the regulatory puzzle.

690 EECC Proposal, art 71(1/f).

In the NGN based transition, market players will face lessened number of interconnection nodes,[691] whereas they might experience new digital gateways which are less standardised and much more controlled by the incumbents. Therefore, both the European Commission and NRAs may have to ensure that interconnection is possible at specific functional levels i.e. transport and service levels, in a reasonable, non-discriminatory and transparent manner. In fact, they ought to consider that operators having market power may not have an incentive to open up their networks to competition at the service level, with a view to limiting the use of emerging NGN capabilities, which potentially affects the ability of independent service providers to integrate their services into the NGN platforms.[692]

Against this background, a broader perspective ideally needs to be upheld concerning ICT interoperability, encompassing not only physical and logical interconnection requirements but also more complex vertical/horizontal interconnectivity problems. However, neither the EECC nor broadly speaking the ECRF, mirrors this viewpoint. Although acknowledging that "[i]nteroperability is an evolving concept in dynamic markets",[693] the ECRF's perspective is mainly concerned with how to solve the infrastructural problems. Having said that, the ECRF appears to consider 'interoperability' as a subordinate problem to be managed through the available tools, i.e. standardisation, access and interconnection remedies, with an emphasis on the bottom layers in the IP stack.

691 See Reichl and Ruhle (n 143) 50.

692 See the ERG, Final Report on IP Interconnection, Project Team on IP - Interconnection and NGN, (2007) ERG (07) 09, 23-25, <https://www.berec.europa.eu/doc/publications/erg_07_09_rept_on_ip_interconn.pdf> accessed 9 October 2020.

693 EECC Directive, recital 305.

6.2.2. Introduction of new ECS categories and the reach of interoperability problems

6.2.2.1. OTT Impact and a new carve-out under the EECC

As mentioned above, the EECC has introduced new categories of electronic communications' services (ECSs), and this new categorisation reaches out to internet-based over-the-top (OTT)[694] services. Having said that, the EECC revitalised the existing regulatory structure along with a rather light-touch regulatory treatment of the OTT services. While the introduction of new service types might not be conceived of as a revolution because of the limited expansion, the EECC addressing the long-debated OTT issue and related interoperability challenges is worth being elaborated.

OTT apps and business models, taking advantage of the global internet, are offered mostly by the global companies i.e. Facebook, Microsoft and Google and, albeit to a small extent, by local companies which often target niche markets and limited customer bases. OTT companies, while serving their customers increasingly on the global scale, pose a competitive threat over the telco companies (telcoes). In contrast to the latter, the former have no physical network infrastructure and offer their services through broadband access networks which are run over the nationally managed electronic communications networks. The big contrast between the telcoes and the OTTs is in consumers being charged with no or a minimum fee by the latter. While they offer their apps and services often with no cost to the end-users, they run ads over their one, or usually multi-sided, platforms. They make a profit through the strategy of

[694] OTT refers to "video, voice and other services provided over the Internet rather than solely over the provider's own managed network" (OECD, *Communications Outlook 2013* (2013) <http://www.oecd.org/sti/broadband/oecd-communications-outlook-19991460.htm> accessed 9 October 2020).

making each side of the platform meet, namely the consumers on the one hand and advertisers / businesses on the other.

Despite the OTTs having no infrastructure deployment, the wide-ranging communication,[695] entertainment[696] and social networking services being offered by these players increasingly arouses a tension between such OTT players and the telcoes. The so-called tension mainly results from the fact that OTT business models potentially affect the traditional revenue streams and profit levels of the telcoes. To illustrate, OTTs like WhatsApp threaten the SMS revenues of mobile operators, and Voice over Internet Protocol (VoIP) services like Skype or Viber threaten their voice revenues.[697]

It is widely acknowledged that the ubiquity of OTT apps for communications, messaging and social media has made the traditional revenue model for telcoes unsustainable.[698] Combining internet access, communications and media services in a more valuable manner, these apps, while replacing the formerly vertically integrated services by telcoes,[699] also raise the risk of obsolescence of the current regulatory rules. Against the dynamic needs of ICT users and new business models including OTTs, the regulatory focus on the traditional carriers has been debated for over a decade, with some regulatory implications concerning OTT players as well. This global agenda has also influenced the European regulatory politics, ending up with some reflections on

695 Communication services by OTTs may partly replace services by traditional providers of electronic communications, but also offer new and differentiated services such as voice calls, which are not part of the conventional package of services offered by traditional providers (Peitz and Valletti (n 94) 899).

696 Real-time entertainment by OTTs contains on-demand entertainment involving viewing or listening, whereby audio and video may be streamed or buffered (Peitz and Valletti (n 94) 899).

697 Richard Feasey, 'Confusion, denial and anger: The response of the telecommunications industry to the challenge of the Internet' [2015] 39(6) *Telecommunications Policy* 444, 445.

698 Peitz and Valletti (n 94) 901. A recent study produced for incumbent telecommunication operators suggests that, for example, cashflow within the European telecommunications industry will almost halve, falling from €44bn to €23bn by 2020 (Feasey (n 697) 446).

699 Peitz and Valletti (n 94) 907.

new regulatory burdens to be imposed on the online communication service (OCS) providers, namely OTT players.[700]

European legislators, considering that a growing convergence between OTT players and ECS providers exists, seems to have triggered a more equivalent regulatory response between them. Not for all the regulatory purposes, but mainly from the consumer protection viewpoint, a number of modifications were covered by the EECC. Based on not purely technical but more on economic reasons i.e. substitution, ECS and OCS providers were considered to have comparable features. Notwithstanding, OCS providers, e.g. WhatsApp, Skype and Viber, cannot fully control access to the end-users. More explicitly, they cannot fully control the signal when it is carried over the 'best-effort' access network.[701] Despite these technical points, OCS providers are widely acknowledged to offer equivalent communications services with ECSs, as reflected in the EECC.

According to the EECC, not only ECS but also OCS based voice communication services are covered within the definition of 'inter-personal communications services' (ICSs).[702] Thereby, both of these services have been exposed to regulatory control,

---

700 These reflections could be found in several recent reports. See ECORYS and TNO, *A study on future trends and business models in communication services* (Final Report: A Study prepared for the European Commission DG Communications Networks, Content & Technology, 2016) ('2016 OTT Report') 141-9; ITU Telecommunications Development Sector, *Regulatory Challenges and Opportunities in the New ICT Ecosystem* (Regulatory and Market Environment, 2018) 25-26 and 51. See also CERRE, 'Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets' (CERRE Study, 2014) 53-55 <https://www.cerre.eu/sites/cerre/files/141029_CERRE_MktDefMktPwrRegInt_ECMs_Final.pdf> accessed 9 October 2020.

701 2016 OTT Report, 28. OCS providers can, to a certain degree, control the conveyance of their signals with a combination of CDN servers and client software on client terminals; however, the actual degree of control depends on the degree of congestion in the 'best effort' access networks (2016 OTT Report, 28).

702 Under the EECC, 'interpersonal communications service' is defined as "a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service" (EECC Directive, art 2(5)).

albeit with significant differences. That is to say, a more light-touch regulation is envisaged for the OCSs, whereas ECSs are meant to be regulated under heavy-handed access regulations, as mentioned above. Before delving into the details of the newly envisaged obligations of OCS providers, it is important to draw the whole picture of ECSs, including different types of OCSs i.e. number-based and number-independent.

6.2.2.2. Introduction of new ECS categories

In the original (2002) form of the ECRF, an 'electronic communications service' was defined as a service normally provided for remuneration which consists *wholly or mainly in the conveyance of signals on electronic communications networks*.[703] According to this definition, an ECS simply meant "conveyance of signals on electronic communications networks" in return for a remuneration, reflecting on the distinction between 'transmission' and 'content'. As described above, the main thrusts and access remedies were designed according to this distinction by which an infrastructural vision is embedded within this framework.

While this regulatory mindset is still being kept on, an important change has taken place regarding the definition and categories of an ECS. According to the EECC, an 'electronic communications service' (ECS) means a "service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:

[703] Framework Directive, art 2(c). This definition "exclude[s] services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks" (Ibid).

(a) ‘internet access service’ as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;

(b) interpersonal communications service, and

(c) services consisting wholly or mainly in the conveyance of signals, such as transmission services used for the provision of machine-to-machine services and for broadcasting”.[704] According to this renewed definition, an ECS will contain;

(i) internet access services (IASs),

(ii) inter-personal communications services (ICSs), encompassing two sub-categories of number-based and number-independent, and

(iii) services consisting wholly or mainly of the conveyance of signals, e.g. M2M transmissions.

The abovementioned new categorisation reveals a diversion from the criterion ‘conveyance of signals’ in defining an ECS. While the formerly acknowledged ECSs supposedly meant IASs, number-based ICSs and M2M broadcasting transmissions based on the referred criterion, the EECC includes number-independent ICSs into the scope of ECSs as well. While M2M transmission is worth being elaborated separately, it is important to emphasize here that ICSs are grouped into two, by looking at whether end-users are assigned numbers by the service provider. ICSs being offered to customers on the basis of the assigned geographical or non-geographical numbers means a lower threshold for ex-ante regulation, compared to number-independent ICSs.[705]

---

704 EECC Directive, art 2(4).

705 See the EECC Directive, recital 18, reading as follows:

> Number-independent interpersonal communications services should be subject to obligations only where public interests require that specific regulatory obligations apply to all types of interpersonal communications services, regardless of whether they use numbers for the provision of their service. It is justified to treat number-based interpersonal communications services differently, as they participate in, and

Another key aspect of the new classification is the issue of 'remuneration' that diverges from the classic monetary relationship between the parties. According to this, it is acknowledged that ECSs "are often supplied to the end-user not only for money, but increasingly and in particular for the provision of personal data or other data. The concept of remuneration should therefore encompass situations where the provider of a service requests and the end-user knowingly provides, personal data within the meaning of Regulation (EU) 2016/679 or other data directly or indirectly to the provider."[706]

Finally, as long as "the interpersonal and interactive communication facility is a minor and purely ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing electronic communications services", one could not mention about a number-based ICS, or broadly speaking an ECS.[707] This is to pre-empt all types of OCS-enabled services and products from being taken as an ECS, although many of them would make it possible for their users to communicate with each other through VoIP. While the thrust behind this delimitation seems to create a boundary between the mainstream OCSs and others that make use of 'interpersonal and interactive communication' as "a minor ancillary feature", it seems hardly possible to set out the intended boundaries against the dynamic nature of future communication means, technologies and devices.

hence also benefit from, a publicly assured interoperable ecosystem." (EECC Directive, recital 18).

706 EECC Directive, recital 16.

707 EECC Directive, recital 17.

6.2.2.2.1. Number-independent inter-personal communications services

As mentioned above, if an undertaking provides ICSs based on the numbers assigned according to a national or international numbering plan, then it is assumed to provide number-based ICSs within the meaning of the EECC. On the other hand, all of the online communications services (OCSs) provided by ICS providers are not necessarily affiliated with a geographical or non-geographical number. Whereas number-based ICSs are usually provided by conventional telcoes, Skype, WhatsApp and Viber and many other OCS and OTT providers could be assigned numbers as they wish within the context of a national or international numbering plan.

According to the EECC, number-based ICS providers are to be treated the same as other ECS providers, e.g. telcoes, concerning a number of issues relating to consumer protection, which incorporate certain contractual, technical and administrative standards. For instance, according to Article 109(2) of the EECC, providers of number-based ICSs have an obligation "to provide access to emergency services through emergency communications to the most appropriate PSAP [public safety answering point]".[708] Bundle-related requirements, e.g. relating to the extension of subscription periods, are likewise imposed on number-based ICS providers, as well as IAS providers, according to Article 107 of the EECC. Last but not least, it is established that providers of number-based ICSs should respect the end-users' decision when making data available to directory service providers.[709] Exceptionally, information

[708] EECC Directive, art 109(2). See also the EECC, recital 286. NRAs are supposed to require number-independent ICS providers to provide emergency services insofar as a PSAP is accessible to such service providers. See ibid, reading; "Where such standards and the related PSAP systems have not been implemented, network-independent number-based interpersonal communications services should not be required to provide access to emergency services except in a manner that is technically feasible or economically viable" (EECC, recital 286).

[709] EECC Directive, recital 300, art 112.

requirements for contracts are arranged as to address all the ICS providers comprising both providers of number-independent ICSs and IASs.[710]

As stated above, number-independent ICS providers are treated more lightly than number-based ICS providers are treated under the EECC. Except with a few contractual obligations mentioned above, i.e. information requirements, number-independent ICS providers are only subject to generic security obligations as per Article 40 of the EECC.[711] Number-independent ICS providers do not have any other ex-ante obligation directly imposed by the EECC, apart from those specified above, i.e. under Articles 40, 102 and partially 109. On the other hand, an exceptional remedy is envisaged under Article 61(2/c) of the EECC. According to this provision, such undertakings could be subject to an obligation:

> "in justified cases, (⋯) to make their services interoperable, namely where access to emergency services or end-to-end connectivity between end-users is endangered due to a lack of interoperability between interpersonal communications services."[712]

---

710 EECC Directive, art 102. Service providers addressed in Article 102 of the EECC are phrased as "providers of publicly available electronic communications services other than transmission services used for the provision of machine-to-machine services".

711 Article 40 of the EECC Directive titled 'Security of networks and services' reads as follows:
1. Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services.
2. (…)
3. Member States shall ensure that in the case of a particular and significant threat of a security incident in public electronic communications networks or publicly available electronic communications services, providers of such networks or services shall inform their users potentially affected by such a threat of any possible protective measures or remedies which can be taken by the users.

712 EECC Directive, art 61(2/c).

Hence, in the event of an actual threat to end-to-end connectivity or to effective access to emergency services, the Commission and where necessary the relevant NRA, may identify a need for measures to ensure interoperability, for instance through a standardisation process.[713] This regulatory prospect means that OCS and OTT providers, e.g. Skype, WhatsApp and Viber, will potentially be exposed to the abovementioned measure(s) should their consumers face problems with regards to "access to emergency services or end-to-end connectivity" resulting from the lack of interoperability. This is a note-worthy regulatory step towards ensuring the interoperability of upper layer applications and services, going beyond traditional telecommunications networks[714] and the conventional wisdom of infrastructural regulation.

Against this background, ensuring 'end-to-end connectivity' appears to be the main policy driver for ICT interoperability, being adjusted and expanded in view of accompanying reasons, i.e. access to emergency services, that would warrant public policy interventions. Notwithstanding, this expansive step would be deemed incomplete in view of the ever-growing convergence between the OCSs and OTTs and conventional ECSs. As a matter of fact, around 3% of the global OCS users are encompassed by the definition of inter-personal communications services,[715] and the multiple criteria for interoperability-centric interventions would not effectively comprehend the everyday expanding ICT world with all its constituent dynamics.

713 EECC Directive, recital 150.
714 Unver (n 30) 108.
715 Cornelia Kutterer, 'Future Models for Service Regulation - Implications for OTTs, Telcoes and Consumers' (WIK Conference: New rules for digital networks and services?, Brussels, 18 October 2016).

6.2.2.2.2. M2M transmission services

As mentioned above, M2M transmission represents another new ECS category within the meaning of the ECRF. Under the EECC, "services consisting wholly or mainly of the conveyance of signals, such as transmission services used for M2M communications and for broadcasting" are set out as the third ECS category, alongside ICSs and IASs.[716] If not the same as ICS or IAS providers, undertakings which offer M2M transmission to the consumers, e.g. either using mobile numbering codes (MNCs) assigned to themselves or relying on third party MNCs, are subjected to ex-ante regulation for certain purposes, e.g. network security. This new service cluster comes up with not only responsibilities but also with more rights, along with a more IoT (M2M) friendly legal environment.

This EU approach seems to have arisen in view of the challenges as well as the opportunities brought about by the IoT services, which rest on broadband connectivity as well as other inputs, e.g. smart devices, clouds and microprocessors. Usually, Subscriber Identity Module (SIM) cards are distributed by the mobile operators to M2M providers, e.g. gas and electricity suppliers, thermostat manufacturers and smart car producers, which do not normally capture the management of SIMs that are embedded into the M2M devices, e.g. smart meters. Based on the idea of transferability of this management to M2M providers, the EECC's policy approach envisages that M2M providers will be able to manage MNCs, according to the numbering plans of the relevant countries. By then, it is expected that M2M providers can easily manage their subscribers, have a closer contact and marketing approach from having the ability to differentiate their products e.g. with possible advantages like multi-network roaming.

716 EECC Directive, art 2(4/c).

Going beyond the management of MNCs, M2M providers might step forward having their virtual networks. In such a case, they will be able to act as authorised ECS providers as long as they meet the required standards under the ECRF. This means M2M providers, which represent the IoT providers utilising cellular networks, will then be an ECS provider of a separate status, according to the EECC. This is a real and would-be common scenario as the IoT networks will potentially become more prevalent in our daily lives with a greater interplay with electronic communications networks and services. Given this fact, the IoT/M2M providers might consider running separate networks as a feasible option and opt to have and govern their network facilities rather than relying on a hosting network.

Although having a physical or even virtual (hosted) network offers the full potential to solve numbering related problems, such problems would not be fully dismissed under other scenarios where the IoT service providers have limited management capabilities over their subscribers. In the scenarios where M2M providers do not have fully-fledged MNC management i.e. because of contractual and/or network-related constraints with the network operators, their customers will eventually face switching difficulties while they wish to port their SIMs across the mobile networks. Another noticeable fact behind this situation is that number portability is not possible on a technically convenient and widely applicable basis in such scenarios, unlike the mobile number portability which individual mobile users currently benefit from.

Against this background, the EECC implicates a solution called ‘over-the-air (OTA) provisioning of numbering resources’ based on industry implementations.[717] OTA

[717] The GSMA89 has specified a mechanism for the remote provisioning and management of embedded SIMs, allowing OTA provisioning and enabling the change of subscription from one connectivity service provider to another. This mechanism has been designed to answer the IoT

provisioning of numbering resources enables the reprogramming of communications equipment identifiers without physical access to the devices concerned.[718] By this means, switching would no longer be a problem for the M2M providers and users when they opt for changing their connectivity (ECS) providers. According to the EECC,

> Without prejudice to Article 106, Member States shall promote over-the-air provisioning, where technically feasible, to facilitate switching of providers of electronic communications networks or services by end-users, in particular providers and end-users of machine-to-machine services.[719]

Should OTA provisioning be adopted widely as encouraged by the EECC, M2M providers would easily have their SIMs changed across the mobile network operators with remote controlling. Assuming many M2M providers will not have their networks, this solution would be helpful for them switching with no or minimum cost. This will undeniably help the development of M2M services on a larger scale although infrastructural, legal and regulatory conditions would differ among Member States. On the other hand, this solution, which seems to be a technologically oriented measure, does not cover non-cellular network options. It also seems that data-related constraints, e.g. portability of the IoT data, and interoperability problems, e.g. compatibility of the IoT hardware and software, are kept outside of the regulatory vision contemplated by the EECC.

---

needs where SIMs may not easily be changed manually (BEREC Report (n 31) 31). See also OECD, *The Internet of Things: Seizing the benefits and Addressing the Challenges* (Background report for Ministerial Panel 2.2, 2016) 43.

718 EECC Directive, recital 249.

719 EECC Directive, art 93(6).

While M2M providers or users switching between connectivity service providers, e.g. mobile operators, is envisaged by the EECC, facilitating migration of IoT providers/users from one software-governed platform to another is not mandated or encouraged. In this regard, lack of common standards enabling interoperability between the IoT platforms would be a barrier for competition, having the potential to prevent or delay new entries to the market. In addition to this, data portability constraints that would hamper transferability of the IoT data from one platform to another should be added as another problem closely associated with interoperability. Summing up, the ECRF seems to be incomplete and potentially overridden by the running pace and dynamics of the IoT markets, considering that the abovementioned problems surrounding the lack of interoperability would affect a competitive marketplace, despite the envisaged solutions, e.g. OTA provisioning.

6.3. Assessment of the ECRF

The ECRF, starting from the liberalisation period in the nineties, was built on the idea that elimination of monopolies, either public or private, would ensure a competitive market resulting in the benefits to be reaped by the end-users. To that end, European policy makers mandated Member States to remove the special and exclusive rights conferred onto the legal monopolies and enacted harmonization directives with a view to ensure a competitive telecommunications landscape. Until the adoption of the 2002 regulatory framework, the main concern was related to ensuring adequate and effective interconnection along with the required level of interoperability being achieved towards pan-European networks and services. This perspective, while being kept on, has been extended to other areas of ex-ante regulation, including conditional access to the set-box systems. Access to wide-ranging network facilities, e.g. local loops, civil

engineering ducts and inbuilding wiring, are incorporated within the potential access remedies to be imposed by NRAs for competition purposes.

Albeit with the acknowledgment that "interoperability is of benefit to end-users and is an important aim of this regulatory framework",[720] the ECRF's vision was to date, and still is, far more elaborated regarding the assessment of infrastructural problems. Although having a deepening perspective, the regulatory approach pursued by the European authorities is by and large kept within the boundaries of access, interconnection and leased lines markets.[721] Mainly based on the SMP regime, this regulatory vision aims at creating more competitive markets by means of access and/or price obligations formulated and designed according to the new entrants' needs. While interoperability-centric remedies also have a stake in this context, such remedies appear narrow and limited largely because of the infrastructural perspective envisioned by the ECRF. Notably, it appears that achievement of interoperability is viewed as more of a supplementary remedy towards the ascertained goals of the ECRF, i.e. promotion of competition, promotion of the interests of the EU citizens, end-to-end connectivity, and to a lesser extent, media pluralism and cultural diversity.

The last milestone towards the so-called policy objectives has been set out by the EECC, through an overhaul over the ECRF in a number of ways, including by expanding the regulatory vision towards software-governed, mainly online communications, services. First and foremost, it is proposed that ECSs are re-

720 EECC Directive, recital 148.

721 In this regard, the number of retail markets susceptible to ex ante regulation denotes a decreasing trend, whereas wholesale markets to be regulated have kept their importance revolving around broadband or local access, leased lines, mainly terminating segments and interconnection, mainly call termination, which are assessed to far better demonstrate enduring entry barriers, etc. The so-called trend could be observed throughout the period from 2003 to 2014 when 3 recommendations were issued by the Commission (See supra note 651).

categorised as to cover ICSs and M2M transmission in which the former is subdivided into two: (i) number-based ICSs, (ii) number-independent ICSs. Plus, according to this new categorisation, number-independent ICSs as usually being offered by the OTT players such as Facebook, Skype and Viber will be the subject matter of a limited number of obligations. In this regard, OTT interoperability is earmarked as one of the front-line topics, revealing a potential area of intervention, i.e. by means of standardisation, to respond to the end-user needs based on 'end-to-end connectivity' or 'access to the emergency services'.

Given the fact that number-based ICSs constitute a very small percentage of the software-governed OTT services,[722] OTT-based regulatory expansion denotes more of a fine-tuning rather than a radical change. Furthermore, a serious and elaborated regulatory response to NGN including interoperability aspects could hardly be found under the EECC. Nor such a repercussion could be mentioned with regards to many other ICT networks and services, including cloud computing that entails many significant aspects of ICT service provisioning, i.e. virtualisation, multi-purpose capacity allocation and data processing. On that point, it is note-worthy that European policy makers still consider lack of interoperability and accompanying problems as a subordinate topic within the overall regulatory structure. Not only the ECRF's limited scope, but also the partial and limited interoperability obligations thereunder point to a narrow-minded perspective.

Having said that, the ECRF continues to have a regulatory vision focused on the bottom infrastructural layers. However, handling infrastructural problems under the ECRF, but putting other, upper-layer problems aside would not be in harmony with

722 See supra note 715.

the real-life challenges surrounding IP-based convergence. The ECRF's vision comes from the past experiences of ex-ante regulation revolving around how to liberalise formerly monopolised markets and make them competitive. A deeper analysis should be done that incorporates other ICT services than ECSs and notwithstanding the regulatory expansion brought with the EECC. In so doing, a layered and holistic approach encompassing all the IP layers and refraining from the infrastructural focus, needs to be considered first and foremost. It is noticeable that upper layer markets have undergone their infancy and were kicked-off to grow, while telecommunications (lower layer) markets have so far been under heavy regulation. While developmental difference between the former and latter is in favour of the former,[723] their convergence has remarkably increased in time, also with greater implications for interoperability.

In the so-called IP world, the convergence process has in reality been dominated by a process of the delivery of more and more communication services in the internet,[724] often led by the upper-layer, the IT-intensive, software-governed services. With OTT, the internet is seen as the generic platform for the provision of broadcast content and the associated advanced services, regarding for instance the integration with social networking and community services taking advantage of the proven dynamics and huge innovation potentials of the internet.[725] That is to say, internet-driven software markets, or broadly speaking the upper layers, have a transformational power over the

723 See also Plantin, Lagoze, Edwards and Sandvig (n 669), 299-301. This situation made the so-called upper layer ICT markets unfettered from any regulatory burden and arguably enabled them to grow more rapidly in comparison with the electronic communications or telecom markets (Anders Henten and Reza Tadayoni, 'The dominance of the IT industry in a converging ICT ecosystem' in Hitoshi Mitomo, Hidenori Fuke and Erik Bohlin (eds), *The smart revolution towards the sustainable digital society: Beyond the era of convergence* (Edward Elgar 2015) 31.

724 Henten and Tadayoni (n 723) 19.

725 Henten and Tadayoni (n 723) 28.

convergence process ongoing between telecom, media and IT markets. While IT markets predominantly lead the IP convergence,[726] the increasing interdependencies and interrelationships between the infrastructural and software-governed markets should drive new paradigmatic thinking to be translated to the regulatory sphere.

Considering the case studies below will help re-examine the convergence process and the interoperability dynamics, suffice it to say here that the IP convergence, based on the cross-layer relationships, has an increasing role to play in ICT regulation including interoperability aspects. Having said that, the so-called interdependencies between the IP layers require more attention, as they would potentially pave the way for review of the conventional wisdom concerning ex ante regulation.

Summing up, interoperability-centric problems, with some regulatory exceptions given above, are happened to fall under the realm of competition law in the EU legal system. This would automatically mean that market stakeholders will have to await the results from the competition law decisions, and relevant problems will have to be worked out in between such results and industry led solutions. While the current situation under the ECRF whereby a secondary role is conferred to interoperability should not self-evidently justify expanding the regulatory vision, the interdependencies and interrelationships between the ICT markets and players require a more elaborate and in-depth analysis. Given this fact, the chapter below is dedicated to the case studies based on cloud computing and the IoT reflecting on the real-life scenarios, industrial solutions and interdependencies.

[726] Henten and Tadayoni (n 723) 30-32.

7. Case studies: Cloud computing and the Internet of Things

7.1. Cloud computing

7.1.1. Definition, main characteristics and featured models

Cloud computing denotes a modern IT infrastructure in which part of the software or hardware resources are not in the hands of the user but are located on some remote servers and accessible through the internet.[727] Such servers are placed in the cloud centres, which host third parties' data, software and applications, comprising the cloud resources that constitute 'cloud computing' along with the necessary deployment, maintenance and management. A common definition of 'cloud computing' made by National Institute for Standards and Technology (NIST) describes 'cloud computing' as a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources e.g. networks, servers, storage, applications and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction".[728]

Cloud computing applies a utility model to produce and consume computing resources, in which the cloud abstracts all types of computing resources, including storage and as services i.e. cloud services.[729] The cloud user, either application developer or consumer, can access the cloud services over the internet, and the cloud users pay only

727 Bartolini, Santos and Ullrich (n 332) 361.

728 National Institute for Standards and Technology (NIST), US Department of Commerce, The NIST Definition of Cloud Computing (Recommendations of the National Institute for Standards and Technology, Special publication 800-145) 2011, 2.

729 Jiehan Zhou, Teemu Leppänen, Erkki Harjula, Mika Ylianttila, Timo Ojala, Chen Yu, Hai Jin, Laurence Tianruo and Yang Huazhong, 'CloudThings: A Common Architecture for Integrating the Internet of Things with Cloud Computing' (2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design, 27-29 June 2013) 651.

for the time and services they need.[730] Geographically dispersed users' requests, including for the necessary software updates, are met by the cloud (computing) providers in an efficient and customised manner. Resource pooling and rapid elasticity brought by the cloud computing respond to various demands in numerous settings i.e. big data management, the IoT and/or AI-driven services. Accordingly, from basic IT needs e.g. data storage, security and reducing the upfront costs, to advanced levels of utilisation, cloud computing has become a significant driver and part of running businesses in the digital world.

In an increasing fashion, cloud computing constitutes an integral part of the current ICT ecosystems, underlying a significant sphere of the digital economy. As an ever-faster-growing trend, enterprises rely on cloud computing in building and/or running their businesses, considering this either as a way to more efficiently provide their services and/or for storage and/or back-up purposes. This intensive demand is clearly shown by Cisco's forecast that by 2021, 94% of workloads and compute instances will be processed by cloud data centres, whereas 6% will be processed by traditional data centres.[731] It is also note-worthy that, cloud networks and services have a significant role in retrieving, processing and analysing data from various resources in the era of big data. Based on the diversification of user needs, a number of service and deployment models have so far emerged along with key and distinctive features.

Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) are the main categories that denote *service* models. Among these, IaaS

730 Ibid.

731 Cisco, *Cisco Global Cloud Index: Forecast and Methodology* (2016–2021 White Paper, November 19, 2018) ('Cisco 2018 Global Cloud Index') <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html> accessed by 9 October 2020.

is the most flexible model for the cloud users who are allowed to optimise their IT needs based on the networking, virtualised servers, OS, security and storage offered by the cloud (IaaS) provider. In this model, all physical servers and networking elements are virtualised, allowing the users to deploy their software tools, applications, databases, etc. These computing powers are increasingly embedded into the software infrastructure of the clouds, when moving to PaaS and SaaS. In the PaaS model, cloud users are offered web servers, development tools and databases through which they can run their own applications. Such cloud resources are also-called the 'system middleware', giving users the flexibility to manage the application parameters, while the control of the underlying infrastructure e.g. OSs and networking is kept on by the cloud provider. In the SaaS model, all the computing resources e.g. from the underlying hardware and software to the running applications, are purchased from the cloud provider. SaaS providers install, maintain and update software within the cloud back-end, and users' access to the software is managed through the internet, or intranet, via client devices, PCs, etc.[732] Therefore, in this model, the maximised control of the cloud providers is exchanged with the lessened flexibility on the part of the users.[733]

Alongside the service models, four types of *deployment* models are widely acknowledged that reflect the global needs of the users and enterprises. 'Private

---

732 Below are given the examples for cloud providers that rely on particular service models:
- SaaS examples: Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting,
- PaaS Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift,
- IaaS Examples: DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

(Stephen Watts, 'SaaS vs PaaS vs IaaS: What's the difference and how to choose?' (BMC Blog, 22 September 2017) <https://www.bmc.com> accessed 9 October 2020).

733 For further details of the service models, see Christoph Fehling, Frank Leymann, Ralph Retter, Walter Schupeck and Peter Arbitter, 'Cloud Computing Patterns: Fundamentals to Design, Build, and Manage Cloud Applications' (Springer, 2014) 42-59; Kai Hwang, Geoffrey C. Fox and Jack J. Dongarra 'Distributed and Cloud Computing: Form Parallel Processing to the Internet of Things' (Elsevier 2012) 191-206.

clouds' are operated on the basis of meeting individual client demands with the dedicated hardware and software, whereas 'public clouds' are managed to meet the general public's demands. In the case of 'community clouds', the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns e.g. mission, security requirements, policy and compliance considerations.[734] Finally, the 'hybrid cloud' infrastructure is a composition of two or more clouds, private, community or public, that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability e.g. cloud bursting for load-balancing between clouds.[735]

7.1.2. Technical and economic underpinnings

While the existing platforms, software and applications could be run by the users more efficiently and easily in the cloud environment, behind the scene lies a very complicated back-end. In this back-end, lies an assembly of the hardware and software elements from different resources, ending up as a distinct composition and organisational structure. These architectural components also refer to the economic underpinnings of cloud computing.

Technically speaking, the essential concept of cloud computing is that IT resources are made available within an environment that enables them to be used, via a communications network, as a service.[736] Having said this, cloud-based storage, security, processing, messaging and reporting are offered to the users by the cloud

---

734 Ahmed Shawish and Maria Salama, 'Cloud Computing: Paradigms and Technologies' in F. Xhafa and N. Bessis (eds), *Inter-cooperative Collective Intelligence: Techniques and Applications, Studies in Computational Intelligence* (Springer-Verlag Berlin Heidelberg, 2014) 49.

735 Ibid. For further details of the deployment models, see Hwang, Fox and Dongarra (n 665) 192-194.

736 The Open Group, 'Cloud Computing Portability and Interoperability' <http://www.opengroup.org/cloud/cloud_iop/p3.htm> accessed 9 October 2020.

provider, whereas the physical link between the user and the cloud provider is secured by the ECS providers (ISPs). Furthermore, cloud-based content is often delivered to the end-users through content delivery networks (CDNs) that are deployed in premises closer to the end-users with the aim of high-speed delivery of content to the geographically-dispersed end-users.[737] These external elements underlie and complement the cloud infrastructure, assuring the intended usages and benefits from cloud computing. Representing the constituents of evolving supply structures and ecosystems, such internal and external elements are analysed below.

7.1.2.1. Cloud layers and components (internal elements)

While cloud providers mainly aim for the provision of cloud resources to third parties e.g. individual users, commercial enterprises and software developers, each constituent layer has a key role, like a building block, in the supply of cloud services. For instance, the web servers, databases and development tools function as the core of the cloud platforms without which software developers could not create and manage their own applications in the cloud environment. Likewise, in the absence of 'virtualisation', which enables multiple users being served via the same servers, the intended results from clouds e.g. scalability and efficiencies could not be achieved. Virtualised servers, along with the related networking, mechanical and electrical facilities, constitute the 'infrastructure' layer that internally lays the ground for upper layer cloud services, namely the provision of platform and applications, including the necessary maintenance and upgrades. On top of the platform and application layers exists the application layer, which hosts the applications running for various purposes i.e.

[737] CDNs allow large content providers to bypass internet backbone networks when sending their content to users and have ushered in profound changes to how data flows over the internet (Daly (n 23) 42). For further details see infra note 743.

customer relationship management (CRM) and e-mailing. For such applications, when purchased by users, it is usually not known that they already rely on cloud computing. These *internal* elements not only represent the benefits unique to cloud computing but also constitute the key inputs used to create the cloud services offered to third parties and in drawing up the service models specified above. In Figure 8 can be seen these internal elements that constitute the cloud layers as well as the service models.

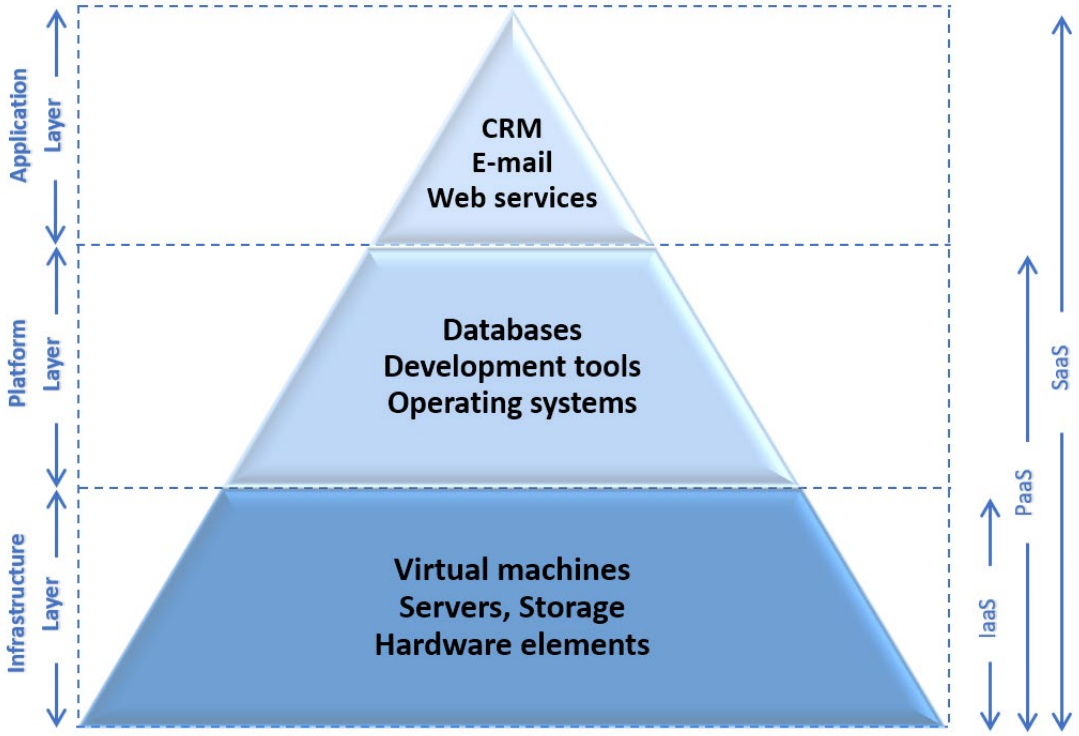

Figure 8: Cloud layers (internal elements)

Source: Constructed by the author

As can be seen in Figure 8, cloud computing consists of several layers functioning as the internal elements. This means a supply structure being managed by a single company, namely the cloud provider. Cloud providers offer services at different layers of the resource stack, simulating the functions performed by applications, operating

systems, or physical hardware.[738] However, these functions are internalised and abstracted within the service provision, and many of these are not visible to the cloud users.

While these internal elements are organised and managed by the cloud provider, this single-handed management does not mean lack of distributed expertise along the layers. That is to say, cloud components do not necessarily have to be created by the cloud provider and could be purchased from third parties and sometimes be outsourced as well. This usually happens because of different companies' expertise in the provision of related ICT services, i.e. virtualisation, networking (routers, switches) and security (anti-malware services), which are combined in the cloud environment in the end. The cloud supply structure is therefore argued to have been constituted from an array of firms whose products and services are complementary to each other.[739] While 'complementarity' has a role to define the relationships between the providers of such services, this is overshadowed by the single management over the internal elements on the part of the cloud provider.

7.1.2.2. Cloud ecosystem with external elements

While generation of the value chains in the cloud ecosystem depends on the effective combination of the cloud layers and components, the emergent cloud models could not be isolated from the underlying network elements. That is, the internal elements, the cloud layers and components, are complemented by the external elements, namely broadband network access and CDNs. As ubiquitous access to the cloud services is

738 Christopher S. Yoo, 'Cloud Computing: Architectural and Policy Implications' [2011] 38 Review of Industrial Organization 405, 408.

739 Tim Cowen and Annabelle Gawer, 'Competition in the Cloud: Unleashing Investment and Innovation within and across Platforms' [2012] 85 1st Q Digiworld Economic Journal 45, 47.

key to any viable cloud model, clouds inevitably rely on fixed e.g. fiber optic, cable and PSTN, and mobile e.g. GSM, UMTS and LTE networks. When the software and data reside in the cloud, the absence of a network connection has more serious consequences, effectively preventing end-users from running the cloud-native applications at all.[740] Although intranet-type closed models are imaginable, what makes the cloud's offerings much more appealing than its predecessors e.g. traditional data centres is the ability of the cloud users to have access to the cloud's resources over the internet, regardless of geographical and time-related constraints.

On the other hand, cloud computing is likely to increase the demands being placed on the local access network that is run by the ISPs, and the access network might not have sufficient bandwidth to support the mass utilization, particularly at the times of unanticipated spikes.[741] This latter issue confers a key role on the CDNs which complements the role of ISPs. Not only to deal with such traffic bursts and load balancing, but also to provide premium, seamless, uninterrupted, quality-guaranteed content delivery. CDNs are extensively used by the cloud, as well as content providers,[742] creating another layer underlying the cloud services.

A CDN takes content from a content provider (CP) and caches it on those distributed servers, which has two effects: first, content is brought closer to the end-user without passing through inter ISP peerings, thus making its delivery faster;[743] second, the CDN

740 Yoo (n 738) 414.

741 Yoo (n 738) 413.

742 In 2017, approximately 52% of all internet traffic crossed CDNs; and just in 2021, that number is expected to jump to 71% (Briana Lassig, 'CDN Technology: How Net Neutrality Will Affect Global CDNs' (*CDNetworks Americas*, 21 February 2018) <http://nl.cdnetworks.com/en/news/how-net-neutrality-will-affect-global-cdns/6811> accessed 9 October 2020).

743 Delivery of IP traffic occurs either through transit or peering agreements among the internet backbone operators and/or ISPs. While transit between these operators generally occurs because of the sizeable differences among the parties, peering takes place between two networks, mostly small ISPs', that have roughly the same size. For the definitions of transit and peering, along with

has a contractual relationship with the ISP as the former often needs to terminate traffic.[744] In this emergent ecosystem, along with additional value chains, clouds have an increasing role to play; yet this role is unthinkable without taking account of these external elements. For connected consumers, content and applications must be seamlessly accessible via a diverse range of mobile devices, and this requires 'cloud-delivered CDNs' as well as 'packet-optical infrastructure'.[745] While the former is realised by cloud services, the latter could be achieved via high-speed broadband access networks i.e. fiber-optic based NGA networks.

CDN providers e.g. Akamai and Limelight, while serving content providers according to their specific needs, would be collaborating with the upper or lower layer operators, namely cloud providers or ISPs. By collaborating with and/or purchasing services from the former, CDN providers would gain added values e.g. cloud security solutions and functionalities e.g. data analytics, to be incorporated into their distribution networks.[746] These complementary services have become more important as the marketplace for basic content delivery services has become more competitive and diverse.[747] On top

---

their regulatory implications concerning internet interconnection, see Rohan Kariyawasam, 'Telecoms Regulation - Peering and Transit Over TCP/IP Networks' [2001] 17(1) Computer Law & Security Report, 36-40; Kariyawasam (n 131) 185-204. While CDNs bypass these networks and agreements by delivering the content directly to the ISPs, they usually face the termination fees to be paid, which is comparable to the 'paid peering' option that is usually done between content providers and ISPs.

744 Thorsten Hau, Dirk Burghardt and Walter Brenner, 'Multihoming, content delivery networks, and the market for Internet connectivity' [2011] 35 Telecommunications Policy 532, 535.

745 Camille Mendler, *CDNs, the Cloud and Carrier Ethernet: The new golden triangle* (Informa, 2012) 9.

746 Thus, CDNs have a wide-ranging variety according to the services and functionalities offered by them. Not only web delivery and content caching but also distributed denial-of-service protection, web application firewalls and bot mitigation; web and application performance and acceleration services; streaming video and broadcast media optimization; and even digital rights management for video might be incorporated in differentiated CDN models (Margaret Rouse, 'CDN (content delivery network)' (*TechTarget*, 31 July 2014) <https://searchnetworking.techtarget.com/definition/CDN-content-delivery-network> accessed 9 October 2020.

747 Volker Stocker, Georgios Smaragdakis, William Lehr and Steven Bauer, 'The growing complexity of content delivery networks: Challenges and implications for the Internet ecosystem' [2017] 41(10) Telecommunications Policy 1003, 1006. For example, in 2015, Akamai generated more than half of its revenues from "Performance and Security Solutions" and cloud security solutions alone accounted for more than 11% of total revenues (Ibid).

of this, collaboration between CDN providers and ISPs i.e. through licensing agreements would enable new channels of scalability, traffic routing and network resourcing for the former.[748] These collaborative acts also support the ISPs expanding their networking capabilities. For example, ISPs with a limited geographic footprint cannot implement a CDN to serve global content providers unless they partner with other CDNs or ISPs.[749]

While CDNs are spread across the globe, ISPs' networks are restrained within geographical (national) territories. Their unmatchable scopes, as well as other distinctive functionalities, make these networks collaborate as well as competing indirectly with regard to content delivery and termination. As the clouds host a significant portion of the IP traffic[750] which transcends CDNs and broadband networks, there is an inherent link between such networks and cloud-based content delivery. From a broader perspective, transactions between these stakeholders are a reminder of the "symbiotic" relationships among the players across the layers, as argued by Fransman.[751] According to Fransman, the ICT ecosystem consists of six, or a simplified four, "layers" that interact with each other through symbiotic relationships.[752] From this viewpoint, the interdependencies between the internal and

748 Ibid, 1013.
749 Ibid, 1016.
750 According to Cisco's forecast for the period of 2016 to 2021, global cloud IP traffic will account for 95% of total data center traffic by 2021, and will be more than triple (3.3-fold) over the next 5 years with a 27% increase rate (CAGR) (Cisco 2018 Global Cloud Index).
751 Fransman (n 118) 13.
752 Ibid. The layers embedded in the ICT ecosystem are classified by him as to include 'networked elements', 'network operating', 'connectivity', 'middleware platforms', 'content, applications and services' and 'consumption'. Such layers, which are simplified by Fransman as to cover 'networked elements', 'network operating', 'middleware' and 'consumption' layers, have been refined by some scholars ending up with several regulatory models. See Rohan Kariyawasam, *International Economic Law and the Digital Divide: A New Silk Road* (Edward Elgar 2007) 87-117; Kariyawasam (n 107) 581-594; Werbach (n 118) 59-95; Joshua L. Mindel and Douglas C. Sicker, 'Leveraging the EU regulatory framework to improve a layered policy model for the US telecommunications markets' [2006] 30 Telecommunications Policy, 136-148; Richard S. Whitt, 'A horizontal leap forward: formulating a new public policy framework based on the network

external elements of the overall (cloud) ecosystem play a key role in understanding cloud computing and the possible inroads to regulatory pathways in cloud computing and broader contexts. The Figure 9 demonstrates all the relevant layers that encompass the overall (cloud) ecosystem.

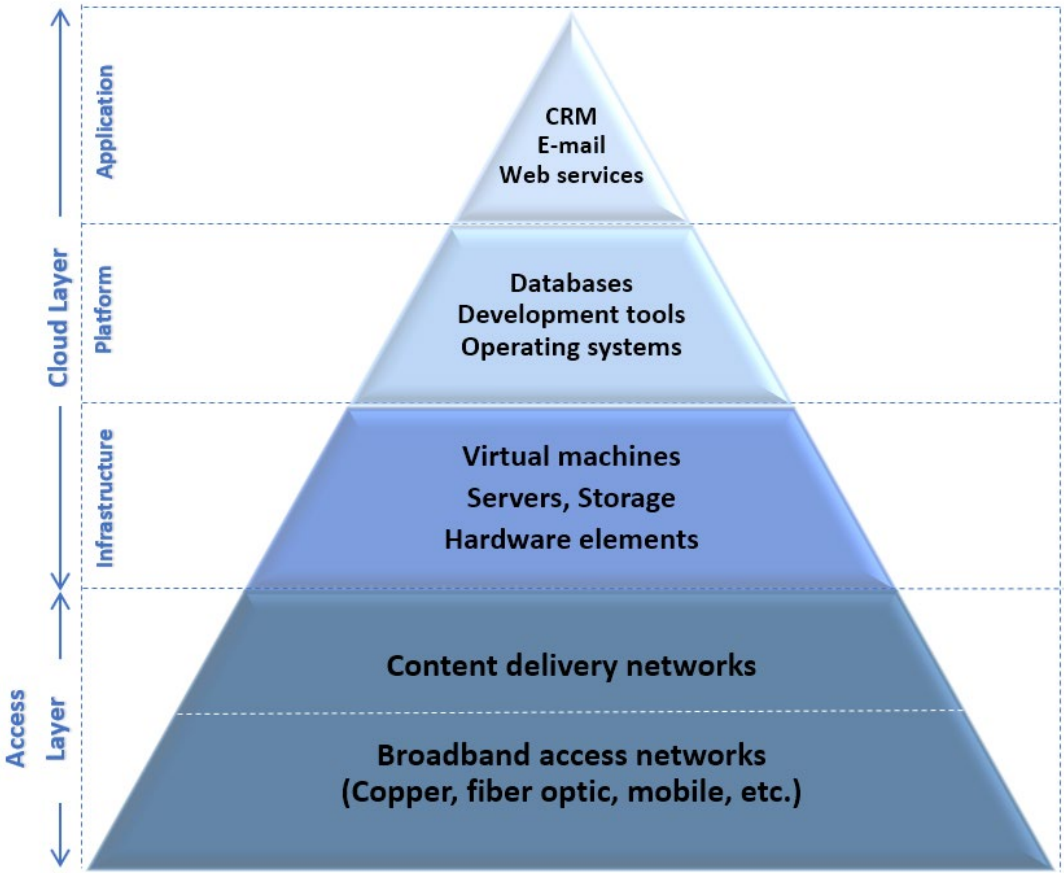

Figure 9: Cloud ecosystem (with internal and external elements)

Source: Constructed by the author

7.1.2.3. The differences and relationship between the organisational (supply) structures

As manifested in Figure 9, not only the cloud components, namely the 'internal' elements themselves, but also the 'external' elements which constitute the 'access

layers model' [2003] 56(3) Federal Communications Law Journal, 587-672. For further information and literature regarding layered models see supra note 118.

layer' denote a multi-layered structure. This structure is comprised of access and cloud layers including sub-layers and services, which all together constitute an ecosystem. Given this fact, the supply structure of the cloud environment, based on the internal elements, differs from that of the cloud ecosystem, based on both internal and external elements.

First and foremost, in the first structure solely based on the internal elements, the demand and supply equilibrium depends on the 'coordination' of the mainstream and complementary cloud services. More explicitly, SaaS, PaaS and IaaS type cloud services are offered by the cloud providers that create the environment whereby various software and hardware are coupled and managed by means of the so-called 'coordination'. To couple these internal elements, the cloud provider identifies the networking, storage, processing, maintenance, security and other needs and makes 'make-or-buy' decisions accordingly. In this vein, the relationship between the mainstream and complementary services is defined and managed by the cloud provider themselves. Upstream and downstream market relationships could emerge out of this coordination and management. Albeit with the difficulties regarding dynamic and allocative efficiencies in solving potential competition and regulatory problems, the decision-making processes could still be built on the traditional concepts and precedents i.e. market definition.

On the other hand, the same could hardly be concluded for the broader setting, namely when the external elements are embedded into the cloud environment. Primarily, the competition/regulatory lens in this setting needs to be more comprehensive and inclusive, not being limited to the cloud components. When including the external elements into the supply structure, the setting turns out to be an ecosystem and could

hardly be restrained with a two-sided market relationship. Considering the coordination of the internal elements rests on the cloud provider's decisions, one-sided decisions based on single cloud management would no longer suit ecosystem relationships in the second broader setting. When passing to the ecosystem setting, the complementarity is replaced with the interdependencies. Then, the demand and supply equilibrium would hardly be truly found because of the emerging complexity and the so-called coordination problem, which often comes up with multiple equilibria.[753]

This problem is indirectly pointed out by some authors e.g. Cowen and Gawer (2012), who refer to the organisational innovation in the cloud because of the multi-party structure.[754] While such arguments rest on the cloud computing market itself, the cloud-based interdependencies reach out to other markets e.g. content, broadband and CDNs in the ecosystem setting, marking a stark distinction from the first setting of the cloud environment. While the self-supply and outsourced cloud components are matched and coordinated across the board in the first setting, a broadening set of transactions and exchange decisions between ISPs, CDNs, cloud and content providers are made in the second setting of the cloud ecosystem.

From the ecosystem perspective, as members continuously innovate and try to create value, they also attempt to gradually gain bargaining power vis-à-vis other members of the ecosystem.[755] In an interdependent ecosystem, as a form of supply chain, it is not only rivals that can exploit the innovation and capture its value: it can be the firm's buyers, suppliers, or complementors.[756] This point, namely the heterogeneity of

753 Regarding the scope and the conditions under which 'multiple equilibria' takes place, see Richard W. Cottle, 'Multiple Equilibria' (International Encyclopedia of the Social Sciences, 2008) <https://www.encyclopedia.com> accessed 9 October 2020.
754 Cowen and Gawer (n 739) 47.
755 Cowen and Gawer (n 739) 47.
756 Cowen and Gawer (n 739) 47.

players and their differential capabilities to interpret their environment and respond to it, marks the main difference between the ecosystem approach and the traditional economics approach which focuses on micro-level decision making processes largely based on linear processes.[757] Given this fact, the ecosystem approach would be appropriate and more relevant for the second broader setting that includes the external as well as internal (cloud) elements, when compared to the first setting.

7.1.3. Interoperability debate in the cloud context

External and internal elements that constitute the cloud ecosystem have some layers interdependent and interconnected to each other. These inter-links between the cloud layers are achieved by means of interoperability. The cloud components, including applications, platforms and infrastructure elements, should speak to each other for the cloud services to be run across the board. This denotes the narrow(est) viewpoint which could be compared to 'intra-operability' based on one provider cloud management, should we disregard the outer space of the cloud environment.

However, just as with the components in the cloud speaking to each other, equivalent elements of different clouds should ideally interoperate with each other. For instance, virtual machines in the infrastructure layers of distinct clouds that are running third parties' platforms or applications, should be able to be moved from one cloud to another. When they are integrated into a cloud environment, they should operate towards the same goal of service provisioning along with other components. Not only virtual machines, but also platforms and applications should be replaceable, exchange data and information across the clouds. From this viewpoint, it is argued that cloud

[757] See Johannes M. Bauer, 'Platforms, systems competition and innovation: Reassessing the foundations of communications policy' [2014] 38 Telecommunications Policy 662, 667.

interoperability refers to the ability of customers to use the same management tools, server images and other software with a variety of cloud computing providers and platforms.[758] All these refer to an understanding for cloud interoperability, which suggests that the users' applications, data and software in the disparate clouds be able to work together based on the mutually agreed specifications. Hereby the aim is to enable the cloud users and providers operating across and within different layers of the supply chain, to interact and exchange data and instructions.[759]

However, neither intra-operability in one cloud nor interoperability between the clouds could be isolated from the underlying external layers. One should consider that the internal elements of the cloud layer, and the external elements of the access layer are constituents for a cloud ecosystem, setting out a broadened need for multi-layered interoperability. The physical link between a cloud infrastructure and an ISP means that the already established standards yielding the intended interconnectivity between the former and latter, includes software interoperability. The same is true for the interlinks between the clouds and CDNs. Thus, the cross-layer protocols that ensure interoperability play a key role across the cloud-CDN-ISP interdependencies. To these interdependencies, content layer would be added as content providers (CPs) are always in interaction with cloud, CDN and internet service providers.[760] Through the

---

758 Claybrook (n 152).

759 See Niamh Gleeson and Ian Walden ''It's a jungle out there'?: Cloud computing, standards and the law' (2014) 5(2) European Journal of Law and Technology <http://ejlt.org/article/view/363/460> accessed 9 October 2020, 2; W. Kuan Hon and Christopher Millard, 'Control, Security and Risk in the Cloud' in Christopher Millard (eds), *Cloud Computing Law* (OUP 2013), 26-27. See also European Telecommunications Standards Institute (ETSI), *Version 1.0.* (Cloud Standards Coordination, Final report, 2013) <https://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF> accessed 9 October 2020, 7, reading; "The cloud service customer should be able to use widely available ICT facilities in-house when interacting with the cloud services, avoiding the need to use proprietary or highly specialized software".

760 As content provision does not underlie the cloud networks and services, the content layer has not been examined within the context of cloud settings. However, from the perspective of ecosystem interdependencies, CPs have a stake and role to play, which goes beyond the scope of this study.

interfaces across the value or supply chain, these ecosystem players coordinate and interoperate with each other.

Given this fact, interoperability comes up as one of the most significant threads across the emergent cloud ecosystems, as well as the cloud environments, which are the supply structures analysed above. Below, interoperability is examined in view of these settings and the attendant needs and problems.

7.1.3.1. Interoperability in the cloud environment

Similar to the traditional legacy networks, such as the internet that builds upon TCP/IP protocols, interoperability in the cloud environment will occur at the various layers, starting with the infrastructure layer e.g. through the Open Virtualization Format (OVF), an industry-wide standard and moving to the upper layers that are mostly designed via proprietary interfaces.[761] Cloud components are run on the dedicated software components which represent the so-called layers, although they might not be typified as a modular layered system. Cloud management provides a complete framework for managing all aspects of the infrastructure i.e. provisioning, deployment, monitoring, securing, messaging, reporting etc., as well as the cloud applications working on these infrastructural elements.[762] As cloud APIs provided by the cloud management layer also allow applications to take control of the infrastructure they run on,[763] it may be argued that a modular theory does not fit well to the cloud context.[764]

---

761 Renda (n 153) 28-29; Unver (n 27) 4.

762 M. Zaid Ahmed 'How Cloud Computing Application Architecture is Different from Traditional Application Architecture?' (2015) <https://www.linkedin.com/pulse/how-cloud-computing-application-architecture-different-muhammad-ahmed/> accessed 9 October 2020.

763 Ibid.

764 It is acknowledged that cloud computing infrastructure virtualization seems to violate key principles of modularity theory (Reuel Edison Ocho, 'Architectural evolution through softwarisation: On the advent of software-defined networks' (PhD Thesis, The London School of Economics and Political Science, 2016) 77).

Given the fact that management of the cloud components is performed by the cloud provider, interoperability confronts new problems i.e. tight coupling in the cloud.

Tight coupling refers to a strategy of pursuing coupling between the essential components in the cloud environment. By contrast, loose coupling means that cloud components make few assumptions about each other e.g. regarding the format of exchanged data or the communication channels used.[765] Coupling strategies indirectly demonstrate the extent to which the cloud provider wants to centralise the application programming and processing within the cloud environment.[766] This could also be interpreted to show the level of the elasticity of cloud management against the third-party applications vis-à-vis cloud-native ones.

Coupling strategies are also supplemented by the fact that a few common standards are in place to govern the cloud computing industry. While the greatest level of interoperability is likely to be found for IaaS cloud services, where functionality is often broadly equivalent and there are a number of standard interfaces, some of which are formally standardized such as the CDMI and others like the OVF being de-facto standards in the marketplace, PaaS and SaaS cloud services have lower levels of interoperability.[767] Except with these few standard interfaces that ensure interoperability at the infrastructure layer, common standards at the upper layers do not exist in the cloud environment.[768] Therefore, undertakings may exploit the fact that their customers have been locked into their cloud service and impose the use of their

765 Fehling et al (n 733) 152. Loose coupling might be compared to the internet layers that communicate with each other through the interfaces which do not prescribe or interfere with the protocols running each layer.

766 See Fehling et al (n 733) 151-159.

767 Cloud Standard Consumer Council, *Interoperability and Portability for Cloud Computing: A Guide* (Version 2.0, 2017) 7 <https://www.omg.org/cloud/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf > accessed 9 October 2020.

768 See ibid; Claybrook (n 152); Gleeson and Walden (n 759) 14-16.

own software.[769] This snapshot of the cloud environment would enable the cloud providers to establish an installed customer base and to heighten the switching costs. In the case of the vendor lock-in scenario, when one cloud customer relying on a PaaS or SaaS wishes to migrate from one provider to another, they would face technical and/or financial challenges resulting from this lack of interoperability. Such challenges primarily relate to the portability of applications, software tools and datasets, although mandated data portability alleviates these problems to an extent.

Under the GDPR (Article 20) was introduced a new right called the 'right to data portability' (RtDP) enabling individual users to move their data across the data controllers.[770] According to this new statutory right, data subjects (natural persons) have the right not only to extract their personal data from the cloud provider but also to have that data transferred from one cloud provider to another. However, this right is subject to various limitations. Firstly, the GDPR allows usage of this second part of the RtDP, namely transmission of personal data "*where technically feasible*" (GDPR, Article 20(2)). Secondly, the RtDP is limited to natural persons and does not cover the data of businesses i.e. regarding management, analytics and marketing, that might be hosted by the cloud providers.

On the other hand, EU Regulation 2018/1807[771] that was put into force under the DSM initiative, paves the way for the elimination of data portability constraints. Aiming at removal of the obstacles against the free flow of data across the EU, Regulation 2018/1807 adopted a self-regulatory process to ensure the portability of non-personal

---

769 Luciano and Walden (n 152).

770 For further details regarding data portability see the thesis section '3.2.4. Data protection rules: Right to data portability'.

771 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303 ('Regulation 2018/1807').

data,[772] alongside other policy objectives i.e. prevention of data localisation. To that effect, "a principle-based approach that provides for cooperation among Member States, as well as self-regulation" is laid down under the Regulation,[773] whereby the Commission will be monitoring and issuing guidance and evaluation reports throughout the period.[774] In the end it is targeted by means of self-regulatory codes of conduct, so users can port data between cloud service providers and back into their own IT environments.[775] Before the entry into force of this Regulation, major stakeholders like Google, Microsoft, Facebook and Twitter had started to collaborate under an open source project to facilitate data portability between competing services.[776]

In the light of these recent legislative and industry-led developments, vendor lock-in concerns might be argued to have dispersed thanks to the emerging data portability tools and safeguards. However, such measures aim at portability of 'data', not the applications and software tools that are hosted by the clouds. A distinction should be drawn between the data that is subject to data portability measures and the applications and software, including databases, which are not. Applications, including databases, will have their own individual design and structure, be it processes, specific formats,

---

772 "[S]pecific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines" (Regulation 2018/1807, recital 9).

773 Regulation 2018/1807, recital 11.

774 According to Article 6, the Commission shall "[e]nsure that the codes of conduct are developed in close cooperation with all relevant stakeholders, including associations of SMEs [Small and Medium-sized Enterprises] and start-ups, users and cloud service providers" and "encourage service providers to complete the development of the codes of conduct by 29 November 2019 and to effectively implement them by 29 May 2020".

775 European Commission, 'Digital Single Market: Free flow of non-personal data' (2019) <https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data> accessed 9 October 2020.

776 John Leonard, 'Google, Microsoft, Facebook and Twitter team up on data portability project' (*Computing*, July 23, 2018) <https://www.computing.co.uk/ctg/news/3036306/google-microsoft-facebook-and-twitter-team-up-on-data-portability-project> accessed 9 October 2020. The companies involved are developing tools that can convert any service's proprietary APIs to and from a small set of standardized data formats that can be used by anyone (Taruka Srivastav, 'Google, Microsoft, Facebook and Twitter collaborate for Data Transfer Project' (*The Drum*, July 21, 2018) <https://www.thedrum.com/news/2018/07/21/google-microsoft-facebook-and-twitter-collaborate-data-transfer-project> accessed 9 October 2020.

behaviours and outputs.[777] This is what differentiates one from another and a legal move to standardise actual applications might have negative implications for innovation and competition.[778] On the other hand, the emergent fragility and fragmentation, along with absent common standards, would harm interoperability at the application and/or platform layers, in spite of data portability.

Against the insufficiency of data portability and standardisation efforts, there might be a need to resort to sector-specific and/or competition law remedies in order to respond to interoperability and accompanying problems. Remarkably, EU legal rules and remedies based on IPR, and sector-specific and competition laws, have different perspectives to deal with the interoperability problems, including vendor lock-in. That is, invoking interoperability-centric tools would require a background scenario of either an abusive behaviour e.g., refusal to supply, or of an imminent harm to ex ante principles or rules i.e. end-to-end connectivity. In the case of such scenarios, available tools and remedies including data portability measures could address the potential problems to be confronted in the cloud environment.

7.1.3.2. Interoperability in the cloud ecosystem

Interoperability, from an industry-specific perspective, is destined to be dealt with through standardisation, in the way the European Commission envisions the picture. This approach could be compared to the narrow-minded approach dedicated to the cloud environment described above. However, an in-depth analysis seems inevitable when one looks at the cloud ecosystem that relies upon the underlying and external

777 Begoña González Otero, 'Mandating Portability as a Strategy to Achieve Interoperability between On-line Platforms: Pros & Cons' (12th International Conference on Internet, Law & Politics, Barcelona. 7-8 July 2016) 217.
778 Ibid.

elements of the broadband and content delivery networks that constitute the access layer and has interlinks with the content value proposition. From this broader point of view, issues regarding interoperability could not be separated from, and need to be analysed with, the associated layers or external elements within the overall ecosystem.

Here, the interactions between the ecosystem players should be reemphasized as they reframe the collaborative as well as competitive relations between the players. For instance, operators of the access layer, namely CDNs and ISPs, aim to enhance and differentiate their services against the newly emerging IP multimedia services, which are not heavily regulated and have a closer connection with the end-users. To that effect, both CDN and broadband operators are on the one hand collaborating and/or merging their powers with the content and application providers,[779] and on the other hand they strive to provide their own virtualisation and platform services, to gain a competitive edge.[780] To capture more frontiers against their competitors, as well as operating more efficiently, access providers would attempt further actions, including network slicing.[781] In its fullest realization of this strategy, the ISP can offer multiple tiers of cloud services ranging from wholesale access to core cloud resources i.e. computing, storage, and transport.[782] Such a scenario could be compared to CDNs deploying their networks to closer areas to the end-user termination points, to gain a favour in their relationship with the ISPs. From a broader viewpoint, CPs' investments

779 Comcast's acquisition of NBC Universal and Verizon's acquisition of EdgeCast and Yahoo! could be given as recent examples of such mergers.

780 See Stocker et al (n 747) 1006. Many of the largest operators of full-service networks such as Telefonica, AT&T, and Telecom Italia, are investing heavily in Network Function Virtualization and Software Defined Networking technologies to "softwarize" their networks, in order to gain finer-grained, flexible and dynamic control over network resources Stocker et al (n 747) 1006.

781 See Stocker et al (n 747) 1006. In this operation, the network infrastructure can be virtualized and then sliced into logical partitions that may support different levels of QoS and network functionality.

782 See Stocker et al (n 747) 1006.

into deployment and management of CDNs should be underscored,[783] albeit with the difficulty for them to have a comparable coverage with CDNs. All these facts while demonstrating the natural, technical and territorial limitations of each ICT players, also denote the very ecosystem where the players do rely on myriad interactions between each other, mostly characterised with multiple equilibria.

Under these circumstances, we are confronted with the term 'coopetition', which is depicted as to comprise cooperation and competition between competitors at the same time.[784] This term suggests no serious contradiction between competition and collaboration, but an enriched relationship built on both. According to this idea, as theorised by Adam M. Brandenburger and Barry J. Nalebuff, in order for the firms to have a sustainable development, they need to collaborate with other firms and organizations, including competitors, to address social, environmental, and economic needs.[785] Coopetition is rapidly becoming a key success factor for enterprises operating in the contemporary business world, along with an increased importance in parallel with the globalization process.[786] This snapshot of 'coopetition' well matches with the cloud ecosystem which could be compared to broader ICT settings.[787] From

---

783 Companies such as Google, Youku, Tudou and, more recently, Netflix, use their own CDNs – either wholly or in conjunction with "pure play" providers – other major players such as Hulu, Facebook and Amazon continue to partner with one or more of the leading Internet CDNs – including Akamai, Limelight Networks and Level 3 (Giles Cottle, *CDNs could help smaller OTT players disrupt the content hierarchy* (Informa, 2012) 7).

784 For detailed analysis of this concept, see Keith Walley, 'Coopetition: An Introduction to the Subject and an Agenda for Research' [2007] 37(2) International Studies of Management & Organisation, 11-31.

785 Joanna Cygler, Włodzimierz Sroka, Marina Solesvik and Katarzyna Debkowska, 'Benefits and Drawbacks of Coopetition: The Roles of Scope and Durability in Coopetitive Relationships' [2018] 10(8) Sustainability 1, 2.

786 Ibid, 19.

787 Broadly speaking, the complex value of network of the internet economy, in which complementarity and platform relations between firms abound, compels coopetition (Volker Schneider and Johannes M. Bauer, 'A network science approach to the Internet' in J. M. Bauer and M. Latzer (eds), Handbook on the Economics of the Internet (Edward Elgar 2016) 72, 72). According to many scholars, these developments change the nature of competition in ambiguous ways, often requiring companies to compete and cooperate with their rivals (Ibid).

this viewpoint, ‘complementarity’ or ‘substitutability’ are destined to be replaced with broader and more complex relationships, coupled with multi-layered interdependencies. Against the cross-layer interactions, it would be highly questionable to pursue market-centric approach, particularly based on predefined markets and potential remedies to be imposed on dominant (SMP) players. Along the same lines, conventional tests to measure the elasticity of demand and supply in the relevant settings potentially lose their ground in defining the competitive relationships between the ICT players against the overarching interdependencies.

Crucially, interoperability stands out as one of the threads for the coopetitive relationships in the ecosystem context. Closely related to the interdependencies, interoperability would come about as part of the overall strategies of ecosystem players, including cloud providers. While one could comprehend intra or inter-cloud interoperability on the basis of standards, consortia, etc., these relationships changing into complex interdependencies in the ecosystem makes any regulatory process much harder. In an era when the defined markets become outdated and blurred, lack of interoperability and accompanying problems i.e. vendor lock-in or other related issues i.e. efficiencies, would not be easily attached to certain market(s) and/or harm theories. In this light, a possible solution for the lack of interoperability from the conventional legal perspectives might be patchy and narrow-minded. Given this fact, an ecosystem-based approach seems persuasive for interoperability and its accompanying problems, across the interdependent layers and players.

7.1.4. Analysis of cloud settings under the EU legal framework

Against the background information above, it is apparent that interoperability could not be singled out as a self-standing problem, but rather needs to be analysed along with other dynamics of the cloud settings. Having said that, based on the narrow and broad settings analysed above of the cloud environment and cloud ecosystem, the evaluation of several parameters i.e. interdependencies, complementarity and substitution, competition, cloud management, interoperability and standardisation is reflected in the table below.

Table 1: Evaluation of parameters for cloud settings

Parameters	**Cloud environment (internal elements)**	**Cloud ecosystem (both internal and external elements)**
Interdependencies	Interdependencies are limited, with the internal elements being governed by the cloud provider	Interdependencies turn out to have a core and determinant effect in ecosystem relationships
Complementarity and substitutability	Complementarity and substitutability would shape out the markets	Lessening impact of market based relationships
Competition	Competition depends on the intra and inter-cloud links and interoperability	Competition is accompanied by cooperation between ecosystem players (resulting in coopetition)
Cloud management	Single cloud management dominates the relationships in the cloud	Multi-layered relationships supersede layer or platform based cloud management
Interoperability	Strong link exists between competition and interoperability	Interoperability is governed by the cross-layer interdependencies and coopetitive relationships
Standardisation	Standardisation might have a pro-interoperability and competitive impact	Standards' role is diminished against the enhanced space for innovation

Source: Constructed by the author

Interoperability could be mapped and figured out across the given settings as summarised above. Given the inputs in the table, ICT interdependencies have a prominent effect, likely to supersede the market and/or platform based relationships, within the ecosystem context. Accordingly, 'substitutability' and 'complementarity' which define the markets and underlying products are not destined to be very influential in contrast to the role they played traditionally in competition/regulatory processes. The overarching interdependencies and underlying coopetitive relationships take over intra and inter-platform (cloud) competition when moving to the ecosystem setting. This ecosystem-based trajectory is clearly being shaped out by cross-layer interactions instead of a single management discourse which take place in the cloud environment.

In the light of the above information, it would be an incoherent and narrow-minded approach to crystallise 'interoperability' as a market or platform specific problem. Along the same lines, standardisation, although it might need to be encouraged, should not be considered as self-promising given the fact that standards are focused on narrower industrial settings which ostensibly match the cloud environment but not the ecosystem. It should be remembered that when moving from the cloud environment to the cloud ecosystem, standards' role decreases given the more space opening up for innovation, along with the interdependencies.

While cloud computing is underlined as one of the five most significant areas that need standardisation by the European authorities,[788] the possible solution(s) to be found out should ultimately have a cross-layer nature. Whereas technically a potential solution

[788] European Commission, ICT Standardisation Priorities for the Digital Single Market, COM (2016) 176 final, 5 <http://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-176-EN-F1-1.PDF> accessed 9 October 2020.

i.e. a common standard, would be fit for purpose from the perspective of the cloud environment, such a solution would no longer have an overarching effect from the ecosystem perspective, considering the interdependent layers including both internal and external elements. As clouds do not work alone but in tandem with other layers i.e. CDNs and broadband access networks, a cloud-specific interoperability solution would be incomplete and partial against the cross-layer interdependencies and accompanying issues, problems, etc.

Given this fact, the *status quo* under EU legal framework, particularly in view of the competition law and ECRF rules, do not offer promising and sustainable solutions against the cross-layer settings and problems. To emphasize, interoperability-centric problems within this framework might undergo a kind of regulatory micromanagement. However, this might turn out to be narrow-minded since exclusionary practices e.g. a dominant player's refusal to supply APIs might be deemed as abusive under certain 'exceptional' circumstances. This rests on the presumption of a central and dominant product, usually to be found via market shares, whereas centralised market products no longer depict the underlying coopetitive relationships. Furthermore, a cloud provider's relationship with other ICT players in the ecosystem context are crucial also in the sense that efficiencies are usually spread across the interdependent layers. As these issues i.e. efficiencies, and problems i.e. the refusal to supply, need to be analysed within the broader context of interdependencies, a wider regulatory lens comprising multi-layered interoperability, would rather be followed.

7.2. The Internet of Things

7.2.1. General Overview

The Internet of Things (IoT) is a natural extension of the internet.[789] The Internet of Things (IoT) is defined as "A global infrastructure for the information society, enabling advanced services by interconnecting physical and virtual things based on existing and evolving interoperable information and communications technologies".[790] This term denotes a trend whereby myriad devices and sensors employ communication services, data exchange and processing towards certain results. At the centre of the IoT lies the connected devices or smart objects, including cars, refrigerators, health care devices and wearable things such as wrist bands and watches, which communicate and exchange data with each other on the basis of end-to-end connectivity that is ensured by certain protocols and standards.

Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are being combined with internet connectivity and powerful data analytic capabilities that promise to transform the way we work, live, and play.[791] The IoT can generate an incredibly powerful breadth of data which can then be translated into a product cloud or networked system, out of which users' information is clustered, filtered and managed. Alongside cloud computing, the IoT serves as one of the leading technologies that stimulate and transform big data into innovative products and new avenues of wealth generation.[792]

---

789 Hwang, Fox and Dongarra (n 733) 576.

790 International Telecommunications Union (ITU), *Overview of the Internet of Things* (ITU-T Y.4000/Y.2060, 2012) <https://www.itu.int/rec/T-REC-Y.2060-201206-I> accessed 9 October 2020.

791 Internet of Things: An Overview (n 154) 4.

792 The IoT is considered to be the most disruptive technology for industries and business models, and is the one having the highest investment amongst others like artificial intelligence, robotics, 3-D

Projections for the impact of the IoT on the Internet and economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025.[793] Behind this big transformational impact lies the combination of ubiquitous network access, the processing power of microchips, miniaturised devices, cloud computing and big data analytics. The IoT enables a very broad range of applications – from more efficient agriculture, manufacturing, logistics, counterfeit detection, monitoring of people, stock, vehicles, equipment and infrastructure, to improved healthcare, retailing traffic management, product development and hydrocarbon exploration.[794] All these point to a hyper-connected world of smart devices, applications and value-added services spreading across to every corner of our daily lives, as manifested below (See Figure 10).

printing, augmented reality, virtual reality, drones and blockchains) (Miguel Dias Fernandes, 'Internet of Things' (PwC Partner, 2018) <https://www.pwc.pt/pt/temas-actuais/pwc-apresentacao-iot.pdf> accessed 9 October 2020.

793 Internet of Things: An Overview (n 154) 4.

794 Brown (n 7) 23.

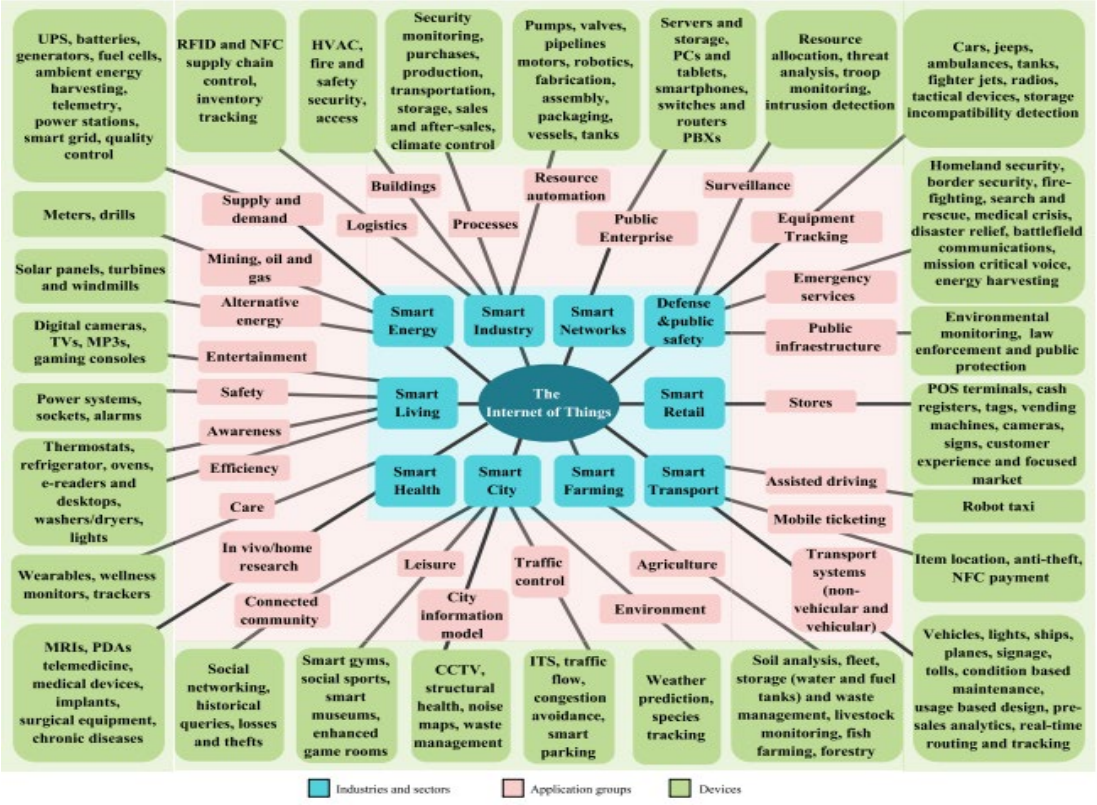

Figure 10: Proliferation of the IoT services, devices and applications

Source: Paula Fraga-Lamas, Tiago M. Fernández-Caramés, Manuel Suárez-Albela, Luis Castedo and Miguel González-López, 'A Review of the Internet of Things for Defense and Public Safety' (2016) 16 Sensors <https://www.mdpi.com/1424-8220/16/10/1644> accessed 9 October 2020

Although distinguishable from each other on industrial grounds, each manifestation of the IoT has similar building blocks. For a viable IoT model, the stakeholders, from manufacturers to application developers, should cooperate in order to match and optimise their resources, both technically and commercially. In this regard, in all the IoT settings i.e. home appliances, smart cars, wearable devices, smart energy and telemedicine, the stakeholders' software and hardware solutions should speak to each other, which echoes IoT interoperability. Below, first the technical and economic underpinnings and then the interoperability aspects of the IoT are examined, respectively.

7.2.2. Technical and economic underpinnings

The IoT brings out an important degree of efficiencies and innovation based on the M2M communications and internet connectivity, ending up with reformation of the industries and sectors. Following the invention of 'computers' and the 'internet', the IoT represents the next biggest wave of transformation, along with large-scale economic implications. It has driven the creation of new business models as well as modernisation of existing businesses, by utilising new software and microprocessors, etc, lessening the need for human resources and reducing operational costs.[795]

Web 2.0 has changed usage of the WWW by providing more intuitive interfaces for user interaction, social networking and the publication of under-generated content, without requiring fundamental changes to the design and existing standards of the internet.[796] Conversely, the IoT, along with other emerging technologies i.e. cloud computing, machine learning and AI, is destined to bring a new industrial revolution (Web 4.0) together with socio-economic repercussions. At the heart of such paradigmatic change lies the IoT connectivity, which takes three forms as follows:

- One-to-one: An individual product connects to the user, the manufacturer, or another product through a port or other interface - for example, when a car is hooked up to diagnostic machine.
- One-to-many: A central system is continuously or intermittently connected to many products simultaneously. For example, many Tesla automobiles are

[795] For instance, new business models include car and truck rental clubs, whose members can book and use vehicles parked around their neighbourhood almost on-demand; or "pay-as-you-drive" insurance based on precise driving patterns, behaviour and risk (Brown (n 7) 6-7).

[796] Dieter Uckelmann, Mark Harrison, Florian Michahelles, 'An Architectural Approach Towards the Future Internet of Things' in Dieter Uckelmann, Mark Harrison and Florian Michahelles (eds), *Architecting the Internet of Things* (Springer 2011) 6.

connected to a single manufacturer system that monitors performance and accomplishes remote service and upgrades.

- Many-to-many: Multiple products connect to many other types of products and often also to external data sources. An array of types of farm equipment are connected to one another, and to geolocation data, to coordinate and optimise the farm system. For example, automated tillers inject nitrogen fertiliser at precise depths and intervals, and seeders follow, placing corn seeds directly in the fertilised soil.[797]

The IoT hubs and connections explained above create new product chains, which manifest new ecosystems in effect.[798] At present, the IoT ecosystems are formed around technological innovations focusing on a specific application domain, such as RFID solutions in retail, mobile M2M communications in remote automated meter reading (AMR), or ZigBee communications in smart home.[799] Albeit with nuances from business perspectives, these nascent ecosystems reveal similarities in terms of architectural aspects, which are detailed below.

7.2.3. Architectural elements and layers in IoT

Albeit with the differences pertaining to the industries and sectors, all the IoT settings depend on end-to-end connectivity and interoperability enabled by interfaces and protocols. That is, in all cases, IoT devices which are embedded to the objects:

---

797 Michael E. Porter and James E. Heppelmann, 'How Smart, Connected Products Are Transforming Competition' (2014) Harvard Business Review <https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition> accessed 9 October 2020.

798 See Oleksiy Mazhelis, Eetu Luoma, and Henna Warma, 'Defining an Internet-of-Things Ecosystem' in S. Andreev, S. Balandin and Y. Koucheryavy (eds), *Internet of Things, Smart Spaces, and Next Generation Networking* (Springer 2012) 2.

799 Ibid.

- should speak to other connected devices;
- should exchange data streams (instructions) with each other and/or convey necessary messages to the service provider, usually via an IP cloud enabling data pooling, reporting, analytics; and
- communicate with the users who aim to control the so-called devices through various applications i.e. via tablets, mobile phones or other personalised devices.

For instance, a smart thermostat should have a set of functionalities, according to which, it should;

a) control temperature and humidity, and inform its consumer about the temperature changes,
b) aim to keep a stable temperature in a room,
c) learn the consumer's usage pattern and adjust the temperature accordingly,
d) notice if there are people present in a room,
e) communicate with the nearby devices and notice if devices that may affect the temperature are turned off/on,
f) be able to be controlled through dedicated remote or wall-mounted controllers, as well as through smartphones, tablets or laptops,
g) show how long a desired temperature is reached, and enable the consumer to set the temperature away from home, and
h) aim to save power and guide the consumer on how to save energy.[800]

[800] Oen (n 65) 7-8.

While some of the above functionalities relate to 'user interfaces' that enable consumers to instruct and get feedback from the thermostat, some others are managed from the central cloud system on the part of the IoT service provider - which however could partially be distributed and embedded into the devices and applications at the edge, to some extent. Also, an IoT device's interaction, in the given case, a thermostat's, with other IoT devices e.g. moisture sensors and windows, denotes another functionality, without which the ultimate benefits could not be fully reaped from these technological innovations.

While the devices and applications are visible to the users, the underlying architecture of the IoT systems depends on a widely acknowledged three layers. These interdependent layers are classified as (i) perception layer, (ii) network (access) layer and (iii) application layer[801] as illustrated below.

[801] See Vivek Kumar Sehgal, Anubhav Patrick and Lucky Rajpoot, 'A Comparative Study of the Cyber Physical Cloud, Cloud of Sensors and the Internet of Things: Their Ideology, Similarities and Differences' (IEEE International Advance Computing Conference (IACC) 2014) 711-712; Elena de la Guía, María D. Lozano and Víctor M. R. Penichet 'Interacting with Objects in Games through RFID Technology' (2012) Intechopen <https://www.intechopen.com/books/radio-frequency-identification-from-system-to-applications/interacting-with-objects-in-games-through-rfid-technology> accessed 9 October 2020; Hwang, Fox and Dongarra (n 733) 579.

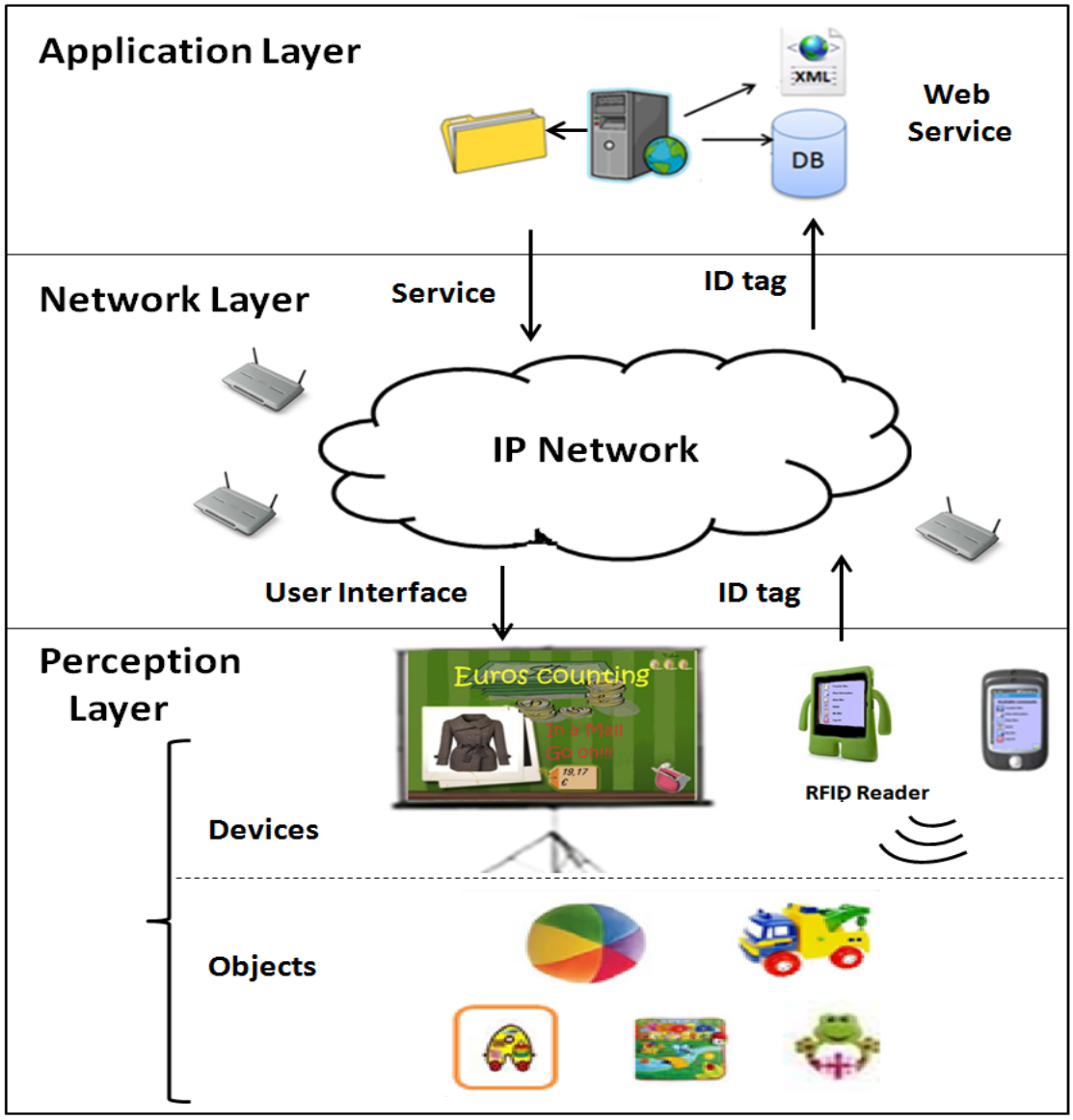

Figure 11: IoT architecture and layers

Source: De la Guía, Lozano and Penichet (n 801) 330

The perception layer consists of embedded devices that have sensors aiming to recognise, perceive and aggregate the data from the things surrounding them.[802] They

[802] Today's sensors can monitor temperature, ambiance, soil makeup, pollution in the air, noise, presence of objects or movements, amongst other actuating functionalities and triggered based on some sensed information (Mahmoud Elkhodr, Seyed Shahrestani and Hon Cheung 'The Internet of Things: New Interoperability, Management and Security Challenges' [2016] 8(2) International Journal of Network Security & Its Applications 85, 87) These sensors collect varied information about the environment, such as mechanical data e.g. position, force and pressure, thermal data e.g. temperature and heat flow, electrostatic or magnetic field, radiation intensity e.g. electromagnetic and nuclear, chemical data e.g. humidity, ion and gas concentrations, and biological data e.g. toxicity and presence of bio organisms (Swaroop Poudel, 'Internet of Things: Underlying

might interact with peer devices, usually via standardised protocols like Radio Frequency Identification (RFID), Near Field Communication (NFC) and Bluetooth, to capture related data and comprehend them. This bottom layer takes the sensed data and perceives intelligent information, using possible means of energy efficiency i.e. low power, low cost.[803] The perceived information is carried through the network (access) layer, which transfers the relevant data to the end-users, namely their hand-sets, PCs or tablets.

The network (access) layer consists of the internet, public or private networks, wired or wireless communication and integrated networks for transferring perceived data to the application layer, using various communication protocols like LTE, 3G, Wi-Fi, Wi-Max, Zigbee etc.[804] Along with data transfer, this layer may also perform the tasks of data processing, knowledge discovery and data storage with the help of the cloud computing environment.[805] The data aggregated by the perception layer and processed by the network layer is conveyed to the application layer, which is visible to the end-user. Similar to the internet stack, the application layer resides at the top of the IoT architecture. Likewise, it uses the layers below itself as the underlying services. In the end, the end-users are communicated to with the apps, usually uploaded in PCs, smartphones and tablets, and are given the 'predictive analysis' including the feedback, suggestions and choices across the real-time scenarios. The figure below illustrates the layers that constitute the IoT architecture.

Technologies, Interoperability, and Treats to Privacy and Security' [2016] 31(2) Berkeley Technology Law Journal Annual Review 997, 1003).

803 Sehgal, Patrick and Rajpoot (n 801) 711.

804 Sehgal, Patrick and Rajpoot (n 801) 711.

805 Sehgal, Patrick and Rajpoot (n 801) 711.

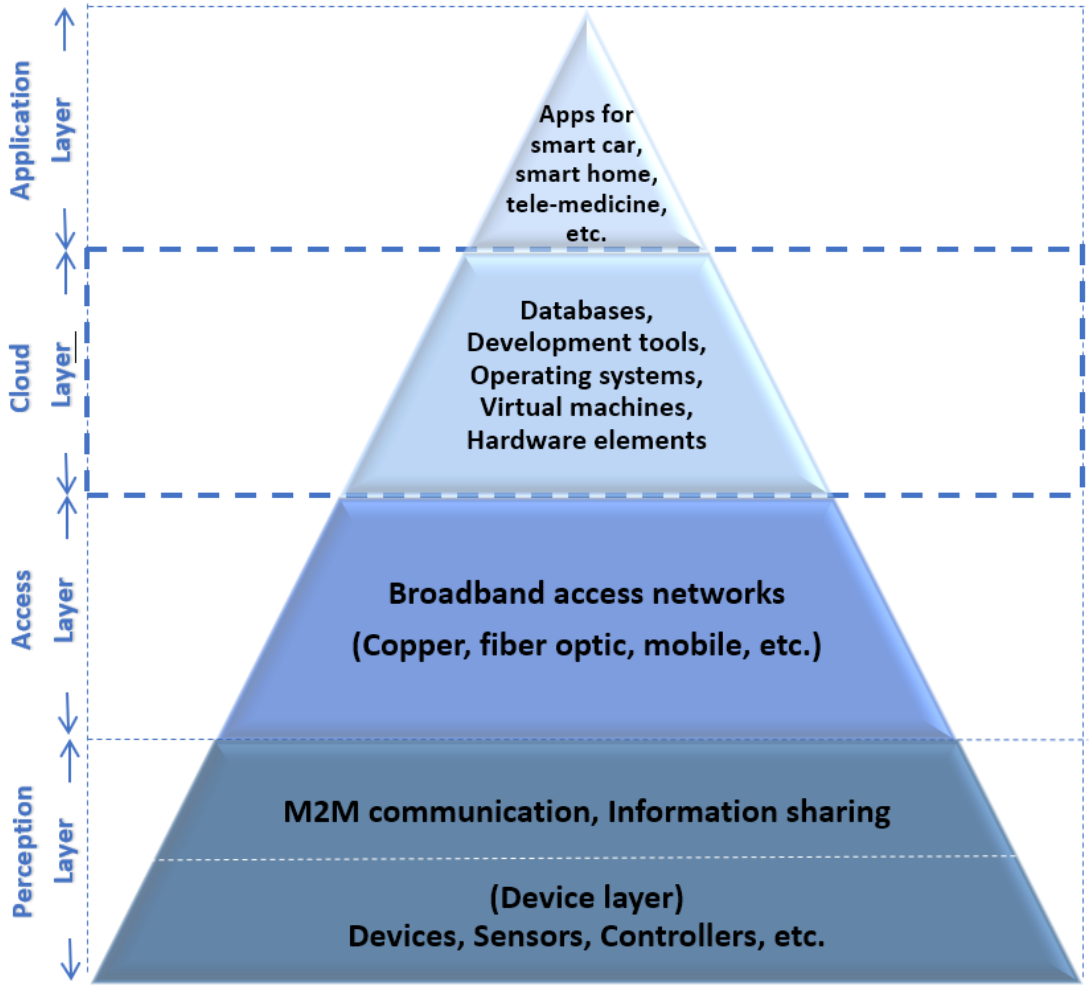

Figure 12: IoT layers (with cloud layer)

Source: Constructed by the author

In the context of the IoT, clouds have a fundamental role to play. This particularly stems from the need for pooling, processing and analysing the big data on the part of the entrepreneurs who aim to invest in the IoT systems. The variety of granular data aggregated from smart objects is transmitted, usually through gateways and pooled into the clouds which serve as the additional layer and sometimes called the 'common services layer', to store, process and analyse the data as well as enabling the personalised data to be accessed by the end-users. In the case of the thermostat, the device transmits data to a cloud database where the data can be used to analyse home

energy consumption.[806] Further, this cloud connection enables the user to obtain remote access to their thermostat via a smartphone or Web interface, and it also supports software updates to the thermostat.[807] Data management, comprising filtering bulk data, translating it into logical clusters and predicting long-term and massively applicable results, is essential in the context of the IoT. As this could not be performed by any other layer, devices usually offload processing and automation capability to cloud-based software.[808] Last, but not the least, diverse management tools and software in the cloud could enable data transmitted from a variety of sources (IoT devices) be filtered and processed through protocol translation. This functionality is sometimes being extended to the edge layers, namely devices and/or the gateway that serve as the intermediary between the devices and the cloud. For example, the SmartThings hub is a stand-alone gateway device that has Z-Wave and Zigbee transceivers installed to communicate with both families of devices, namely bridging the interoperability gap between the devices before transmission to the cloud.[809]

From this viewpoint, edge layering is sometimes compared to cloud layering as both would have comparative advantages and disadvantages. Particularly because of network latency resulting from location e.g. remote cloud sources, that might affect real-time IoT data transmission, more computing power located nearby the end-user devices is highlighted, echoed by the term, 'fog networking'. Not only enabling real-time data transmission, but also reducing data to a more manageable form, enhancing

806 Internet of Things: An Overview (n 154) 19.
807 Internet of Things: An Overview (n 154) 19.
808 Alternatively, a sensor web combines "distributed network" – the sharing of data collected by all sensors across the entire network - and "embedded intelligence" - the system acting on its own without communicating to an end user or an external control system for analysis and decision-making (Poudel (n 802) 1007).
809 Internet of Things: An Overview (n 154) 20. See also Samsung, 'SmartThings – Featured Products' <https://www.smartthings.com/gb/products> accessed 9 October 2020.

reliability and lowering privacy and data security risks from the transmission of granular data over the network, are linked to fog networking.[810]

While every business model, for several reasons i.e. security, reliability and latency depends on various protocols and/or standards, whether with cloud or edge layering, the decisions made by the stakeholders ultimately need to take into account the interoperability to be achieved along the layers, from the bottom to the top. Discourse about such decisions leads to another crossroads with regards to having an 'open' or 'proprietary' system. All these parameters make interoperability more puzzling than it seems at the outset.

7.2.4. Interoperability debate in the IoT context

7.2.4.1. IoT interoperability in general: Overview of different settings

Interoperability is crucial for the IoT and even more importantly than for other ICT systems. This stems from the nature of the distributed network and devices, which serve similar to nerves connected to and fed back by the brain, that should allow a seamless and uninterrupted flow of data and information from the sensors to the platforms, applications and people and vice versa. While this in the first instance encompasses the intra-platform data flow and exchanges and could be compared to intra-operability, IoT interoperability should be understood broadly and considering distinct, proprietary IoT systems and their interoperation.

In this light, IoT interoperability could be considered both from a narrow and broader perspective. Comprising both perspectives, the European Research Cluster on the

[810] Poudel (n 802) 1007.

Internet of Things defines 'interoperability' as "[t]he ability of two or more *systems or components* to exchange data and use information".[811] From the narrow perspective, the typical three or four layers of the IoT architecture are considered for interoperability. Accordingly, the perception, network and application layers, along with the cloud layer, should be able to 'exchange data and use information' to bring out the intended benefits to the users. From a broader perspective, IoT interoperability means a comprehensive outlook comprising both inter-system as well as intra-system approaches. That is, not only the components within an IoT ecosystem but also the IoT ecosystems themselves need to communicate and exchange data with each other.

Hence, IoT interoperability entails compatibility of the products and services offered by the IoT stakeholders i.e. manufacturers, software developers and sensor/chipset suppliers, among each other. This means cross-layer interoperability for and within the IoT ecosystems. Thus, should one manufacturer's devices e.g. lightbulbs, glucose meters and thermostats not work and be incompatible with one of the third parties' software e.g. switch and control systems, this means an interoperability gap for the IoT ecosystem in question. For instance, interoperability in the market of smart 'home appliances' means lightbulbs, windows, thermostats and other smart appliances speaking to each other, even though they are produced by different manufacturers. This could be extended to the broader industrial settings like the 'connected (smart) home' market which includes not only connected appliances but also automated lighting, HVAC (heating, ventilation and air conditioning), entertainment and security.[812] In the broadest setting, which could be described as a hyper-connected

---

811 European Research Cluster on the Internet of Things, 'IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps' (2015) 9 <http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Semantic_Interoperability_Final.pdf> accessed 9 October 2020.

812 Porter and Heppelmann (n 797).

marketplace, smart homes and the integrated devices, appliances, etc. are supposed to be interoperable with the smart cars, smart city components etc. Given this fact, IoT interoperability could be compared to the progressive industrial circles such as enlarging and overlapping loops manifested below.

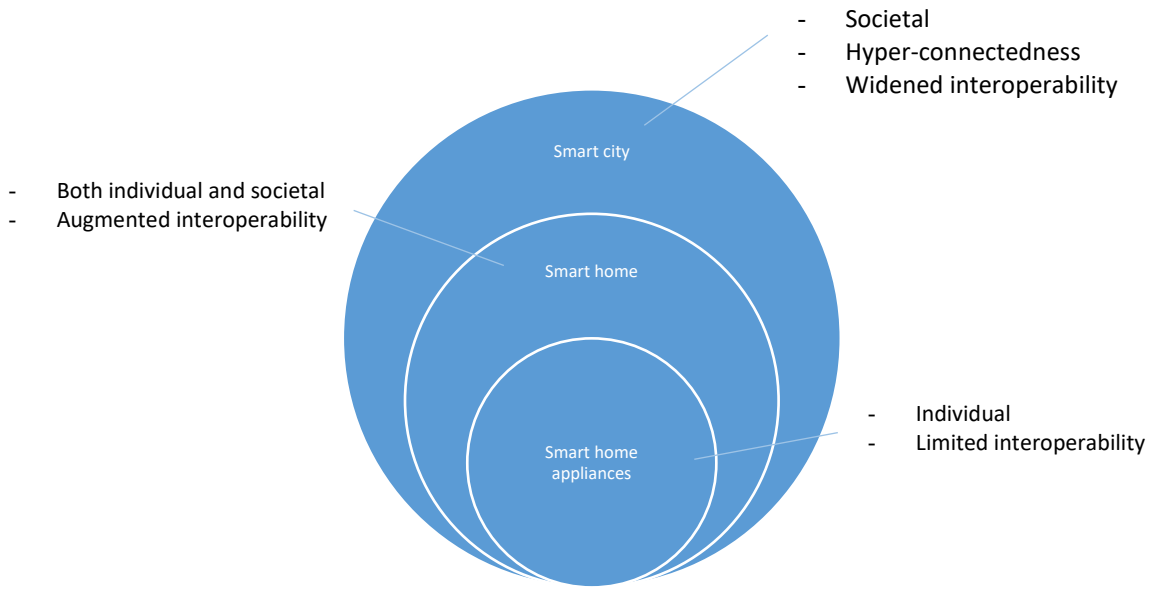

Figure 13: IoT loops showing different industrial settings

Source: Constructed by the author

While it is possible for smart applications e.g. RFID to be built on close-loop processes, namely monolithic business information systems, the conception of the IoT is principally and increasingly based on the idea of end-to-end connectivity in an 'anytime, anywhere' fashion, calling for open, scalable, secure, and standardised infrastructure.[813] Hence, the call for interoperability starts with the close-loop processes e.g. in the 'home appliances' setting and is augmented with the conception of 'smart home' and widened towards 'smart city'. For these concepts to come true, there should be a fulfilling response to the need for multi-layered interoperability. Notably, along the transition from the smallest circle to the bigger ones,

[813] Uckelmann, Harrison and Michahelles (n 796) 2-3.

'interoperability' becomes more compelling across the uses' needs, which are destined to push the boundaries of societal life as opposed to having a direct impact just over individuals.

As implied above, these expansive IoT spheres come about with a complexity along with a pressing need for interoperability. As with the two previous IT waves of computers and the internet, the difficulties, skills, time, and costs involved in building the entire technology stack for smart, connected products is formidable and leads to specialisation at each layer.[814] Just like Medtronic glucose meters, Philips lightbulbs and Tesla smart cars being specialised in their own fields of manufacturing, Intel has specialisation in the production of microprocessors, Oracle in databases and Cisco in underlying hardware.

Thus, it is apparent that every stakeholder in the IoT settings and ecosystems have more unique and distributed roles to play, with the view to maximise the profits to be reaped from their attempted actions. While striving for a more competitive advantage and further commercial frontiers, cooperation as well as competition among the stakeholders becomes of more importance, particularly from the ecosystem perspective. Along the same lines, the need for interoperability points to a crucial and multi-faceted aspect of all the IoT settings.

7.2.4.2. Interoperability in the IoT ecosystems

Architectural elements and layers of the IoT systems constitute the gateways for the IoT players, specifically from the interoperability perspective. For a successful and

[814] Porter and Heppelmann (n 797).

thriving IoT ecosystem, all the constituent layers and elements should interoperate with each other. Otherwise, competitors would face entry barriers because of the lack of interoperability and the technologically erected walls. In an effort to generate network efficiencies, some IoT products are designed to be interoperable with other devices used in a particular location e.g. home, office, and with factory control panels that interact with multiple products used for distinct applications, and use standard data formats to facilitate aggregation into databases for analysis.[815]

On the other hand, dominant IoT service providers and manufacturers tend to build up a proprietary ecosystem by closing off the so-called gateways to third parties, so as to maximise the profits to be reaped from an installed consumer base and their aggregated data. As recently identified by the European project Unify-IoT, there are more than 300 IoT platforms in the marketplace, among which Amazon (AWS), Cisco (Jasper), IBM (Watson), Apple (HomeKit), Google (Brillo), Microsoft (Azure), and Qualcomm (AllJoyn) represent the forerunners.[816] Each of these service or platform providers promotes its own IoT infrastructure, proprietary protocols and interfaces, incompatible standards, formats, and semantics which creates closed ecosystems or truly speaking 'walled gardens', sometimes called 'stove pipes' or 'silos'.[817]

Commercial strategies to increase the consumer loyalty, along with featured brands based on network effects, would effectively drive the leading companies to pursue a closed approach, although a trade-off is always at stake because of the potential data

---

815 Wrobel (n 252) 63. The potential for network effects may be more apparent in some IoT products; for example, traffic monitoring systems may benefit all users by generating real-time data for drivers, or eventually for driverless vehicles, and the benefits of these systems may grow as more vehicles are equipped with sensors, etc. (Wrobel (n 252) 63-64).

816 Mahda Noural, Mohammed Atiquzzaman and Martin Gaedke, 'Interoperability in Internet of Things: Taxonomies and Open Challenges' [2019] 24 Mobile Networks and Applications 796, 796.

817 Ibid.

to be included into the IoT value proposition.[818] Restrictions over the disclosure of APIs would as well result from the security and privacy concerns across the expansive chains of data aggregation.[819] The data streams and user specificity afforded by IoT devices can unlock incredible and unique value to IoT users, but concerns about security and privacy might hold back the IoT service providers from adopting an interoperable and/or open approach.[820]

From this point of view, the degree of interoperability has significant implications for the third parties e.g. software and application developers, in terms of having a restricted or open playing field. This playing field would get narrower or broader with the integration of additional layers i.e. intermediary layers into the IoT ecosystems. Sometimes, the addition of one layer would facilitate conversion of the non-native protocols into native ones that are applicable to the relevant IoT system. Yet it could end up as another wall by which third parties are excluded from the ecosystem. For instance, while full integration of a cloud platform into an IoT ecosystem would usually help bridge the interoperability gap as well as gathering data, this might have adverse effects when the IoT ecosystem creates network effects along with a walled garden structure. Last but not least, building up an IoT ecosystem also involves other

818 In many public projects, the idea of embracing more software developers leads the IoT ecosystem to build on a non-proprietary and open source project. This is illustrated by the European CityService Development Kit (CitySDK) Project, which lets programmers write software that can access data and share IoT services via open APIs, to improve transportation, help report problems to the city council and guide tourists around places of interest (Brown (n 7) 18).

819 Internet of Things: An Overview (n 154) 32. There would be many harms sourced from the poorly secured IoT devices, including; (i) serving as entry points for cyberattacks by allowing malicious individuals to re-program a device or cause it to malfunction, (ii) exposing user data to theft by leaving data streams inadequately protected, and (iii) creating security vulnerabilities (Ibid). Privacy arises as a sensitive issue in the IoT context, considering smart phones and apps that allow the flow of a significant amount of personal data. Researchers have found that smartphone sensor data can be used to infer information about users' personality types, demographics and health factors, such as moods, stress levels, smoking habits, exercise levels and physical activity – even the onset of illnesses such as Parkinson's disease and bipolar disorder (Brown (n 7) 27).

820 See Internet of Things: An Overview (n 154) 6.

concerns i.e. privacy, security, velocity and efficiency creating multidimensional consequences, which would compromise interoperability. Hence, these concerns are potentially augmented when moving from an intra-system setting to an inter-system one, along with more complicated trade-offs, as detailed below.

7.2.4.3. Analysis of interoperability related problems from the ecosystem perspective

While the analysis above suggests that interoperability reflects one of the main threads of the emergent IoT ecosystems, an in-depth look into the ecosystem relationships would be useful to clearly understand the IoT interoperability from a broader perspective. As a starting point, it should be remembered that while an ecosystem builds on adaptive and dynamic relationships between the players, interoperability requires more technical and crystallised solutions, like standards. As the need and user expectations for ubiquity, latency, velocity, scalability, etc. change across the industry settings, a diversification process prevails as to the standards applied to different IoT settings. For example, while the environmental sensors use ZigBee based on IEEE 802.15.4 standard, IoT devices such as Smart TV, printers, air conditioners support traditional ubiquitous Wi-Fi technologies and 3G/4G cellular communications.[821] On the other hand, most recent IoT medical devices are based on ANT+ standard, while other wearable devices mostly support Bluetooth SMART and NFC.[822] This diversified nature of the IoT solutions and standards[823] causes a fragmented structure in terms of interoperability.

---

821 Noural, Atiquzzaman and Gaedke (n 827) 798.

822 Noural, Atiquzzaman and Gaedke (n 827) 798.

823 It should also be noted that some of the IoT standards originate from broadcasting technologies, whereas some others are based on cellular (mobile) technologies. Under the first category exists the wireless standards for low-frequency, short-range and low-data transmission, such as ZigBee,

In conjunction with this fact, walled garden or proprietary systems are often preferred by the service providers, which limits the interoperability to only those devices and components within the brand product life.[824] In the end, interoperability is usually compromised along with lock-in problems, although IoT stakeholders might tend to boast much more data across an enlarged set of devices and applications. This dilemma brings out a hard-to-solve trade-off problem between interoperability and innovation across the distinct IoT solutions. In the short term, it is therefore hard to imagine a hyperconnected marketplace against the trade-offs that entails potentially harmed interoperability. Against this background, demystifying the potential problems, particularly vendor lock-in, across the layers would be useful to understand the holistic picture.

Starting from the bottom, the perception layer consists of numerous sensors attached to the IoT devices and running on the basis of numerous standard protocols, e.g. ZigBee, Z-Wave, ZigBee, WirelessHart or non-standard proprietary ones e.g. LoRa, Sigfox. As the standards adopted by the IoT providers are so diverse and have not ended up with a de facto one, interoperability solutions at this layer are fragmented. To illustrate, a lightbulb would not transmit data streams to the devices surrounding it e.g. windows, thermostat, etc., if they are based and run on different wireless standards. As the industrial developments manifest, a dominant supplier would opt to create a walled garden comprising a brand of family products which exchange data via the same protocol. The result then would be an outcome of vendor lock-in with the potential finding for abuse of dominance i.e. under 'exceptional circumstances'.[825]

Z-Wave, Bluetooth, Wi-Fi, NFC and Lower-Power Wide Area Networks; while the mobile (3G, 4G) communication standards are comprised within the second category.

824 Internet of Things: An Overview (n 154) 47.

825 On the other hand, such a finding would require proven harms that would occur in the presence of exceptional circumstances as well as a dominant player's refusal to supply the APIs which is

This is particularly relevant at the perception layer, as low-power transmission protocols are so diverse and even non-standardised on a truly common basis.

At the access (network) layer, broadband access networks most often serve as the mere conduit for data transmission, which reduces the risk of vendor lock-in. The IoT systems and applications are run on fixed and wireless networks which serve end-to-end connectivity. Cellular networks and standards e.g. GSM, UMTS and LTE, have an increasing share in the IoT ecosystems, considering the potential of mobile handsets and packages for the consumers. As 5G networks are much more promising for the IoT than its predecessors i.e. GSM, 3G and 4G, the deployment of 5G networks is expected to bring out significant benefits for wireless communications, such as high bandwidth, increased efficiency and less latency and have a positive impact on IoT applications.[826] At this layer, common standards dissipate issues of interoperability, while other switching-related problems i.e. based on the remote configurability of SIMs, would prevail, risking the users being locked into their mobile carriers.

As a matter of fact, problems surrounding the configurability of SIMs is an issue that not only creates the risk of vendor lock-in but also threatens the viability of the IoT on the 5G platforms. If the IoT/M2M companies and users running on 4G/5G networks are not able to transfer the SIMs, installed in their manufactured devices, from one mobile network to another, they would get locked to one mobile operator. A solution based on assignment of MNCs – as envisaged under the EECC – would give

indispensable for the competition on the relevant market. See the section '5.3.1.3. Refusal to license/supply interoperability information'.

826 By means of 5G networks, not only seamless low-power IoT communication with much more reduced risk of interference, but also moving analytics closer to IoT edge devices would be enabled (Brown (n 7) 15). Regarding the key features in 5G that will benefit the IoT, see also Vikrant Gandhi, '5G to become the catalyst for innovation in the IoT' (Network World, 13 April 2018), <https://www.networkworld.com/article/3268668/internet-of-things/5g-to-become-the-catalyst-for-innovation-in-iot.html> accessed 9 October 2020.

meaningful results; yet this needs to be checked for the presumably unforeseen implications.[827] While there are other industrial solutions i.e. OTA provisioning of numbering resources, to deal with this switching problem,[828] such solutions require industry-wide memorandum of understanding.[829]

When going up, namely from the access layer to the cloud and application layers, new players come on to the scene alongside the IoT manufacturers, service providers and network operators. Usually, the IoT manufacturers and service providers purchase service from the cloud firms and software developers, which respectively operate in the cloud and application layers. Vendor lock-in risk is high at these layers because of the highly dependent nature of the IoT systems on the clouds and applications.

In the case IoT applications are developed and run by a company as to interoperate with the underlying platform, cloud or device, IoT users would get locked into the featured/supported apps or software. For instance, an IoT health application connected to an only one or two platforms would not be capable of monitoring and conveying health related data e.g. glucose level, heart rate across other platforms, which will otherwise serve locating the person and sending an ambulance to him or her. In such

827 In that case, MNCs are supposed to be controlled either by the connectivity provider (network operator) or IoT service provider. EECC envisages the latter as well as the former being able to be designated as ECS provider. Yet, this would bring about new rights and obligations to be imposed on such undertakings under ECRF. See the section '6.2.2.2.2. M2M transmission services'.

828 OTA provisioning is envisaged as one of the regulatory measures to be invoked by the NRAs under certain conditions (See the section '6.2.2.2.2. M2M Transmission Services').

829 See the BEREC Report (n 31) 30-31. If an IoT user wants to make a change using OTA provisioning, it will always depend on the cooperation of mobile operators and it will certainly not be instantaneous for all devices, in part because it takes time to update devices, and because not all devices will be on at all times (OECD (n 717) 43–44). In addition, there is limited space on a SIM card and mobile operators do not want to reserve numbers for potential customers; so for customers that are roaming occasionally, the device may not be able to select a less expensive local offer, because the credentials have not been updated (OECD (n 717) 44). In the light of these information, key success factors for IoT switching process lie at the EU-wide application of a sound policy choice as well as enabling 'permanent roaming', which, however, are not reflected fully under the ECRF (See Unver (n 30) 111).

cases, unless users purchase and pay for a new IoT product/device, e.g. glucose meter, which is interoperable with the particularly chosen apps, they could not switch easily from one IoT platform/service provider to another because of such technical constraints. Lack of interoperability based on application layer would result in technical restrictions that potentially lead up to walled gardens in contrast to self-regulatory ecosystems.

Lack of interoperability could also be seen at the cloud (platform) layer, originating from implementation of diverse OSs, software architectures, data structures, programming languages, etc. There are currently many different OSs developed specifically for IoT devices such as Contiki, RIOT9, TinyOS and OpenWSN, each with several versions, to deliver services to users.[830] For example, Apple HomeKit supports its own open source language Swift, Google Brillo uses Weave, and Amazon AWS IoT offers SDKs for embedded C and NodeJS.[831] This fragmentation often results in a barrier that needs to be surmounted for the application/software providers in order to develop cross-platform IoT apps. A scenario would be in the case a smart city application, e.g. serving to find the closest grocery, recent movies, etc., would not exchange their users' saved data and/or communicate with other apps, e.g. to make an order or booking with already chosen places, after one particular IoT platform has been opted for. This situation featured at the platform layer, whether resulting from a platform native language or data structure/formats, would cause or facilitate silo type IoT supply structures along with legal, economic and social costs for the society.

[830] Noural, Atiquzzaman and Gaedke (n 827) 799.
[831] Noural, Atiquzzaman and Gaedke (n 827) 799.

Walled gardens would be induced by motivations of profit maximisation e.g. out of network effects or purely quality and/or security concerns tracing back to the trade-offs mentioned above. While every case needs to be analysed based on their characteristic features, fragility of each layer and accompanying interoperability gaps across the IoT settings would turn into unsolvable legal problems and irreparable harms in the absence of intensive and vivid coopetition which usually echoes with self-regulatory ecosystems.

7.2.5. Analysis of the IoT settings under the EU legal framework

IoT interoperability, as the analysis above suggests, denotes an issue that could not be isolated from neighbouring issues and problems, whether relating to IPRs, competition law or sector-specific rules. On the one hand, a great many channels of collaboration and competition among the IoT players would result from the emergent complexity out of IoT ecosystems. On the other hand, industry stakeholders that invest in cutting-edge technologies e.g. AI, machine learning and 3D printing, also deploy some of their resources into the IoT, aiming at advanced big data management including data gathering, processing and analysing, as well as modernising their operations.

As the IoT products gain favour, an important focus of market analysis will be whether a product generates direct or indirect network effects, and if so whether these effects promote and thereby explain consolidation that may occur in markets for these products.[832] Either network effects, or the potential efficiency increases may not be attributed to the IoT itself but to the overall ecosystem that it works in. Crucially, the interdependencies between the layers which underlie the IoT ecosystems have a key

[832] Wrobel (n 252) 64.

role in defining the competitive relationships across the layers and their players. The more determinant such interdependencies are, the less significant and reliable the market definition and accompanying remedies would be.[833] Not only the complexity of the ICT interdependencies but also the efficiencies cutting across the layers - sometimes creating ecosystems – make the market definition an enormously difficult and painstaking exercise.[834] This also means less justified regulatory interventions from the perspective of either EU competition law or ECRF rules.

On the other hand, the prevalence of walled garden type IoT supply structures would affect the cross-layer relationships and diminish the very nature of the ecosystem that is normally built upon coopetition between the interdependent players across the technological layers. In the case of high number of vertically integrated IoT supply structures, walled gardens that are reminiscent of old type silos would not be dismissed at all. This focal point which directly affects the ecosystem characteristics needs to be taken into utmost account across all the industrial settings i.e. from the 'home appliances' to the 'smart city'.

From this viewpoint, many IoT settings, within their current forms, would not match an 'ecosystem', marking a contrast to many of the cloud computing settings. In fact, cloud computing often serves as the bottleneck and utility type facility for the many

---

833 The IoT component could be considered a significant yet complementary service, for the mainstream services e.g. industrial products to be manufactured and offered more effectively and for less cost. However, as time passes with emerging needs and expectations, the IoT-based services would be regarded as stand-alone products creating their own market. For now, it would be speculative to draw definite boundaries regarding IoT-enabled services and products because of the emerging market features. See supra notes 422-423.

834 For instance, wrist bands or tech shirts would create separate markets for many customers would opt for buying such products against SSNIP towards certain aims e.g. following up the calories burnt, the distance covered, movement intensity, heart rate. On the other hand, many other IoT products such as smart TVs that compete with non-smart LCD or Plasma TVs that do not have enhanced features e.g. user interaction on internet could be covered within the same market.

other services, including the IoT. The IoT depends on the clouds, which offer common or middleware services e.g. provision of platform, databases and OSs for the third parties, including the IoT service providers. Clouds therefore play an intermediary role between the third parties and bridge the interoperability gap between them i.e. through protocol translation. On the other hand, most IoT systems, when considered with the underlying standards and IPR-based restrictions, would not create or subsist within an ecosystem, while sustaining a multi-layered basis.

Notably, stakeholders' efforts to push their standards in the IoT environments, particularly in the low-power wireless domain,[835] lead to a puzzled picture in terms of IPRs e.g. SEPs and interoperability relationships.[836] While a number of open source initiatives e.g. AllSeen Alliance, AVnu Alliance (AVB/TSN), Open Connectivity Foundation (OCF) and the Hypercat Consortium prevail and contribute to the IoT standardisation, the fragmentation is remarkable because of the lack of coordination and collaboration between them.[837] It should also be noted that such standardisation efforts lag behind the individual market forces based on the proprietary systems e.g. Google's Home, Amazon's Alexa and Samsung's SmartThings, that are being commercialised and marketed very fast. IPR portfolios, along with the absent common

---

835 See Elkhodr, Shahrestani and Cheung (n 802) 87; Stephanie Sharron and Nikita Tuckett, 'The Internet of Things: Evaluating the Interplay of Interoperability, Industry Standards and Related IP Licensing Approaches' [2016] The Licensing Journal 8, 10.

836 Stakeholders' power struggles over the standards that are applicable to the IoT environment effectively supersede the emergence of a common interoperability-enabling standard under SSOs, consortia, etc. Crucially, while companies might be willing to participate in standard-setting activities by disclosing and openly licensing their entire range of intellectual property, the tools deployed within the context of SSOs to promote that behaviour are currently limited, as they are generally focused on a small set of IPRs, or on a limited notion of interoperability (Zingales (n 62) 29).

837 Going through a collaboration, the OCF and AllSeen Alliance merged under the former's (OCF) name and bylaws in October 2016 (See Open Connectivity Foundation, 10 October 2016 <https://openconnectivity.org/announcements/allseen-alliance-merges-open-connectivity-foundation-accelerate-internet-things> accessed 9 October 2020). While this exceptional merger is appraisable for many potential benefits including interoperability, whether or to what extent such benefits are to be passed on across the IoT industry is questionable.

standards, often affect the interoperability among the IoT systems. As interdependencies and underlying coopetition do not characterise such IoT settings, the lack or insufficiency of interoperability is able to threaten IoT competition and innovation in these settings. In such cases, regulatory/competition law interventions would be responded to cure the accompanying problems such as vendor lock-in or switching costs.[838]

However, no one can exclude the possibility that an IoT setting can turn into an ecosystem structure. From the ecosystem perspective, would-be problems are supposed to be solved within the self-regulatory structure of the ecosystem.[839] This presumption potentially leads up to the conclusion that it is more appropriate to adopt light-touch regulation and/or principles-based regulation for the ecosystems.[840] However, given the above analysis, a cautious and more robust approach would need to be followed within the fragility of the IoT settings. Hence, a regulatory approach ideally comprising ecosystem and non-ecosystem settings would rather be adopted. While ecosystems represent the widest supply structure of all, other structures e.g. narrow IoT settings and cloud environments also need to be embodied by any policy approach and would-be regulatory model.

838 Notwithstanding, such interventions need to follow and build on ascertained conditions and circumstances. These pre-requisites, unravelling the loopholes as to each body of law as described above, demonstrate neither competition law nor ECRF remedies sufficiently cope with the interoperability problems.

839 Cowen and Gawer (n 739) 49.

840 Bauer (n 757) 669-671.

8. Conclusion: Building up the appropriate policy approach and regulatory model

8.1. Summary of the findings

8.1.1. Assessment of the EU legal framework

Interoperability is crucial for running ICT networks and services. It constitutes one of the threads for meeting the ICT-inclusive needs of society. It is remarkable that all the relevant disciplines i.e. IPR, competition and sector-specific rules in EU law have adopted interoperability-centric principles, although each body of law has distinctive goals, principles and instruments. Interoperability is attributed significant meanings and roles under these legal disciplines, albeit with different results and implications.

From the IPR point of view, the debate revolves around whether and to what extent interoperability between the software systems needs to be considered as an exemption to the protected subject matter at stake. For instance, whether the interfaces of ICT services and products that are distributed in object codes should be covered by copyright protection is currently the most debated question in the copyright context. With regards to not only the copyrights, but also the patents, trade secrets and database rights underlying the ICTs, it is not unequivocally set out under the EU law as to the extent to what interoperability is warranted as a secure ground or given right for the third-party access seekers.

The unclear boundaries of interoperability-based exceptional rights is a common concern in the academic scholarship, as over-protection of IPRs incorporating the interfaces is acknowledged to result in unpredictable or disproportionate impacts

regarding new entries to the marketplace, innovation and information flows. In practice, IPRs are spread across the ICTs, with a view to create a shield against third-party access to the underlying software, including the interface specifications. This situation however aggravates the concerns based on the vendor lock-in, particularly when the rights holder has a dominant position in the relevant market(s) and is able to heighten the switching costs for the consumers and prevent third parties from creating derivative products. These concerns go beyond the permissibility of interoperability for ICT products and services i.e. software and hardware, and reach out to the informational barriers and cultural productions, and ultimately to participatory democracy.[841]

As the IPR-based rules are not designed to and primarily aimed at, dealing with lock-in and accompanying anti-competitive conducts, EU policy makers have thus far preferred to invoke competition law in the relevant cases. Not only technologically, but also on the contractual basis, the possibility of customers being locked into a dominant product is usually not welcomed by the EU competition rules, which are designed to keep the markets effectively competitive and to increase consumer welfare.

Even in the markets which are subject to sector-specific or IPR-based measures i.e. copyright exemptions based on reverse engineering, EU competition law rules have an overriding effect and applicability should a breach of competition rules take place. Being not limited to the software-to-software compatibility, any market failure that needs to be solved across concentrative actions e.g. M&As and joint ventures,

[841] See the section '3.1.2. Main concerns surrounding lack of interoperability'.

coordinative undertakings e.g. agreements and concerted actions, and unilateral behaviours e.g. abuse of dominance, falls within the scope of EU competition law.

Notwithstanding, EU competition law rules and remedies reveal several shortcomings, which need to be underlined. Firstly, high thresholds e.g. dominant position and uneven pre-requisites e.g. exceptional circumstances, are sought for the implementation of EU competition law. Secondly, while EU case law lays out a firm policy in favour of interoperability and effective competition, the enforcement procedures entail a lengthy process to be confronted by the related parties. The *Microsoft* case illustrates such an unbearably long process of enforcement, which lasted for nearly a decade subsequent to the Commission's decision.[842] While able to produce an interoperability-enabling and competitive result, such a lengthy process would not be sustainable, particularly in view of the deprived societal benefits, would-be closed market(s) and further implications based on the affected information flows.

Against this background regarding the limitations of EU IPR and competition law rules, the ECRF needs to be fleshed out as another source of law for enabling ICT interoperability. The ECRF means a regulatory framework under which interoperability is featured as a core value and a principle, particularly to ensure end-to-end connectivity. Ex-ante tools of the ECRF partially respond to the problems unsolved by the EU competition rules, sometimes going beyond the 'consumer welfare' standard by not seeking a likely consumer harm and protecting the consumers regardless of the demand and supply parameters in the marketplace. While interoperability is also covered within the dominance-based rules of the ECRF e.g. the

[842] See the section '5.5. Assessment of EU competition law'.

SMP regime, this is subordinated to its consumer-oriented and end-to-end connectivity based approach.

The interconnection policy of the ECRF illustrates this regulatory mind-set. In fact, while the SMP (dominant) players are obliged by the NRAs' market analyses to provide interconnection e.g. call termination and origination through their networks, similar obligations comprising interoperability might also be imposed on non-SMP players under certain conditions e.g. when end-to-end connectivity is at stake. Likewise, according to the CAS obligation covered by the ECRF, interoperability between the CAS provider and broadcaster needs to be secured when the content transmission is to take place via the former's conditional access system e.g. set-top box. Considering that consumers' access to their intended content is crucial for media plurality and cultural diversity, the ECRF mandates access to and interoperability with the underlying technological platforms, without regard to any potential competition problem. Similarly, EU net neutrality regulations comprise all of the ISPs, regardless of their market power or any potential anti-competitive behaviour, considering the 'gatekeeping' functionalities that could emerge.[843] Having said that, although a great many concerns are well responded to within the context of the ECRF, the regulatory tools and instruments in it are of a non-holistic and disaggregated structure.

[843] According to EU Regulation 2015/2120, all ISPs are required to "treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used" (Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union ('EU Net Neutrality Regulation') art 3(3/1).

Primarily speaking, the ECRF has a legacy aim of removing the monopolies and regulating the infrastructural elements of ICT services. While the broadly designated policy objectives[844] warrant a wide range of regulatory means, NRAs are bound up with certain boundaries, primarily based on the 'transmission' and 'content' distinction. Focusing on the former, the ECRF allows NRAs to intervene in not every case of ICTs, but those related to the ECSs and not entailing IP-based data transmission and interconnection, nor covering many upper layer services – apart from certain exceptions e.g. number-based ICSs for consumer-protection reasons. Hence, an access or interoperability problem occurring in the domain of other ICT services than ECSs falls within the remit of EU competition law, but not the ECRF, principally.

At this point, it needs to be emphasized that electronic communications networks and services representing the lower layer ICT services, may not be the source of the problem e.g. market failure or informational barrier, in every case. Other ICT services could equally be the cause of the related problems surrounding lack of interoperability. Thus, it is criticisable to leave out some ICT cases following the legacy viewpoint of the ECRF.

The lack of interoperability does not automatically pose a threat by itself and all the ICT layers and services do not have to be regulated *a priori*. Nevertheless, regulators should be aware of the need to consider all the ICT layers and the interdependencies among such layers. While the interdependencies across the layers, particularly in an ecosystem environment, might reduce or eliminate the need to regulate interoperability,[845] the legacy mind-set and remit of the regulations i.e. ECRF needs

844 EECC Directive, art 3(2).
845 See Cowen and Gawer (n 739) 49.

to be checked out in any case. Before elaborating the possible ways to revise this remit and concerning how to advance an appropriate regulatory model, findings from the case studies firstly need to be taken into consideration.

8.1.2. Assessment through the lens of case studies

As emphasised above, from the interoperability perspective, EU-based solutions have shortcomings in terms of completeness and coherency. The pertinent rules of the EU legal framework fall far from being fully responsive and effective against the lack of interoperability and accompanying problems across the ICT layers. To evaluate the multi-layered aspects of ICT interoperability and delve into policy elaboration, along with an appropriate, holistic regulatory design in the end, cloud computing and the IoT have been examined as the case studies of this thesis. The case studies, having both explanatory and exploratory nature for technical and economic assessment of such layers, have led to important findings on how to restructure regulatory pillars in a holistic way.

Cloud computing denotes an environment whereby a great many stakeholders e.g. software developers, security firms, virtualisation companies and network operators, collaborate and/or compete. Under the management and coordination of the cloud provider, cloud computing services, which include hosting, processing and updating relevant software and data, are offered to the users. While cloud architectures rely on three components, or internal elements, consisting of ‘infrastructure’, ‘platform’ and ‘application’ layers, this tripartite structure expands with the underlying external elements, namely content delivery and broadband access networks, which constitute

the 'access' layer.[846] When considered with these external elements, cloud computing architectures most often turn into ecosystems, which inhabit players i.e. ISPs, CDNs, CPs, coopeting with each other via their respective strategies and means.[847] This transition from the cloud 'environment' to the cloud 'ecosystem' provides us with an in-depth outlook, allowing us to revitalise the interoperability debate.

Primarily, the interdependencies within the cloud settings of the 'environment' and 'ecosystem' have different breadths. While in the cloud environment interoperability is limited to the interlinks between the 'infrastructure', 'platform' and 'application' layers being governed by the cloud provider, such interlinks expand and deepen in the cloud ecosystem. In the ecosystem setting, the volume and intensity of the interdependencies culminate in the 'coopetition' among the players, namely cloud providers, the CDNs, ISPs and CPs. This 'coopetition' minimizes the need to regulate interoperability gaps as they are being governed and filled through the cross-layer, even sometimes 'symbiotic', relationships.

This does not mean ecosystem-wide 'openness', as opposed to the proprietary systems, but rather it denotes the self-sustainability based on the interoperability channels neutralizing the effect of walled gardens.[848] This situation is comparable to 'contestable' markets, which are depicted by low barriers to entry and exit along with

---

846 See the section '7.1.2.2. Cloud ecosystem with external elements'.

847 Notably, the term 'ecosystem' is used with differing meanings and purposes e.g. describing a plethora of software apps surrounding a 'platform' – platform ecosystem, within the literature. While having some overlaps with such definitions, the approach used in this study entails 'coopetition' in itself as the core component. According to this approach, 'complementarity' and 'substitution' are not as influential as 'coopetition' which come about with the interdependencies of the ecosystem players (See the section '7.1.3.2. Interoperability in the cloud ecosystem').

848 Within the context of those channels, should be noted the industry-led findings and solutions to achieve interoperability, whether based on standardisation e.g. NIST's effort to create vendor-agnostic technologies, or architectural solutions e.g. microservices, containers. See Sandeep Shilawat, 'Cloud Interoperability and Portability' (*Forbes*, 22 June 2018) <https://www.forbes.com/sites/forbestechcouncil/2018/06/22/cloud-interoperability-and-portability/#5512c41f4577> accessed 9 October 2020. See also Unver (n 27) 164.

short-term prices and price-sensitive consumers.[849] Across such a potential for competition e.g. when switching is easy and fast, lack of interoperability no longer has the effects of preventing new entries and/or innovation. However, in such situations, competition dynamics shift from the market or platform level to the ecosystem level, whereby no classic "silos" could survive without a competitive threat across the layers. What is more, not only competitive but also co-operative relationships exist at the same time, heightening the difficulty to designate the boundaries for any ICT market.

In this broader setting of a cloud ecosystem, crystallising a lack of interoperability based on a one or two-sided market relationship, would mean isolating a problem from a narrow-minded perspective with potentially negative implications for the cloud users e.g. by chilling innovation and affecting competitive equilibrium(s). Most potential efficiencies that are engendered by the cloud-based competition and innovation and would emerge in the larger industry settings e.g. ecosystems would also be dismissed in the case of smaller scale definitions e.g. based on a market or platform.[850]

The IoT, similarly, entails various settings and different organisational supply structures based on several layers and components. IoT systems, while having unique architectural elements, including devices, sensors, microprocessors, etc., depend on clouds and broadband access networks, which all constitute interdependent layers underlying IoT applications and services. Constituent IoT elements are widely acknowledged to comprise the 'perception', 'access (network)' and 'application'

849 Alberro and Shcwabe (n 155).

850 The limitedness of the market-based approach across the efficiencies and interdependencies could also be caught from the *Microsoft* decision. While the *Microsoft*-formulated 'incentives balancing test' has not been applied fully in the *Microsoft* finding, the Commission's reference to *'*the level of innovation of *the whole industry*' instead of market-wide innovation remarkably hints on the limits of the market-based approach. See also supra note 506.

layers, albeit with absent classifications for the internal or external elements.[851] These layers represent not only the technological components interlinked by the interfaces but also the value chains demarcated by the economic activities of the IoT players e.g. IoT platform/service provider, connectivity provider and software/apps developer. The IoT layers comprising wireless LANs (WLANs) and broadband access networks and clouds that serve as the middleware layer for the IoT service provisioning, interact with each other creating the cross-layer interdependencies. As a result of such interdependencies, an ecosystem setting would emerge insofar as they build on the coopetition between the IoT players.

From this point of view, IoT settings resemble the cloud's 'environment' and 'ecosystem' settings in terms of the cross-layer interdependencies, which potentially refashion the competition and innovation dynamics. However, differing from the clouds, IoT systems are not functioning as bottleneck intermediary services for ICT connectivity and usage. Additionally, IoT settings e.g. smart city, smart energy, public transport, telemedicine and industrial processes, being so diverse and fragmented, drive the respective SSO processes on an unintegrated basis. Furthermore, stakeholders are pushing their own standard and/or protocol for IoT systems, trying to gain a significant advantage from the potential markets. As a result, silo type walled garden structures and vendor lock-in cases are far more confrontable in IoT settings, compared to the cloud environments and ecosystems. As a matter of fact, coopetitive and symbiotic relationships could not be attributed to many IoT driven settings or sectors, e.g. transport, smart city and telemedicine. This, however, creates significant challenges for the emergence of ecosystem characteristics.

---

[851] See the section '7.2.3. Architectural elements and layers in the IoT'.

Given this fact, many IoT settings boast far more interoperability problems and gaps, when compared to the cloud settings. While both cloud and IoT settings are fraught from the absent multi-layered common standards, clouds are typified by utility and bottleneck characteristics, which bridges the interoperability gaps as the major hubs for the ICT interconnectivity and usage. This and other aspects of cloud computing e.g. ever fast increasing cloud adoption by the entrepreneurs,[852] and its closer interlinks with the external elements e.g. CDN, broadband access networks, bring out the result that clouds are far more depicted with the 'ecosystem' characteristics, e.g. coopetition among the players.

On the other hand, it is always possible that walled garden structures including IoT silos could turn into ecosystems ensuing intensive and pervasive cross-layer interdependencies. Having said that, in response to the diverse possible scenarios to be faced by the regulators, the legal system should be flexible enough to entail ecosystem and non-ecosystem settings, just as it needs to be holistically designed. Given the fact that the EU legal system is of an inflexible, fragile and non-holistic nature, an overhaul based on a wider outlook seems compelling, particularly from the perspective of ICT interoperability. Alongside the ecosystems that represent the widest supply structure, other supply structures or settings also need to be comprehended and included within the regulatory model to be designed.

[852] See supra notes 731 and 750.

8.2. Policy refinement and elaboration for the EU legal framework

8.2.1. Refining the assessments: Setting out the baseline policy approach

Under the EU legal framework there is no holistic treatment for ICT interoperability. Notwithstanding the pressing need to have a wider outlook, to evaluate the ICT services and layers, the EU system is built on disaggregated instruments, which cause some significant gaps and overlaps. Not only to deal with the lack of interoperability but also to have a sustainable and holistic regulatory framework, the EU legal framework needs to be revitalised with broadly and appropriately designed new rules.

To emphasize, the EU's predominantly market-based approach relies on a narrow-minded approach by which some parts of the ICT ecosystems are dealt with via regulatory rules, whereas others are not. Although one should refrain from a simplification that all ICT services be regulated, as this would not automatically remedy the access and interoperability problems. Instead, filtering the ICT layers from a holistic regulatory lens arises as a necessity for the evaluation of the regulatory and competition problems, including the lack of interoperability. Flowing from this, a holistic and fulfilling regulatory analysis across the ICT interdependencies should be possible, as opposed to the *status quo*.

In the current ICT ecosystems, systemic interrelatedness goes beyond complementarity and substitutability; complex patterns of feedback and non-linear developments arise, and micro-level decision making becomes uneasy with the multiple dynamic equilibria of such systems.[853] Regarding the ICT supply structures

[853] Bauer (n 757) 666.

as ‘static’ by narrowing them down into markets does not well respond to the cross-layer interdependencies. In fact, neither the underlying concepts for market analysis i.e. complementarity and substitution, nor the accompanying instruments i.e. the SSNIP test, are inclusive and holistic enough as they aim to segment the ICT landscape into markets, leaving out the cross-layer efficiencies, innovation and competition.

In view of the interdependencies, a potentially new regulatory approach needs to embrace all the supply structures including ecosystems and non-ecosystem settings, given the cases of the IoT and cloud computing. From the perspective of these case studies, it is clear that various settings would tend to regulatory and competition problems. Although many other settings could be found leaning towards ecosystems, this should not be taken as reflecting all the scenarios in which the ICT networks and services are supplied. Thus, a purely ecosystem-based approach would overlook narrower ICT settings and not fit well with many situations e.g. where silo-type vertically integrated firms exist. In such a situation, as represented by many IoT settings, absent controlling or mitigating tools would result in augmented interoperability gaps and problems e.g. vendor lock-in. For instance, when a dominant IoT-based software management system has a partnership with certain applications and devices, it could be considered to create a market and/or a platform, but not an ecosystem.

This contrasts with the cloud-type ecosystems where ex-ante regulation is no longer needed for self-regulatory functionalities e.g. coopetition across the layers. The concept of ‘coopetition’ is of a key role for acknowledgement of an ‘ecosystem’, involving both cooperative and competitive relationships, and existing horizontally and vertically, e.g. between the IoT platform/service providers, manufacturers and the

software developers. These vertical and horizontal relationships, echoing layer interdependencies and denoting the ecosystem features, has also the key potential to dissolve the interoperability-based problems.

Against this background, the layout on which the regulatory design will be shaped out needs to be flexible and holistic enough to reach out to ecosystems, as well as to non-ecosystem structures. In other words, both self-perpetuating ecosystems and other settings that warrant regulation need to be comprehended and covered by the regulatory model that is to be built up. Having said that, technologically neutral, widely applicable and interdependent layers would provide the appropriate layout or the ideal building blocks for a regulatory model.

Overall, a well-designed layering-based approach, by which ICT layers are regulated to the appropriate extent, seems to be sustainable and widely applicable as this approach will provide the regulators with the necessary dynamic ground for defining and remedying the related interoperability problems. Before delving into regulatory design of the appropriate model, it needs to be clarified whether the ex-ante or ex-post approaches need to be followed within this context.

8.2.2. Policy choices between ex ante and ex post

Although interoperability has so far figured as one of the important policy items of the EU agenda, it has not been translated into the ICT regulations at the equivalent level. While the ICT-based transformation, which is echoed in the fourth industrial revolution or Web 4.0 paradigm, has unraveled new challenges e.g. AI, cloud computing, IoT, these have yet to be resolved from a broader interoperability-based perspective.

EU IPR rules and safeguards, which are privately enforced, are of a limited role in this respect and hence ICT interoperability becomes much more of an issue to be solved by means of competition law and sector-specific ECRF rules. While under EU competition law there is no such a self-standing interoperability rule, the ECRF attributes a key underlying role to interoperability. Not only this stark distinction, but also the very nature of the ECRF e.g. more detailed, target-based and ICT-enabling character, would promise more responsive solutions to interoperability problems.

From a broader point of view, NRAs being equipped with wide-ranging roles and responsibilities i.e. authorization, monitoring, dispute resolution, access, tariff and competition measures, provides a comparative advantage over EU competition law, which mainly consists of ex-post remedies. While some competition law tools e.g. merger control entail ex-ante measures, these are applicable to the concentrative and/or cooperative relationships at hand, being limited to the related parties. For instance, the Commission's *Microsoft/LinkedIn* decision, whilst entailing a detailed and pro-interoperability intervention, is not applicable to the parties outside of the merger.

Arguably, competition law interventions such as the Commission's 2004 *Microsoft* decision could have far-reaching implications, exceeding the boundaries of an ex-post remedy. Any super-dominant firm like Microsoft, subsequent to this decision, would have to either refrain from withdrawing the interfaces in order not to be considered as abusing its market power, or envision a long-term policy to not disclose any of their proprietary interfaces from the beginning.[854] For substantiating and evidencing an abuse of dominance, resources to be deployed by the competition authorities would be enormous, considering the decade-long *Microsoft* case. Not only the duration but also

[854] Unver (n 27) 162.

the uneven standards applied in *Microsoft* pose a hazy ground for any intervention of this kind and elevates the uncertainty for the market actors. Remarkably, the emergent uncertainty would easily disrupt the uneasy balance between the short-term and long-term competition in favour of the former along with potentially lessened innovation. From this viewpoint, establishing and maintaining the trade-off between these two goals is hardly achievable under the EU competition law precedents.

On the other hand, at the disposal of NRAs which are in charge of implementing the ECRF, are timely and directly applicable rules and remedies. To emphasize, 'interoperability' is attributed a key role under the ECRF, although designed as subordinated to interconnection, end-to-end connectivity, etc. When certain harms e.g. regarding end-to-end connectivity and access to emergency services are at stake, access and interoperability remedies could be applied without regard to 'consumer welfare', which requires elaboration of likely costs and benefits in case-by-case analysis. While the latter, basically competition law grounded, approach promises more elaborate and substantiated findings, this would come up with undeniable costs e.g. ineffective and belated solutions, for it looks at the entirety of the circumstances through long-lasting investigations. All the underlying circumstances being considered in each case, is ironically deemed to be an important aspect of competition law; however, not only the accompanying cost for this but also the inadequateness of the underlying notion of 'consumer welfare' is compelling for a broader regulatory thinking.[855]

[855] Regarding inadequateness of the notion of 'consumer welfare' see the section '5.5. Assessment of EU competition law'. See also José van Dijck, David Nieborg and Thomas Poell, 'Reframing platform power' (2019) 8(2) Internet Policy Review, 4-6 <DOI: 10.14763/2019.2.1414> accessed 9 October 2020.

A good harmonisation of static and dynamic rule making, is implicated in many areas of DSM initiative,[856] reflecting this broader thinking, if not sufficiently, and having the potential to promise effective and timely results in terms of consumer satisfaction and interests. Likewise, representing a consumer-oriented regulatory framework under which both dynamic and static elements co-exist, ECRF incorporates a set of effective and responsive tools if not from a holistic perspective. Through such a combination based on a wider perspective, certainty and flexibility could exist and be harmonised under ex-ante regulation, as needed to be reflected in the intended regulatory design.

It is remarkable that EU authorities, having regarded the competition law tools as insufficient to achieve such objectives, focused on the enhancement of the ex-ante tools and considered the DSM process as a significant leverage for this. While the legislative measures regarding cross-border content delivery, (un)interrupted data flow and portability and the transparency of the platform-to-business relationships[857] illustrate these recent steps made in this regard, it is note-worthy that their added value primarily stems from their ex-ante nature in the first instance. The EU's recent attempt to regulate the digital platforms for their wide-ranging economic powers and capabilities, should also be read from the same outlook.[858]

On the other hand, EU legislative measures have a patchy and complicated nature, which might sometimes have the opposite effect to what is intended. This flip side of the coin could worsen the situation of the ICT actors and diminish the so-called advantages to be gained from the ex-ante regulations. Therefore, while the main

856 See supra notes 615-17.
857 European Parliament, 'Legislative Train Schedule' <http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market> accessed 9 October 2020.
858 See supra note 193.

regulatory path would ideally be ex-ante, it is equally important to strike the right balance between flexibility and predictability.

Ostensibly, the ever-faster-growing nature of the ICTs has driven the fast-paced development of the ex-ante tools and measures under the DSM in recent years, and this seems to go on further. However, it is debated as to whether such safeguards would alone suffice to respond the multi-layered regulatory problems surrounding interoperability. Thus, would-be ex-ante rules and regulations had better aim to filter the interoperability-based problems for the interdependent layers, seeking out coherent solutions in the field of ICTs. Reflecting this, details of the ex-ante regulatory model that is to be proposed by this study are elaborated below.

8.3. Layering theory and regulatory implications

After concluding that interoperability and accompanying problems could be better addressed with an 'ex-ante' and 'layering-based' regulatory model, the next task is to determine the main pillars and contours of the model. Having said this, it first needs to be reemphasized that the intended regulatory model should have a holistic and flexible nature. The layering perspective and approach should thus be fit for purpose. Given this the starting point will be the investigation of the layering theory that is built upon, via elaboration of the IP layers, to design a regulatory approach. Based on this, the proposed framework and necessary details of the intended regulatory model will be set out.

8.3.1. Layering theory and models in general

The internet layers and governing protocols i.e. developed under Open Systems Interconnection (OSI) or TCP/IP stacks[859] lay the ground for development of the 'layering theory', which generally means adapting the IP layers to policy and regulatory approaches. The vital role of the protocol layering within the IP ecosystem came to the fore in the late 1990s and had a remarkable influence on the literature with regards to the reconstructing of the regulatory policies. IP-based convergence, along with the layer-based internet structure, led scholars to revisit the conventional sector-specific policies focused on the regulation of certain infrastructures e.g. the PSTN, which were considered as natural monopolies or essential facilities at the time.

This conventional regulatory establishment in the 1990s was criticised as being technologically biased and adopting a single-minded approach concerning the communications networks and services. As a response, particularly in the USA, layering theory was found to pave the way for an environment whereby regulatory rules against different networks, e.g. cable, the PSTN and services, for example VoIP and voice telephony, were to be filtered on the basis of convergence across the internet layers (TCP/IP) on a technologically neutral basis. The effective outcome of adopting the layering theory mainly incurred challenging the regulatory rules that were designed to regulate certain vertically integrated networks, so-called 'silos'.[860]

The layering-based approach is usually credited, as it allows that each module or layer of the whole ICT system could be analysed in a self-contained division, whilst

[859] See the section '2.2.1. Architectural underpinnings of the internet: Layered IP Stack'.
[860] See the section '2.2.2. Convergence'.

acknowledging the interdependence among the layers,[861] namely the 'physical', 'logical', 'application' and 'content' layers, as widely accepted.[862] Having regard to the cross-layer interdependencies, Fransman, developed business and innovation models built upon the layering theory and fleshed out its implications for the industrial dynamics. While acknowledging the distinct natures of the layers, Fransman underlined the interdependencies between them and reached the conclusion that there exists a symbiosis between the ICT layers and players, invoking the 'ecosystem' approach at the core of his narrative and proposition.[863]

Overall, layering theory and its approach was first intended as a tool for examining policy implications on technology and later evolved into a policy model intended to promote a technically neutral view of the various emerging network platforms.[864] On the techno-political ground cultivated by this, several 'regulatory models' have thus far been developed, inspired by the theory.[865] The main arguments of the policy proponents for layering models evolved on the; (i) differentiated treatment for each horizontal layer along with a lighter regulation in the higher layers and[866] (ii) adoption of a more technology-neutral and refined regulatory treatment for the ICT networks and services.[867]

---

861 Nuechterlein and Weiser (n 96) 164; Whitt (n 752) 592.

862 See also supra note 752 and infra note 869.

863 Fransman (n 118) 37-38. Fransman invokes the biological concept of "ecosystem" to analyse the developmental pathways of the ICT layers that implicate six symbiotic relationships. The focal point of his study concerns how to enable and develop innovation potential across the layers, with important implications for the European ICT sector.

864 Mindel and Sicker (n 752) 140.

865 See Kariyawasam (n 752); Kariyawasam (n 118); Werbach (n 118); K. Werbach, 'A Layered Model for Internet Policy', [2002] 1 Journal on Telecommunications & High Technology Law, 39-54; Whitt (n 752); Mindel and Sicker (n 752); D. Sicker and J. Mindel 'Refinements of a layered model for telecommunications policy' [2002] 1 Journal on Telecommunications and High Technology Law, 69-94.

866 Sicker and Mindel (n 865) 79; Werbach (n 865) 59-60; Whitt (n 752) 632.

867 Sicker and Blumensaadt (n 130) 302; Werbach (n 118) 58-60; Sicker and Mindel (n 865) 79-81.

Scholarly perception of the theory led to the idea that heavy regulations were to be attributed to the bottom physical and transport layers, whereas the upper application and content layers were to be subject to zero or minimum sector-specific regulation because of their very characteristics e.g. being conducive to innovation and no serious upfront costs for operation with no bottleneck aspects. As an exception, Kariyawasam suggested a broader and systemic approach called the "layered policy model", in which layers are configured enabling a more homogenous and holistic regulatory treatment and pertaining to ECSs, in the broadest sense.[868]

Rather than describing each layer as strictly representing the providers of the services, Kariyawasam argues that an ECS could either fall in its entirety into one of the access, transport, application, or content layers,[869] or will have component parts that will fit into any one, or several of the layers, simultaneously.[870] In a systemic approach, Kariyawasam suggests to regulate the operators that run their multi-layered activities based on the type and amount of the IP packets, namely the volume of the data traffic that transcends each layer - by means of deep packet inspection and allocating them into each layer via accounting seperation.[871]

---

868 Kariyawasam (n 752) 100-104; Kariyawasam (n 118) 41-50.

869 Albeit with nuances, the layering-based regulatory models depend on four distinct layers, comprising 'physical or access', 'logical', 'application' and 'content' layers (Whitt (n 752) 624, Werbach (n 865) 59), although the 'logical' layer is being replaced with the 'transport' layer by some others (Kariyawasam (n 752) 99; Sicker and Blumensaadt (n 130) 310). In these latter models, a more technical perspective is being reflected along the lines of the original internet stack i.e. the TCP/IP model. Despite this close matching, this study leans towards the former approach that incorporates the logical layer along with other layers i.e. access, application and content, because this far better reflects the economic and industrial realities. See also Derek Wilding and Ivor King, 'Reviewing the Layered Model' [2018] 46(1) InterMEDIA, 13-17, for the comparative analysis of the layering-based models, including the layers chosen by the developers.

870 Kariyawasam (n 752) 101; Kariyawasam (n 118) 597.

871 In so doing, Kariyawasam focuses on; (i) the definition of the relevant market and (ii) the establishment of market strength, but not further details i.e. regarding the remedies. Except with such details, Kariyawasam adapts the SPM regime and pillars to the layering theory, ending up with a unique 'layered policy model' developed by him.

Considering the ICT layers not in a self-divided manner but rather as components of ECSs, this proposed model ends up with new definitions regarding electronic communications network and services and criteria regarding market definition and market power, to replace the legacy ECRF rules, specifically SMP regime. While doing this, the volume of the traffic across the layer(s) is attributed a key role to determine market presence, with direct implications to determine SMP in the relevant layers, instead of markets. The established link between the amount of data transcending each layer and the market power makes Kariyawasam's model a unique one and fully based on IP convergence and transmission, from a holistic viewpoint. Since then, no further model has been developed to refashion the regulation of the ICT networks and services based on the layering theory.

8.3.2. Critical analysis of the layering models

After an overall analysis, one could infer three common aspects that could be attributed to the layering models: (i) categorisation of the ICT networks and services under horizontal 'layers', (ii) technologically neutral treatment of the layered networks and services, and (iii) differentiated treatment of the horizontal layers. The most prominent aspect of the layering models is reconceptualising the ICT layers so as to identify the problematic areas where the market failures would occur. Targeted regulation based on the layering models is to ensure that market failures do not occur, that market power at lower layers cannot be levered into control of upper layers and that policy objectives are achieved in the face of market incentives.[872] In this setting, the lower layers are believed to be kept under ex-ante regulation, whereas the upper layers are largely left

[872] J. B. Meisel and M. Needles, 'Voice over Internet Protocol (VoIP) development and public policy implications' [2005] 7(3) Info 3, 14.

to market forces, considering the innovation potential of the latter as opposed to the bottleneck aspects of the former.

However, these presumptions are open to criticism under the light of the detailed analysis given in this study. As a matter of fact, the extensively voiced differences between the upper and lower layers in terms of innovation and bottleneck features faded away and are no longer relevant today. Notably, the undertakings that represent the lower layers i.e. traditional telcoes, have long been and are still under regulatory pressure, posing questions as to the equal footing between these and the upper layer firms i.e. software companies, which has appealed regulatory attention in a slower pace through the last decade. Existing regulations, i.e. net neutrality, being applicable only to the ISPs, signifies and exemplifies the distinctly marked boundaries between the lower and upper layers, in contrast to the ever fast increasing IP convergence.[873]

By the same token, telecom operators, which represent the characteristics of the access layer, increasingly invest in network configuration, virtualisation and softwarisation, whereas the software companies have already expertise in these areas, taking this advantage to get closer to the users through data-driven software and apps, voice assistants, handsets or devices, smart watches, etc. As a matter of fact, the broadband access networks often serve just as the mere conduit for the users, who meet their ICT-inclusive needs from the popular software companies e.g. the so-called FAGMA of Facebook, Apple, Google, Microsoft and Amazon. While FAGMA manipulate the users' behaviours with a view to make them rely on their services, their already

[873] The upper layer companies could be argued to have taken these advantages in order to maximise the benefits flowing from the convergence. As a result, the locus of the central operations meeting the users' ICT-inclusive needs appears to be shifting from the bottom layers towards the upper ones, mitigating the differences between the ICT players.

reserved areas for competition and innovation help this to be managed more thoroughly e.g. with the AI support and configuration.

From this vantage point of view, a more neutral and homogenous treatment arises as a key component and to be attached to the layered regulatory model to be proposed by this study. Drawing a distinction within the layering-based models, Kariyawasam's model suggests layers be treated in an equivalent manner, based on the measurement of IP data, as per the protocols used, to designate the SMP players. Hence, the model proposed by Kariyawasam diverges from other models for its advanced regulatory homogeneity across the layers. It is important to note that the homogenous and equivalent treatment of the layers, as featured in this model, arises as the key aspect of a regulatory model because of the reasons explained above.

On the other hand, not only Kariyawasam's model but also other layered models heavily focus on the IP layering and protocols, with no delving into the economic relationships between the layers and players. While IP convergence drives data transmission being considered as a common thread of the layers, the abovementioned locus of the users' activities and the potential threats over them e.g. because of lacking interoperability, needs to be prioritised. Data transmission means the path, being represented by IP stack, along which the IP packets go and reach their destination. Notwithstanding, neither controlling power of the 'gatekeepers' across the layers nor their restrictive activities are well depicted within the so-called IP stack and related models. That is to say, the potential restrictions over this data transmission needs to be considered as equally important as the transmission path and calculation of data transmitted through the IP layers.

To illustrate, in the case of discriminatory traffic management e.g. blocking or throttling unaffiliated content by the ISPs, account is and ought to be paid to the gatekeeping activities and the attributable consumer harms, but not to the amount of the transmitted data. Likewise, in the case of access to the CAS facilities, CAS operators e.g. set-top box providers are required to provide access regardless of the amount of transmission, or market power, but just because of the CAS operators' gatekeeping position. Other cases regarding access and interconnection could also be compared to the so-called gatekeeping functionalities, particularly when wide-ranging restrictions would make the users worse off in terms of the potential choices they would have, for example regarding connectivity, speed and quality. These concerns need to be extended to the absent free information flows and its techno-social underpinnings particularly in view of the restricted participatory democracy and cultural production. Summing up, rather than the volume of the transmitted data and/or market power, prevention and/or manipulation of data flow appears as the real determinant for the intervention, as reflected in the net neutrality and the CAS regulations.

The intended outcomes of ECRF regulations, including net neutrality and for CASs, signify co-existence of the economics-based, mostly competition-oriented, aspects and the non-economic characteristics that are of mostly techno-social nature under the same regulatory framework. While both types of 'competition' and 'techno-social' concerns find a room under the ECRF, in parallel with the shifting locus from the lower layers to the upper ones, the latter concerns need to be prioritised because of the changing ICT dynamics. Online activities which are run by data-driven algorithms and manipulative AI technologies may cause access/interoperability restrictions and covert discrimination at the upper layers, which may not well match the typical activities of

the lower layers e.g. denial of access or interconnection, that are well responded and sorted under the ECRF.

As the software-based manipulations, access or interoperability restrictions and discriminations supplant those formerly seen e.g. mostly overt and infrastructure-based access restrictions, the attention primarily needs to be paid to the 'gatekeepers' along with their gatekeeping involving activities as are encountered at upper layers. Having said that, it becomes compelling to examine the 'gatekeepers' rather than dominant undertakings, across the layers, embracing access and interoperability restrictions and responding to them effectively and from a broader point of view. Given this fact, not a purely transmission-based or SMP-oriented perspective, but rather gatekeeping-centric and holistic perspective needs to be upheld in designing the layered regulatory model.

8.4. Construction of the 'layered regulatory model'

8.4.1. Main features of the model

In building up a layered regulatory model that is both 'holistic' and 'flexible', the crucial point is to have a systemic approach along with the functional tools and criteria to be applicable across the layers. In so doing, the first task is designation of the layers. The layers to be adopted need to match and reflect both the technical and economic realities of the ICT networks and services. Whereas the protocol stacks analysed in the Chapter 2 represent the technical layers that were promulgated by the SSOs e.g. IETF, ISO, this thesis has not directly opted adopting any of these.

As implied above, scholarly adopted layers, if not the models, were found to better reflect the gatekeeper positions or the so called gateways across the widespread economic value chains.[874] Given the need to consider the IP layers that truly represent such interdependent chains as well as the prevailing restrictive acts across them, the layering approach followed here aims to abstain from the technical restraints that were embedded with the formerly adopted layer stacks, particularly those of the SSOs.

From the given standpoint, this study proposes that the 'layered regulatory model' be built on the following four layers: (1) Access Layer, (2) Middleware Layer, (3) Application Layer and (4) Content Layer. The main distinctive features of each proposed layer are explained below:

1) Access layer: Includes both passive and active network elements that enable the conduit and the intelligence necessary to provide end-to-end connectivity. By means of the QoS and technical standards, the access layer offers the broadband connectivity which is key to all the other upper layers, including middleware, applications and content.

2) Middleware layer: This denotes the layer where the software infrastructure, including OSs, management tools and data structures, resides and enables running of the applications. Serving as the medium to support the users, software developers, etc., this layer is employed by the platform owner or the cloud provider, the latter being the increasingly utilised option.

[874] Among these, the four-layer stack model containing access layer, middleware layer, application layer, content layer is preferred instead of more technical ones e.g. access, transport, application, content layers. At this preference lies the better exposition of the economic realities of the ICT activities being mirrored in interdependent value chains. See supra note 869.

3) Application layer: Includes apps and web services e.g. e-commerce, e-mail and instant messaging and is used for a variety of purposes such as entertainment, communication, transactions, etc. Often running from the clouds and being displayed on the devices e.g. tablets, laptops and smart phones, applications on this layer are highly interdependent with the lower middleware and upper content layers.

4) Content layer: This layer comprises the content generated, either by the end-users or producers and provided in TV channels e.g. Sky, online platforms e.g. Facebook, websites or apps e.g. Netflix, being subject to certain rules and conditions prescribed by state or EU agencies, as well as IPRs.

The layers described above denote not only the transmission paths of IP data but also and even more importantly, the value chains that represent the activities of the ICT players. An ICT player may not operate only in a certain layer and could have different activities matching several ones. The interdependence between these layers, as analysed in the case studies above, unravels the players' abilities and potential to collaborate and compete with each other. Thereby, symbiotic relationships might take place because of the open and/or interoperable channels across the layers, as are usually represented by the 'coopetition' between the players. Such a situation means an 'ecosystem' already exists, eliminating or reducing the need for ex-ante regulation. However, an ecosystem may not be mentioned for the walled garden or silo type supply structures that are driven by the proprietary protocols and/or standards.

Given this fact, an ideal strategy for the 'layered regulatory model' should embrace both settings, namely ecosystems where the players have coopetition along with widespread interoperability and non-ecosystem environments where walled gardens

or silos prevail along with access and interoperability restrictions resulting in lack of coopetition. Considering the need to embrace both type of settings since they will co-exist, the regulatory criteria need to be coherent and flexible. To that effect, it is suggested that a neutral and broad concept of 'gatekeeping' be integrated into the multi-layered model with a view to respond to the access and interoperability restrictions. According to the proposed structure, as depicted in Figure 14, gatekeeping roles and functionalities have a key role to play across the layers.

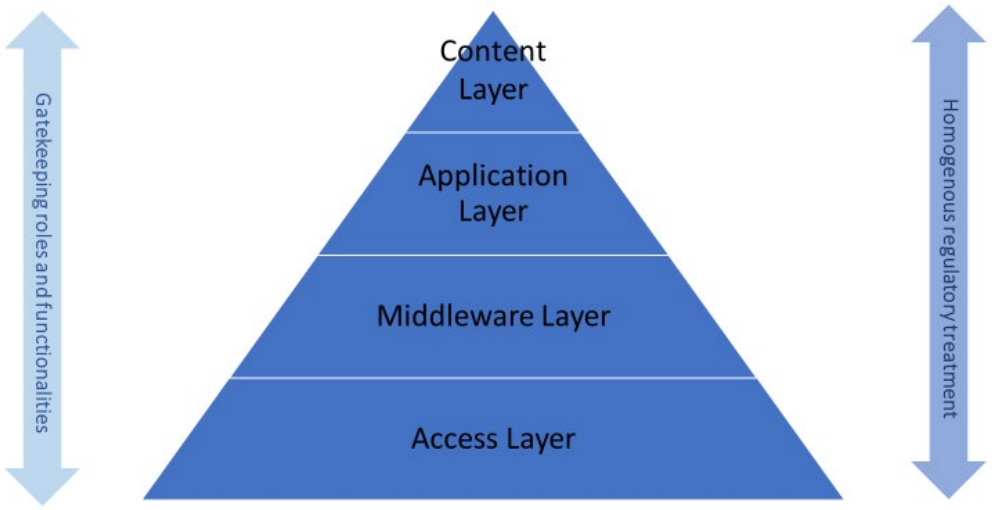

Figure 14: Main features of the layered regulatory model

Source: Constructed by the author

8.4.2. Revitalising gatekeeping and gatekeeping activities

In a layered model, where the layers are to be dealt with on a homogenous basis, 'gatekeeping' emerges as a crucial concept within the proposed model. While the above layers provide the necessary layout for ex ante regulation, the 'gatekeeping' refers to the activities that capture 'competition' and 'techno-social' concerns which need to be addressed within the layered regulatory model. At this chosen term and understanding lies its better reflection of the gateways (interfaces) and their

exploitation by the ICT players. Thus, 'Gatekeeping' morphs into a key technical term under this normative framework, marking a distinction from the rhetorical uses of this concept in the past.

While 'network gatekeeping' was first developed by Barzilai-Nahon to mean "the process of controlling information as it moves through a gate (a network or its sections)", a functional approach has been followed in which the 'gated' meant 'the entity subjected to gatekeeping'.[875] This definitional framework and the related scholarly work[876] suggest existence of 'gatekeeping' in the case of directly or indirectly allowing or denying information flows through a 'gate'. 'Directly' selecting and/or letting the relevant information to flow usually happens in the case journalists and publishers assume this role, whereas 'indirect' gatekeeping usually happens when the gatekeeper acts as 'innovator, change agent, communication channel, link, intermediary, helper, adapter, opinion leader, broker, and facilitator'.[877] In the latter case, intermediation comes to the fore, as legally acknowledged and reinforced by liability exemptions set out under DMCA[878] and E-Commerce Directive of the EU (Directive 2000/31/EC).[879]

The pervasiveness of gatekeeping activities should thus be noted against the everyday-expanding ICTs and their usage for information gathering and communication. Usually, the potential for 'gatekeeping' lies much more in affecting the choices made

875 See supra note 185.
876 See the section '3.1.3. Brief analysis of major concerns on the cumulative ground of 'gatekeeping''.
877 See Laidlaw (n 179) 41.
878 17 USCA § 512 ('Limitations on liability relating to material online').
879 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178 ('E-commerce Directive') art. 12-14.

by users who do not yet know what content to consume or where to find it.[880] From the perspective of the original theory, it is argued that network gatekeepers "can choose which information they let flow and which information they withhold, and more generally they can choose the extent to which gatekeeping is exercised".[881] This core aspect of the 'gatekeeping' fits not only with the informational sources but also to the infrastructural elements, which enable comparable gatekeeping functionalities.

These functionalities need to be considered broadly in view of the ever fast increasing information platforms and intermediary services, notwithstanding the limited number of examples referred to in this thesis e.g. the position held by the CAS operators and ISPs. Both of these undertakings are presumed to have gatekeeping positions and are obliged not to block third-party access and interoperability. Being not limited to these examples, rendering control measures over the information flows or the critical intermediary resources that would enable such flows potentially pave the way to gatekeeping activities. While it connotes controlling mechanisms e.g. TPMs, IPRs and their exploitation over the information flows, the scope and meaning of this key term would expand cutting through all across the IP layers, particularly when consumers' online activities meet up with the AI-based manipulations.

From this point of view, 'gatekeeping' would mean software-governed architectural codes enabling control over access and interoperability, from the bottom to the top layer. Such a key node or gateway does not mean holding an essential facility and/or

880 Helberger, Kleinen-von Königslöw and Van der Noll, (n 190) 60.

881 Dustin W. Edwards 'Circulation Gatekeepers: Unbundling the Platform Politics of YouTube's Content ID', [2018] 47 Computers and Composition 61, 66, referring to Karine Nahon and Jeff Hemsley, *Going viral* (Polity Press 2013) 43.

an accompanying market power,[882] rather it implicates various means to control consumer activities via prevention, manipulation, prioritisation or discrimination. At the infrastructural or bottom layer can exist non-neutral activities that target third parties' non-subsidiary content, which might face delaying, blocking or throttling by the ISPs. Going to the upper layers, such activities would change their form, often obscured behind hidden and algorithmic ways, although having same or comparable restrictive aims. Remarkably, this way of data and operation management might have further consequences as it takes place in the upper layers addressing the content dissemination and consumption by the consumers.

Importantly, such upper layer activities reach out to the consumers in ways they would not realise, like in the way they would be captured via personalised recommendations, prices, customised products, etc. Likewise, individuals' participation on the social media and other information platforms would be captured and affected by the gatekeeping roles and functionalities as they are driven by AI and related algorithms. Furthermore, the democratic culture that is expected to be infused by the society through individuals' participation to the information platforms and channels would also be affected as opposed to what the digital platforms would suggest.[883] Hence, it is right to assert that gatekeepers not only filter and select information but also qualitatively alter the informational content, for better or for worse, through active accumulation, processing and packaging i.e. the gatekeeper adds 'value'.[884]

---

882 See also Orla Lynskey, 'Regulating 'Platform Power' (2017) LSE Law, Society and Economy Working Papers, 1/2017, 10 <http://eprints.lse.ac.uk/73404/1/WPS2017-01_Lynskey.pdf> accessed 9 October 2020; Edwards (n 881) 66.

883 See the section '3.1.3. Brief analysis of major concerns on the cumulative ground of 'gatekeeping''; Laidlaw (n 179) 33, 46.

884 Pieter Ballon, 'The Platformisation of the European Mobile Industry' [2009] 75 3rd Q Communications & Strategies 15, 23.

Against this background, 'consumer welfare' seems unharmed, whereas the access and interoperability channels get restricted and the consumer choices are affected, along with far-reaching consequences towards the democratic culture within the society.[885] Remarkably, in contrast to the legacy understanding of the abusive practices echoed with narrow-minded gatekeeping activities, 'gatekeeping' roles and functionalities have both an economics-based nature and a techno-social character; the former usually surfacing when effective competition is deteriorated and the latter in case of AI manipulations across the cross-layer activities.[886]

Conventional regulatory focus would overlook these restrictive behaviours that would take place across the technological layers. In an era of far-reaching platformisation of the ICT markets,[887] abusive behaviours and underlying markets need to be revitalised following the premise of gatekeeping and cross-layer gatekeeping activities. Platform leaders build up a business model around a set of crucial gatekeeper functionalities and roles that help them to exercise a form of control over the wider value network, and to add and capture significant value in the process.[888] While controlling mechanisms underlying such functionalities should not necessarily be deemed abusive or illegal by themselves, access and interoperability restrictions need to be spotted as they widely capture gatekeeping activities.

Within the framework of proposed model, it needs to be re-emphasized that 'gatekeeping' entails not only controlling the media and information flow, but also access to infrastructural, physical and software interfaces. In understanding both

885 See also Dijck, Nieborg and Poell (n 855).
886 See the section '3.1.3. Brief analysis of major concerns on the cumulative ground of 'gatekeeping''.
887 Pieter Ballon and Eric Van Heesvelde 'ICT platforms and regulatory concerns in Europe' [2011] 35 Telecommunications Policy 702, 704.
888 Ibid.

aspects, it is crucial to put the 'consumers' at the centre, before considering the potential harms they are exposed. The so-called exposure does not only relate to the lessened consumer surplus resulted from the reduced price and quality choices, but also to the reduced opportunities of cultural production and democratic participation that are generated through information flows.[889] Infrastructural elements are not featured for directly restricting free flows information; however, their role of mere conduit for the information platforms alike is most likely to capture interoperability related restrictions, and unlocking the underlying gateways is key to resolve would-be gatekeeping activities.

Since 'gatekeeping' first and foremost means controlling access and interoperability through these gateways e.g. architectural codes, *restrictive acts* in granting third party access and interoperability should be deemed unacceptable. Whether relating to software sources e.g. middleware, including search engines, application stores and browsers, or to infrastructural elements e.g. network interfaces, the same criterion of 'restriction of access and interoperability' should be followed with regards to these gateways or technically speaking 'interfaces'. From the regulatory perspective, a wide spectrum of restrictive activities need to be comprehended within this context, incorporating discrimination, manipulation, prioritisation and quality deterioration, considering their restrictive nature over the consumers' freedom to choose from across the alternative networks, platforms, apps, services or products.

Against this background, 'restriction of access and interoperability' should be acknowledged to happen regardless of the market power. All the layers would be

[889] See the section '3.1.3. Brief analysis of major concerns on the cumulative ground of 'gatekeeping''.

exposed to gatekeepers and their restrictive activities within the meaning of the proposed ‘layered regulatory model’. As a matter of fact, every ICT player that operates in one or more of the layers would potentially have a gatekeeper role insofar as they are positioned to be able to restrict the consumer choices via control over access and interoperability. In many cases, this role would allow the gatekeeper to leverage their gatekeeping position to favour their own activities in other layers. This means applying restrictions on the consumers that seek access to the gateways from other layers. The strong likelihood of the so-called access and interoperability restrictions should be deemed sufficient for the application of ex-ante regulation within the meaning of proposed model, along the same lines with the ECRF and its consumer-oriented perspective.

In the table below could be seen several examples regarding gatekeeping activities which have a restrictive nature.

Table 2: Potential gatekeepers and gatekeeping activities across the layers

Layers	**Potential gatekeepers**	**Potential gatekeeping activities**
Content	Content providers	Providing premium content to affiliated ISPs, CAS or platform providers e.g. in exchange for priority placement.
Application	App providers	Developing apps so as to interoperate only with the affiliated OSs, browsers, search engines, etc.
Middleware	Search engine providers	Selective ranking favouring certain content, apps and web services.
	OS providers	Discriminatory supply of the functionalities to the CPs, app providers or network operators.
	App store providers	App prioritisation, delaying or blocking based on the app or app type.
	Browser providers	Selective or strategic browsing favouring certain web sites, their ads or ad-blocking strategies.
Access	CAS providers	Denial of access to the set-top boxes, including APIs and EPGs, or discrimination in the ranking of the access-authorised content.
	ISPs	Blocking, throttling or delaying certain/ unaffiliated content.
	Network operator	Refusal to supply network e.g. NGN interfaces to the service providers.

Source: Constructed by the author[890]

8.4.3. 'Gatekeeping' from the perspective of underlying concerns

As could be seen from the above examples, gatekeepers might have layer-specific or cross-layer activities. Their operations mainly target controlling the 'gateways', namely the 'interfaces', in and across the layers by which they allow new entries often

[890] Partly inspired by Robert Easley, Hong Guo and Jan Kraemer 'From Network Neutrality to Data Neutrality: A Techno-Economic Framework and Research Agenda' (*SSRN*, 8 March 2017) 26 <https://ssrn.com/abstract=2666217> accessed 9 October 2020.

in a selective way. Gatekeeping connotes more control than the term 'intermediary',[891] and in conjunction with this, controlling mechanisms incorporating IPRs, TPMs and AI based algorithms utilised by the ICT players are the main sources of concern in relation to the gatekeeping roles and functionalities. Underlaid by wide-ranging control features, ICT players' activities having a 'restrictive' nature is key to defining the 'gatekeeping' that is reconceptualised in this study. From this point of view, every means of control over the layers and the interfaces would not be sufficient to qualify the ICT player at hand as gatekeeper.

Restrictive activities pursued by the ICT players signify the existence of a gatekeeping activity, no matter whether it leads to losses in consumer welfare (surplus) based on distortion of competition, or harm or restraint to consumers in the sense that their informational choices are affected. In this context, restricted information flows come to the fore along with far-reaching implications over the individuals' autonomy and dignity, often based on the discriminatory, biased, manipulative, unfairly selective architectural choices. To understand these causes and implications, it is worth reconsidering the competition and techno-social concerns from the perspective of gatekeeping.

Notably, competition concerns would arise should the underlying restrictions have a long arm reaching out to the competitors and their ability to effectively compete in the relevant layer(s). As stated above, competition problems are supposed to create losses in consumer welfare which is the conventional harm theory. Mostly calculable and

[891] See the section '8.4.2. Revitalising gatekeeping and gatekeeping activities'. See also Emily B. Laidlaw, 'Private Power, Public Interest: An Examination of Search Engine Accountability' [2009] 17(1) International Journal of Law and Information Technology 113, 115.

well established within the EU competition law, consumer welfare losses represent most recognisable feature characterising an anti-competitive behaviour which would also capture a gatekeeping activity in conjunction with the competition concerns.

On the other hand, in case of techno-social concerns, the restrictive act would not necessarily have an anti-competitive effect or cause a consumer welfare loss but often result in 'unfair outcomes' or 'transformative effects', as per the exposition put forward by Mittelstadt et al.[892] While these outcomes/effects frame the two normative concerns surrounding algorithms,[893] these could also be taken encompassing the relevant gatekeeping activities under the proposed model. Given the fact that AI-based operations tend to be the 'norm' all across the layers, one can conclude that these two normative categories, namely 'unfair outcomes' and 'transformative effects' explain the so-called techno-social concerns in association to the gatekeeping roles and functionalities.

According to the framework drawn by Mittelstadt et al, *unfair outcomes* mean the consequences brought by the actions driven by the algorithms that can be assessed according to numerous ethical criteria and principles, and are found to have an unfair nature.[894] Within this category are included not only indirect discrimination but also unfavourable results against neutrality and independence. Starting from the bottom

---

892 See Brent Daniel Mittelstadt et al., 'The ethics of algorithms: Mapping the debate' July-December 2016, Big Data & Society 1, 4.

893 There are other literature analysing the concerns attributable to algorithms and AI. See Karen Yeung, 'Why worry about decision-making by machine?' in K. Yeung and M. Lodge (eds) *Algorithmic Regulation* (OUP 2019) 21-48; Teresa Scantamburlo, Andrew Charlesworth, and Nello Cristianini, 'Machine decisions and human consequences' in K. Yeung and M. Lodge (eds) *Algorithmic Regulation* (OUP 2019) 49-81; S. C. Olhede and P. J. Wolfe, 'The algorithms ubiquity of algorithms in society: implications, impacts and innovations' Phil. Trans. Royal Society <https://dx.doi.org/10.1098/rsta.2017.0364> accessed 9 October 2020.

894 Mittelstadt et al (n 892) 5 and 8.

(access) layer, one would come across non-neutral activities performed by the ISPs involving throttling, delaying and prioritising the net traffic ending up with filtered results to be conveyed to the end-users fall in this category. Google's discriminatory ranking,[895] and other online platforms' exclusionary behaviours[896] exemplify the gatekeeping activities from inside the middleware layer. Facebook filtering the news feeds to be featured in users' customized account pages[897] could be given as an example matching the upper layers. Notably, while these examples entail unfair outcomes within the meaning of techno-social concerns, the underlying gatekeeping activities are often scrutinised within the meaning of competition law by the European Commission or competition authorities. While competition concerns are well established and reflected through the EU precedents and legislation, there exist no holistic legal framework governing the unfair outcomes implicated through the

---

895 Google's discriminatory ranking in online shopping comparison services, as was found as an 'abuse of dominance' by the EU Commission, illustrates a restrictive practice arousing techno-social concern, to be qualified as a gatekeeping activity. In June 2017, Google was fined 2.4 billion EUR for abusing its dominant position in the 'online search' market, to hamper the competition 'online shopping comparison' market during the years between 2008 and 2013. Google thereby was ordered by the Commission to ensure "equal terms" for all competitors in the online shopping comparison market based on the fact that they favoured their own services with the result being restricting the users' freedom to choose among the available options. (See the European Commission, Press release, 'Antitrust: Commission fines Google €2.42 billion for abusing its dominance as a search engine by giving an illegal advantage to its own comparison shopping service', 27 June 2017 <http://europa.eu/rapid/press-release_IP-17-1784_en.htm> accessed 9 October 2020).

896 Platforms' exclusionary behaviours would have far-reaching impact on the app providers and their services. Apple's exclusion of the 'Drone +' application from its app store and exclusion of 'Disconnect' from Google Play illustrate this (Luca Belli and Nicolo Zingales, 'How Platforms are Regulated and How They Regulate Us' Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility (United Nations Internet Governance Forum, 2017) 88-91). In the former instance, Apple's rejecting launch of an app that would provide real-time alerts of drone strikes, called 'Drone+', in its app store, was the conflict between the parties. The app provider was given two reasons for this rejection, respectively for it was 'not useful' and on the ground that it was 'objectionable and crude'. While not clear-cut unlike with the former, Google's rejection of Disconnect, a privacy enhancing technology app provider, implicates an allegedly unfair discrimination among the software provided by them and Google's subsidiary, also denoting a likely 'unfair outcome'. While the first instance exemplifies a platform's arbitrary reasoning for an exclusion, the latter instance would potentially be representative of an unfair discrimination in favour of a platform's own software also creating a competitive advantage for himself.

897 Stuart Dredge, 'How does Facebook decide what to show in my news feed?' (Guardian, 30 June 2014) <https://www.theguardian.com/technology/2014/jun/30/facebook-news-feed-filters-emotion-study> accessed 9 October 2020; Nikki Usher-Layser, 'Newsfeed: Facebook, Filtering and News Consumption' (2016) 96(3) Phi Kappa Phi Forum, 18-21.

gatekeeping activities. In addition, sorting these outcomes and concerns separately from the competition concerns is uneasy and often unpromising as they are often intertwined.

When it comes to *transformative effects*, two challenges emerge:

(i) *challenges to autonomy* in the sense that (often personalisation) algorithms reduce the diversity of information user encounters by excluding content deemed irrelevant or contradictory to the user's beliefs. The subject can be pushed to make the institutionally preferred action rather than their own preference.

(ii) *challenges for informational privacy* in the sense that the individual's informational identity is breached by meaning generated by algorithms that link the subject to others within a dataset.[898]

The transformative effects might overlap the unfair outcomes and to a lesser extent the competition concerns. Competition concerns would not be manifest in this context for the very nature of the detriment caused by these effects. Here, information flows and adverse consequences to cultural production and ultimately participatory democracy surface as having crucial results in the wider context of data and traffic management. On the grounds of IPRs, TPMs and/or AI-based algorithms, information flows often become affected to be attended by the accompanying challenges, namely the challenges to 'autonomy' and 'informational privacy'. Combination of these challenges has the potential to transform the data subjects that are exposed to the

[898] See Mittelstadt et al (n 892) 9-10.

underlying gatekeeping activities, i.e. restricted/filtered/manipulated information flows.[899]

Acknowledgement of 'gatekeeping' activities is sourced from the techno-social concerns as equally as, even more, frequently than the competition concerns, considering the far-reaching implications depicted above. Competition law tools and enforcement focus on consumer welfare or deadweight losses, while the IPR rules encompass exceptional safeguards to protect the consumers against the controlling mechanisms that are of a restrictive nature. 'Interoperability' subsists within this environment as a subordinate tool or target with certain limitations. Although having a responsive and a consumer-oriented perspective, the ECRF does not have a nature all-encompassing the ICT layers and falls short of dealing with gatekeeping activities and addressing the related concerns. As a result, many of the gatekeeping activities and relevant concerns fall untouched or unaddressed under the available tools and safeguards of the EU legal system. Below, it is put forward how and through which tools and principles the layered regulatory model could respond the abovementioned concerns and the underlying gatekeeping activities.

[899] It could be argued that even in the presence of data protection tools and safeguards, the transformative effects at stake could not be mitigated easily for the persistent nature of the gatekeeping activity that reach out to individuals' dignity. However, while the individuals grant their consent as an autonomous/independent person, this does not deter the possibility that the unfairly selective content being reached to themselves through the underlying algorithms.

8.4.4. Matching the gatekeeping roles and functionalities with the layered regulatory model

8.4.4.1. Setting the governing principles

As examined above, gatekeepers and their restrictions regarding access and interoperability could be witnessed across all the ICT layers. Crucially, the premise of homogeneous treatment of the ICT layers across the gatekeeping functionalities signifies the need to reconsider ex-ante regulation on the basis of the 'layered regulatory model'. As the risk of over-regulation arises should all the ICT services be subject to ex-ante regulation based on a widely implemented 'gatekeeping' concept, filtering of this concept seems necessary.

Filtering means an uneasy task, given the extraterritorial and quite wide nature of the multi-layered ICT networks and services. Regardless of how well-equipped a regulatory authority is, filtering and designating the gatekeeping roles and functionalities would go beyond the established regulatory limits of an NRA that is normally charged with electronic communications regulation in a national context. Further to this fact and the cross-border nature of the ICT landscape, 'homogenous regulatory treatment' is another thrust of the layered model that needs to be factored into an appropriate regulatory design.

As a starting point, the proposed 'layered regulatory model' should not be seen as a milestone along the way of conventional regulatory wisdom that is heavily attributed to national territories. One could argue, EU regulatory thinking and design is of the utmost importance for properly interpreting and implementing the gatekeeping-centric approach. On the other hand, the long-lasting EU experience and its conventional mind-

set would not be able to address the holisticness and flexibility required for the regulatory treatment of the ICT layers.

Against this background, form-based and top-down regulation needs to be replaced with a principles-based and bottom-up approach. Otherwise, the gatekeeping concerns from a layered perspective would not be met and dissolved in the long run. Ever fast changing ICT dynamics would not be captured by resource consuming, patchy and shortcoming regulatory safeguards of the EU legal system including those of the ECRF. Having said that, in lieu of adapting or modifying the ECRF's tools and measures, its consumer-oriented perspective and more responsive ex ante approach would be transposed into the proposed layered model. In so doing, a dynamic regulatory course would rather be adopted by giving a leeway to collaboration as well as soft law principles that would eventually be enforced under certain conditions.

This bottom-up approach partially reflects the solution recommended by the House of Lord's recent Report regarding regulation of the 'digital services facilitated by the internet'.[900] To emphasise, after a long period of consultation, the House of Lords ended up with a set of ten principles to pave the way for the establishment of a rigorously designed, comprehensive and forward-looking framework. Setting the scene for the proposed Digital Authority to advance further guidelines, the Report clearly recommends that industry stakeholders be actively involved in the future process.[901]

---

900 House of Lords, Select Committee on Communications, *Regulating in a digital world* (2nd Report of Session 2017-19, March 2019) 3-4.

901 Ibid, 5.

From this point of view, it is considered that the 'layered regulatory model' would be better run by setting the governing principles which will lay down the main pillars and instructions for the ICT players, specifically gatekeepers, in the first instance. To commence with, it is proposed the core and main principle include a prohibition on "restricting access and interoperability at the expense of limiting consumer choices". Further to this baseline principle, gatekeepers should also;

- report their management of data and traffic across the layers to the regulator(s) (transparency),
- refrain from biased or unfairly selective supply of services unless justified on an objective ground of technical reasoning (fairness),
- establish that the software management e.g. AI-driven processes underlying the services supplied by them rely on ethical, accountable and democratically justifiable reasons (accountability).

This fourpartite set of principles draw the main pillars of the layered regulatory model. In the emergent response echoes an oversight for the multi-layered ICT activities, with a view to address gatekeeping activities that arouse competition and/or techno-social concerns and posing a restriction over the consumers. Notably, the latter means informational, ethical and democratic concerns reflecting on the restrictions mostly based on the manipulative and algorithmically driven algorithms, which are often obscured from the end-users unlike with TPMs and most IPRs.

Crucially, the above principles mean the key requirements which all the gatekeepers should adhere to. Accordingly, there is no need for a gatekeeper to have a market power in order to be subjected to these principles which are generic and ex ante. As

long as these principles are complied with, there would be no need to intervene on the part of the regulatory authority, namely European Commission at the EU level and NRAs at the national level. Conversely, in circumstances where the principles are breached and consumer choices are restricted, additional safeguards would need to be enforced. Having said that, the thesis also proposes the given principles be translated into enforceable obligations, as detailed below.

8.4.4.2. Further regulatory steps and obligations

Based on the governing principles explained above, evaluation of the ICT settings for any potential obligation needs to be supplemented by a finding as to the conditions under which ex-ante remedies need to be responded. As stated above, in view of the dynamic nature of the ICT layers and interdependencies, a bottom-up approach is the key for the successful implementation of the layered regulatory model. Pursuit of this approach will potentially unravel the extent to which further regulatory steps are to be taken in a self-perpetuating manner.

For a better and constructive regulatory thinking, one could refer to the ecosystem characteristics from inside the case studies as such characteristics might prevail across the layers mitigating the need for any remedial situation. While all the gatekeepers could potentially be subject to ex-ante remedies as well as principles, finding ecosystem characteristics would lessen further regulatory steps to be taken. Further steps of ex-ante regulation, when considered with the dynamic nature of the ICT layers, requires a deeper insight into the investigated ICT settings.

Principally, the main prohibition over “restricting access and interoperability at the expense of limiting consumer choices” would be assumed to have been fully or

partially met by the ecosystems. In case an ecosystem that is driven and characterised by coopetition exists, this situation should be taken into account as a significant reason to reduce ex-ante regulation for the layer(s) in question. Potentially, access and interoperability gaps will be bridged via the coopetitive relationships within the ecosystem, so that the need for extra regulation would be diminished, particularly as far as competition concerns are concerned.

Notwithstanding, assessment of access and interoperability restrictions suggest elaboration of transparency, fairness and accountability, as reflected within the principles. This is compelling, because techno-social concerns would have an undiscernible yet potentially more legacy nature which might not be addressed via simply prohibiting restrictions over access and interoperability. Having said that, transparency, fairness and accountability should exist and be secured in the relevant layer(s), regardless of ecosystem characteristics e.g. coopetition, myriad interactions. More explicitly, according to an evaluation against the principles stated above, appropriate obligations might need to be imposed on the gatekeepers by the regulator. Such potential obligations include, but not limited to, the following:

- Access and interoperability: Consumers' access to infrastructural/informational resources might be affected when a gatekeeper denies or delays the demands for access to and interoperability with the access, middleware, application and content layers controlled by themselves. In that case, access and interoperability remedies might be imposed on the gatekeeper(s) to make the relevant layers or layer elements accessible to the relevant consumers.

- Transparency: A gatekeeper might be subject to transparency obligations when the same-layer or cross-layer operations carried out by them reveal a gatekeeping activity in view of the restricted consumer behaviours and preferences, particularly as a result of hidden aspects of underlying software and algorithms.
- Fairness: In case certain restrictions by means of discrimination and bias e.g. selective ranking, filtering, prioritising take place across certain layer(s) resulting in a gatekeeping activity, the gatekeeper could then be ordered to carry out their activities in an unbiased and ethically justifiable manner.
- Accountability: In the case of consumers being manipulated towards certain content, apps, services, etc. the gatekeeper involved in that activity might be required to redesign their underlying software and algorithms in relation to the pertinent layer(s) or layer elements.

These obligations denote the remedies that are presumed to keep the governing principles alive and enforceable. As gatekeeping activities usually happen across more than one layer, these obligations might need to be adjusted accordingly and should thus fit with the pertinent layers or layer elements, in view of the related restriction(s) at stake. Having said that, these remedies mark a distinction from those under the ECRF, which are only applicable to the access layer elements with certain exceptions and are thought of remedying competition problems with an infrastructural focus. Crucially, not only the nature, scope and extent of the obligations but also the way they are supposed to be imposed, differs in the 'layered regulatory model'.

Under the 'layered regulatory model', the ICT stakeholders' collaboration with the regulators and among themselves is of a key importance in running the proposed

model. As this regulatory process primarily builds upon and commences with the governing principles, it has quite a dynamic nature, differently from the traditional top down ex ante regulation. In this dynamic process, roles and responsibilities would be reshaped based on the stakeholders' multi-tiered collaboration, e.g. with the regulators, as well as amongst themselves.

It is note-worthy that ecosystem characteristics could mitigate but not obviate the entire regulatory needs and obligations. Remarkably, ecosystem players could meet at an equilibrium point where they could continue non-transparent, unfair and non-ethical activities. Attention should still be paid to such kind of activities including the underlying algorithms, which would arouse further concerns going beyond access and interoperability. That is to say, even in case interoperability gaps and problems are diminished through self-regulatory ecosystems, additional remedies would need to be invoked for a sustainable ICT landscape.

According to the response taken from the ICT players and their level of commitment to the governing principles, further remedies may always be necessary. In this regard, a 'one size fits all' approach would not respond each layer's distinctive gatekeeping activities, some of which could be addressed more easily or effectively than others. The principle of 'homogenous regulatory treatment' does not contradict with applying appropriately chosen and/or filtered remedies against the gatekeeping activities that are encountered in related layer(s).

For instance, in the application layer would exist a self-regulatory ecosystem, within which access and interoperability problems are already resolved and only the need for certain remedies concerning transparency and accountability. On the other hand, in the

middleware layer the need for ex-ante regulation would embody more obligations, starting with access and interoperability and proceeding with further ones e.g. transparency and redesigning the underlying software and algorithms. It should also be underlined that many of the gatekeeping activities cut across the layers and would need to be dealt with by cross-layer remedies. While gatekeeping activities usually originate from one layer, their cross-layer nature would require regulators to formulate the obligations in a multi-layered fashion.

Overall, implementing layer-specific or cross-layer remedies represent the final phase of this dynamic and bottom-up process, through which regulators would oversee and reconsider the applicable gatekeeping obligations, from a holistic perspective. Given the evolving nature of the ICT settings, these remedies would need to be reconsidered on a recurring basis i.e. at least every five years, or in case of a pressing need for re-evaluation. Reflecting on this, the figure below illustrates the key stages of the 'layered regulatory model'.

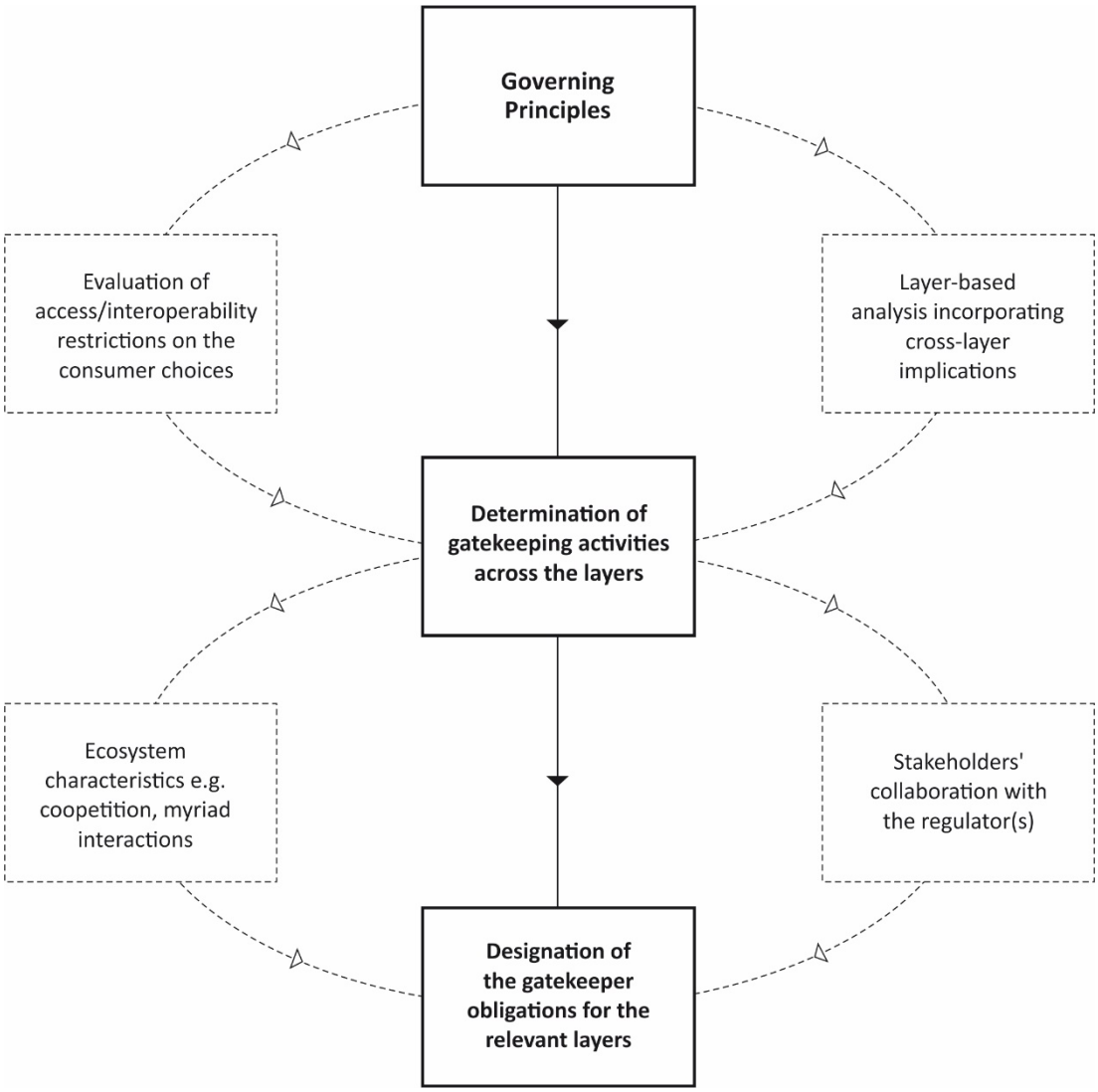

Figure 15: Key stages of the layered regulatory model

Source: Constructed by the author

8.4.5. Review of the institutional roles and responsibilities

As could be seen above, the proposed model has a dynamic and evolving nature. For the smooth and better functioning of the model, top-down measures are avoided at all. Given the central tenets of the proposed model i.e. consumer-oriented perspective, holistic and multi-layered nature, there would no longer be a need to the existing access related measures of the ECRF e.g. SMP remedies, nor to the competition law remedies

that aim to designate and penalise the abusive behaviours in field of ICTs.[902] Therefore, it is suggested the proposed principles and remedies replace the competition oriented ECRF rules e.g. SMP remedies, and have precedence over the EU competition rules. Since both the EU competition law and the ECRF have other rules than those that target abusive conducts, these legal frameworks need to be maintained for other compelling reasons i.e. merger control under the EU competition law or universal service obligations under the ECRF. Notwithstanding, all the ICT-based competition concerns already captured by either EU competition law or ECRF need to be first and foremost dealt with through the 'layered regulatory model' for its wider scope and overarching nature.

This proposition stems from the normative framework presented above, considering it all encompasses and addresses the behavioural aspects that are underlaid with gatekeeping roles and functionalities across the IP layers. Given the wide-ranging competition and techno-social concerns surfacing in this context and the response developed by the proposed model, this model should have an overreaching role to play against the existing ex ante and ex post competition rules, except for the dedicated areas to be ascertained. From this point of view, the complementarity between the sector-specific regulation and the EU competition law needs to be revised from a broader perspective, rendering a prioritised role to the former since the proposed model is constructed to deal with the related concerns from a holistic manner, replacing the ECRF.

[902] Having a novel character, it is envisaged that the 'layered regulatory model' will replace the entrenched terms e.g. 'market' and norms e.g. 'market failure' with new ones e.g. respectively 'layer' and 'gatekeeping', and these radical changes would create new inroads for implementation of competition law alongside the proposed model.

The perspective upheld by the model expands based on the main thread of ICT interoperability, reaching out to the non-transparent, unfair, algorithmically biased or discriminatory, democratically unjustifiable cross-layer activities. Against such activities, the model develops its safeguards by instructing and forcing the ICT players to comply with the governing principles and remedies, and operationally not to perpetrate any restrictive e.g. discriminatory, biased, unfairly selective, non-transparent, activity. Since this features a behavioural roadmap by and large, it might be argued the proposed model and its underlying normative framework should not affect any given right including IPRs.

Notwithstanding, some IPRs as well as TPMs would enable overprotection on the ICT interfaces sometimes jeopardising the very nature of interoperability, which entails behavioural freedoms, innovation and information flows. This often comes up with the protective statutory rules and would result in a potential clash between the exploitation of IPRs/TPMs and application of the layered regulatory model. In case of such a clash, the broadened vision of the proposed model needs to step in for the encroaching rights and technological measures, should they intervene users' freedom to choose disseminated content, applications, services and networks. This very notion is crystallised and rooted within the first governing principle of the model, which stipulates ICT players not to restrict access and interoperability at the expense of limiting consumer choices. Since this principle is a clear signal to the over-intrusive controlling mechanisms including the IPRs and TPMs, an ICT player needs to pay extra attention while exercising their IPRs as these would have the effect of limiting the consumers' choices along with hindered interoperability. On the other hand, unless the utilised rights and technological measures restrict access and interoperability

across the layers, there would be minimum or no room for competition or techno-social concerns that potentially denote a gatekeeping activity.[903]

From a broader perspective, the proposed model would accommodate libertarian views regarding information flows and scholarly calls for 'information justice'.[904] It underpins and aims to protect the consumers' freedom to choose, communicate and access to the information, over which considerable control is exerted across the technological layers, increasingly by means of AI-based algorithms. While the onus is to enhance the access and interoperability links and channels, the driving reasons that need to be highlighted is to unlock the gateways against the consumer choices and give leeway to free information flows. Proposed model envisions informational barriers are removed across all the IP layers, where necessary by means of coercive tools and mechanisms, and supplanting contradicting statutory rules. It is noteworthy that this broadened vision reveals the flip side of the constitutional human rights including freedom of expression,[905] which needs to be free of chains and reinforced as such.

---

903 On the other hand, the proposed model envisages that the governing principles and remedies are enforceable also in the case access and/or interoperability is provided in an unfair, non-transparent or ethically unjustifiable manner. In such cases, further safeguards of transparency, fairness and/or accountability remedies would be applied even if there is no need to remedying access/interoperability, meaning that there are still legacy restrictions that need to be addressed. See the section '8.4.4.2. Further regulatory steps and obligations'.

904 See Griffin (n 160) 59. Griffin, after comparing 'economic justice' and 'information justice' which has been conceptualized as a new notion by himself, concludes as follows:

> In the era of information justice, the shift moves towards the conception that the individual should be able to obtain access to information in order to encourage further information production. The invisible hand of Adam Smith that guides the capitalist process is the same hand that guides the information exchange process, namely, the idea that exchange should be a possibility (Griffin (n 167) 59) (…) To start to regulate information in a new way raises the possibility that regulation will stifle the use of information in a way that will impact the fundamental rationales and existence of exchange, that very notion of exchange which was central to the development of society. This is the ultimate paradox that information regulation brings, and it is why this regulation must also be subject to the notion of information justice. (Griffin (n 160) 61-62).

905 See Lessig (n 175) 186-187, 269; Boyle (n 174) 94-95.

While at the centre of the model lies the safeguards to enable ICT interoperability, its implications reach out to the democratic and free society whereby informational barriers are removed. As informational barriers embody over-intrusive IPRs, TPMs as well as AI based algorithms that manipulate the consumers by restricting their freedom to access to the information, and given the key nature of information flows against the gatekeeping activities, it is proposed that the proposed model have a superior role, ideally with a 'meta law' character, over the applicable laws and rights including IPRs in view of any potential conflict regarding implementation.

Summing up, the layered regulatory model would offer an effective and overarching response to the interoperability based problems, going beyond the narrow-minded and fragmented European perspective. Among the examined EU bodies of law including competition law, IPR and ECRF rules, the ECRF appears as the befitting place for the integration of this model into the EU legal system in view of its ex ante and consumer-oriented nature. This integration, meaning replacement of the core, mainly SMP oriented, principles of the ECRF, would give way to far-reaching implications in terms of regulatory governance and institutional structure of the EU. This study sets the ground for a potential debate along with the proposed model, whereby it is envisaged that how to transpose this model into the EU legal system and its far-reaching implications would be subject matter of further research.

8.5. Concluding remarks: Brief summary and further research

This thesis mainly examines the regulatory governance of ICT interoperability across a number of legal disciplines and is based on multiple case studies following the doctrinal analysis. While lack of interoperability raises several significant concerns,

incorporating vendor lock-in, switching costs, follow-on innovation and information flows, regulation of interoperability has differing reflections within the distinct areas of EU law i.e. IPR rules, competition law and ECRF. The lack of interoperability being dealt with on the disparate grounds of the EU law, often with shortcomings and partial solutions, signifies the absence of a coherent and holistic approach under the given legal disciplines against the so called concerns. It is also important to note that applicable legal tools under EU law, when providing insufficient and partial responses, do not keep pace with the ICT dynamics e.g. cross-layer interdependencies, pursue the traditional harm theories i.e. consumer welfare, and overlook the fast-evolving gatekeeping activities based on the controlling mechanisms including IPRs, TPMs and AI-based algorithms.

From this point of view, this study endeavours to build up a normative framework focusing on the EU legal system and reaching out to broadly figured interoperability-based concerns in the ICT field. After the multi-disciplinary doctrinal analysis, it is found that a holistic and multi-layered approach is lacking and appears a pressing need across and to the limitedness of the EU law. This need surfacing during the doctrinal analysis has become more apparent in the case studies conducted in this research. While the EU law does not have a holistic perspective and all-encompassing framework, gatekeeping activities being addressed to a limited extent e.g. under net neutrality and CAS regulations, also needs to be stressed, as elaborated while examining the ECRF. Following up on this analysis, multiple case studies have revealed that cross-layer interrelationships, whether fraught with walled gardens or not, would ideally be treated by a layering-based ex ante regulatory policy. In other words, layering approach has been found to offer the needed holisticness and

flexibility through which responsive tools could be designed against the major concerns and the surrounding gatekeeping activities.

Against this background, the layers of the IP stack, from the bottom to the top, are revisited, elaborated and then adapted into an ex ante model called 'layered regulatory model'. This model proposal constitutes the most remarkable 'contribution to knowledge' of this thesis. According to this proposed model, the 'access', 'middleware', 'application' and 'content' layers build up the layout, which means the regulatory field for the technologically-neutral treatment of interoperability related problems. Crucially, it is considered that this 'layered regulatory model' is fit-for-purpose in dealing with the related (competition and techno-social) concerns, with a holistic outlook encompassing both ecosystem and non-ecosystem settings.

Based on this layered structure, the concept of 'gatekeeping' to which attention is drawn at the outset morphs into a key term particularly against the interfaces between the layers that are exploited to manipulate or filter the consumers' online activities. Given the need for holistic and homogenous regulatory treatment, the thesis proposes that layered model be invigorated with a revitalised conception of 'gatekeeping' by which to comprehend and respond both 'competition' and 'techno-social' concerns. That is to say, 'interoperability' lying at the core of such layer interdependencies, should be elaborated with the surrounding 'gatekeeping' concept and related (gatekeeping) activities that capture the underlying concerns on a cumulative ground. This exposition based on the layering approach constitutes another major 'contribution to knowledge' of this thesis.

From this point of view, the concept of ‘gatekeeping’ is used to mean restrictive control features incorporating the IPRs, TPMs, and algorithmic design and preferences whereby discriminatory, unfairly selective, biased or democratically unjustifiable AI-driven activities are encompassed. Based on a number of principles and corresponding remedies, the model aims that gatekeeping activities that restrict access and interoperability in the described ways are diminished. To that end, the proposed model brings out the major prohibition over “restricting access and interoperability at the expense of limiting consumer choices”. This representing the baseline principle, the further principles of ‘fairness’, ‘transparency’ and ‘accountability’ are integrated into the model by which to diagnose and deter the gatekeeping activities. Furthermore, a set of remedies translated from the principles are designed in view of the potential scenarios whereby gatekeeper(s) do not adhere to the governing principles. While it is ultimately proposed this model replaces the core (access and competition related) ECRF principles and remedies, its dynamic nature goes beyond the ECRF and reaches out to a broader vision capable of dealing with other problems e.g. hindered information flows, unfair outcomes and transformative effects conducive to ICT landscape.

Reflecting these, sequential steps and milestones of this research are manifested in Figure 16 below. This figure also features the main findings and outcomes of the research, including the key aspects of the ‘layered regulatory model’.

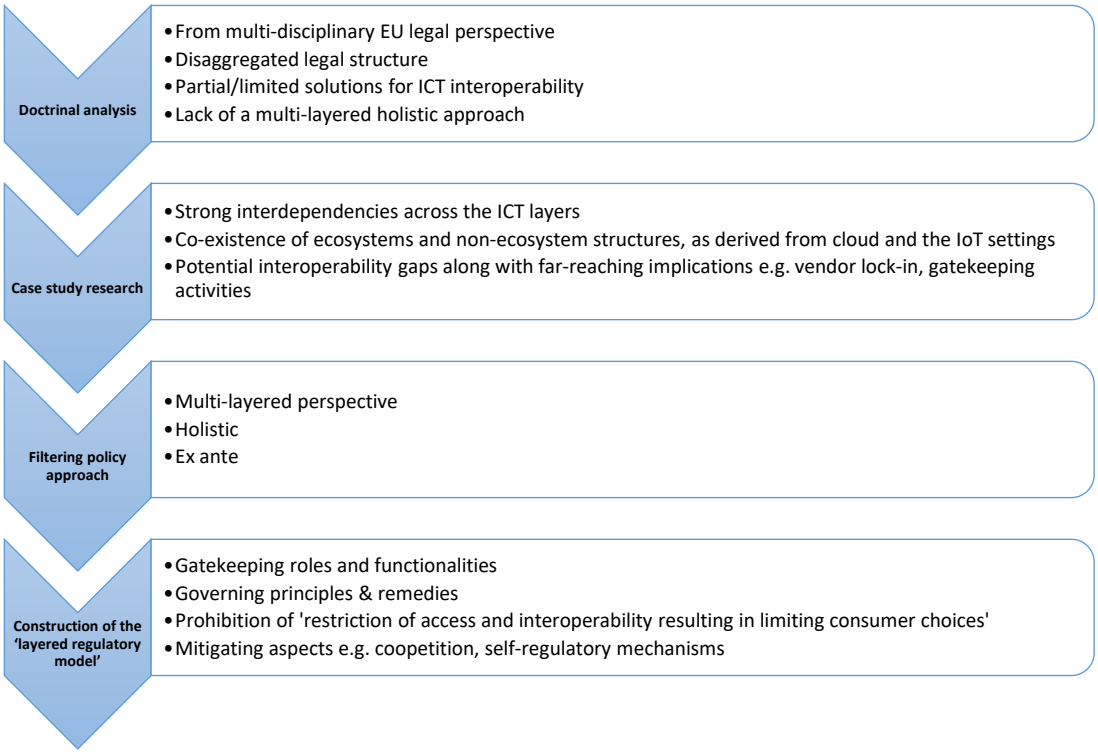

Figure 16: Key milestones of the research

Source: Constructed by the author

As the figure above demonstrates, the research outcomes entail a number of normative findings following the given milestones. While the main outcome and contribution to knowledge is the proposed 'layered regulatory model', this model's interaction with many related themes and concepts e.g. gatekeeping activities, AI based algorithms and accompanying ethical concerns, also needs to be noted. While this interaction is elaborated in the thesis to a certain extent, this endeavour would better be complemented and pursued with further research. It is always welcome to see future efforts in this field of research delving further into the regulatory frontiers of the proposed model, particularly regarding un-ethical and democratically unjustifiable aspects of the gatekeeping activities with a more focus on the AI aspects.

Bibliography

International and European Treaties

- Agreement on Trade-related Aspects of Intellectual Property Rights, Annex 1C of the Marrakesh Agreement Establishing the WTO ('TRIPS Agreement')
- Berne Convention for the Protection of Literary and Artistic Works (as amended on 28th September 1979) ('Bern Convention')
- Consolidated Version of the Treaty on European Union [2008] OJ C115/13 ('TEU')
- Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326 ('TFEU')
- Paris Convention for the Protection of Industrial Property (as revised at Stockholm in 1967)

EU legislation (Regulations, Directives)

- Commission Directive (EEC) 90/388 of 28 June 1990 on competition in the markets for telecommunications services [1990] OJ 1990 L 192/10
- Commission Directive (EEC) 88/301 of 16 May 1988 on competition in the markets in telecommunications terminal equipment [1988] OJ 1988 L 131/73
- Council 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 [2019] OJ L 130 ('Directive on Copyright in the Digital Single Market')

- Council Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36 ('European Electronic Communications Code' or 'EECC')
- Council Directive (EU) 2016/943 of the European Parliament and of the Council on 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157 ('Trade Secrets Directive')
- Council Directive (EU) 2014/53 of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Software Directive)
- Council Directive (EC) 2009/140 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services [2009] OJ L 337/37 ('Better Regulation Directive')
- Council Directive (EC) 2009/136 of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications

networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L 337/11 ('Citizens' Rights Directive')

- Council Directive (EC) 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201 ('E-Privacy Directive')
- Council Directive (EC) 2002/22 of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services [2002] OJ L 108 ('Universal Service Directive')
- Council Directive (EC) 2002/21 on a common regulatory framework for electronic communications networks and services OJ L 108, 2002/19/EC ('Framework Directive')
- Council Directive (EC) 2002/20 of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services, [2002] OJ L 108/21 ('Authorisation Directive')
- Council Directive (EC) 2002/19 on access to, and interconnection of, electronic communications networks and associated facilities OJ L 108 as amended by Directive 2009/140/EC OJ L337/37 ('Access Directive')

- Council Directive (EC) 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] L167/10 (‘InfoSoc Directive’)
- Council Directive (EC) 96/9 of the European Parliament and of the Council on 11 March 1996 on the legal protection of databases [1996] OJ L 77 (‘Database Directive’)
- Council Directive (EU) 90/387 of 27 June 1990 on the establishment of the internal market for telecommunications services through the implementation of open network provision [1990] OJ L 192/1
- Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303
- 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 [2016] OJ L 119/1 (‘General Data Protection Regulation’ or ‘GDPR’)
- Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union [2015] OJ L 310 (‘EU Net Neutrality Regulation’)

- Regulation (EC) 139/2004 on the control of concentrations between undertakings [2004] OJ L24/1 (‘EU Merger Regulation’ or ‘EUMR’)
- Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2003] OJ L 1
- Regulation (EU) 2887/2000 of the European Parliament and of the Council of 18 December 2000 on unbundled access to the local loop [2000] OJ 2000 L 336
- Regulation (EEC) 4064/89 of 21 December 1989 on the control of concentrations between undertakings [1989] OJ L 395 (‘Merger Control Regulation’ or ‘MCR’)

European Commission Guidance, Guidelines,

Notices and Recommendations

- European Commission, Commission guidelines on market analysis and the assessment of significant market power under the Community regulatory framework for electronic communications networks and services (2002/C 165/03) [2002] OJ C 165 (‘Commission’s 2002 Guidelines’)
- European Commission, Notice on Application of Competition Rules to Access Agreements in the Telecommunications Sector [1998] OJ C 265/02 (‘Commission’s 1998 Access Notice’)
- European Commission, Commission Notice on the definition of relevant market for the purposes of Community competition law (97/C 372 /03) [1997] OJ C 372/03)

- European Commission, Commission Recommendation of 9 October 2014 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (2014/710/EU) [2014] OJ L 295
- European Commission, Commission Recommendation of 17 December 2007 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (2007/879/EC) [2007] OJ L 344
- European Commission, Commission Recommendation of 11 February 2003 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (2003/311/EC) [2003] OJ L 114
- European Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (2009/C 45/02) [2009] OJ C 45 ('Commission Guidance')
- European Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-

operation agreements (2011/C 11/01) [2011] OJ C 11 (‘Commission’s 2011 Guidelines’)

- European Commission, Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentration between undertakings (2004/C 31/03) [2004] OJ C 031.

Proposals

- European Commission, Digital Services Act package ex ante regulatory instrument for very large online platforms with significant network effects acting as gate-keepers in the European Union’s internal market, Document Ares (2020) 2877647
- European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, COM(2013) 627 final, 2013/0309 (COD)
- European Commission, ‘Proposal for a Directive of the European Parliament and of the Council on the patentability of computer-implemented inventions (2002/C 151 E/05) COM (2002) 92 final - 2002/0047(COD)

Other Official Materials

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee

of Regions, A Digital Single Market Strategy for Europe, COM (2015) 192 final

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM (2010) 245 final/2
- European Commission, European interoperability framework for pan-European eGovernment services (Version 1.0) 2004
- European Commission, ICT Standardisation Priorities for the Digital Single Market, COM (2016) 176 final
- European Commission, Towards a Dynamic European Economy: Green Paper on the development of a Common Market for Telecommunications Services and Equipment [1987] COM (87)290 ('1987 Green Paper')
- Council Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 [1988] OJ C 257/1
- UK Copyright Designs and Patents Act 1988
- US Horizontal Merger and Guidelines (US Department of Justice and Federal Trade Commission, 2010
- US Digital Millennium Copyright Act of 28 October 1998 ('DMCA')
- US Copyright Act of 19 October 1976 ('USCA')

Newsletter, Press Releases

- European Commission, 'Antitrust: Commission fines Google €2.42 billion for abusing its dominance as a search engine by giving an illegal advantage

to its own comparison shopping service' (Press release, IP/17/1784, 27 June 2017) <http://europa.eu/rapid/press-release_IP-17-1784_en.htm> accessed 9 October 2020)

- European Commission, 'Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover' (Press Release, IP/17/1369, 18 May 2017 <https://europa.eu/rapid/press-release_IP-17-1369_en.htm> accessed 9 October 2020
- European Commission, 'Antitrust: Commission Probes Allegations of Antitrust Violations by Google' (Press Release, IP/10/1624, 30 November 2010) <http://europa.eu/rapid/press-release_IP-10-1624_en.htm> accessed 9 October 2020
- European Commission, 'Commission opens proceedings against Nintendo distribution practices' (Press Release, IP/00/419, 28 April 2000), <https://europa.eu/rapid/press-release_IP-00-419_en.htm?locale=en> accessed 9 October 2020
- EC Competition Policy Newsletter, 1998, No. 3 <http://ec.europa.eu./competition/publications/cpn/cpn19983.pdf> accessed 9 October 2020

Cases and Commission Decisions

Commission Decisions

- Case M.8124, *Microsoft/LinkedIn* [2016] OJ C95 ('*Microsoft/LinkedIn* decision')

- Case No COMP/M.7217, *Facebook/Whatsapp* [2014] OJ L 24 (‘*Facebook/Whatsapp*’ decision)
- Case COMP/M.6281, *Microsoft/Skype* [2011] OJ L 24 (‘*Microsoft/Skype* decision’)
- Case COMP/M.5984, *Intel/McAfee* [2011] OJ C95 (‘*Intel/McAfee* decision’)
- Case COMP/M.5669, *Cisco/Tandberg* [2010] OJ L 24 (‘*Cisco/Tandberg* decision’)
- Case COMP/39530, *Microsoft* [2009] OJ C 45 (‘*Microsoft Tying*’ decision)
- Case COMP/C-3/37.792, *Microsoft* [2004] (Commission’s *Microsoft* decision’)
- Case COMP/M.2876, *Newscorp/Telepiù* [2003] OJ L 110
- Case COMP D3/38.044, *NDC Health/IMS* [2002] OJ L 59/18
- Case No.IV/M.2050, *Vivendi/Canal+Seagram* [2000] OJ C311/3
- Case IV/M. 0037, *BSkyB/KirchPayTV* [2000] OJ C 100
- Case IV/M.0048, *Vodafone/Vivendi/Canal+* [2000] OJJ C 11
- Case IV/M. 993, *Bertelsman/Kirch/Premiere* [1998] OJ L 53
- Case IV/M. 1027, *Deutsche Telekom/Beta Research* [1998] OJ L 53
- Case IV/M. 469, *MSG Media Service* [1994] OJ L 364
- Case IV/34.689, *Sea Containers/Stena Sealink* [1994] OJ L 15/8
- Case IV/33.544, *British Midland/Aer Lingus* [1992] OJ L 96/34
- Case IV/34.174, *B&I Line plc/Sealink Harbours Ltd.* [1992] 5 CMLR 255
- Case IV/32.318, *London-European Sabena* [1988] OJ L317/47 [1989] 4 CMLR 662
- Case No IV/29.479, *IBM* [1984] (‘Commission’s *IBM* decision’)

EU Judgements

- Case C-406/10, *SAS Institute Inc v World Programming Ltd* [2012] 3 CMLR 4 ('*SAS v WPL* judgement')
- Case C-393/09, *Bezpečnostní Softwarová Asociace - Svaz Softwarová Ochrany v Ministerstvo Kultury* [2011] ECDR 3 *('Softwarová* judgement')
- Case C-280/08 *Deutsche Telekom v Commission* [2010] ECR I-9555
- Case T-201/04 *Microsoft v Commission* [2007] ECR II-3601 ('GC's *Microsoft* judgement')
- Case C-418/01 *IMS Health GmbH & Co OHG v. NDC Health GmbH& Co KG* [2004] ECR I-5039, 4 CMLR 1543 ('*IMS Health* judgement')
- Case C-7/97 *Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG* [1998] E.C.R. I-7791, [1999] 4 CMLR 112 ('*Oscar Bronner* judgement')
- Case T-504/93, *Tiercé Ladbroke SA v. Commission* [1997] ECR II-923, [1997] ECR II-923, [1997] 5 CMLR 309 ('*Tiercé Ladbroke* judgement')
- Case C-333/94 P, *Tetra Pak International SA v. EC Commission* [1996] ECR I-5951
- Case C-53/92 P, *Hilti v. EC Commission* [1994] ECR I-667
- Joined Cases C-271, C-281/90 and C-289/90, *Kingdom of Spain, Kingdom of Belgium and Italian Republic v Commission of the European Communities – Competition in the markets for telecommunications services*, [1992] ECR I-05833

- Case C-202/88, *French Republic v Commission of the European Communities – Competition in the markets in telecommunications terminal equipment*, [1991] ECR-I-01223
- Case 238/87, *AB Volvo* v. *Eric Veng (UK) Ltd.* [1988] ECR 6211, [1989] 4 CMLR 122 (‘*Volvo* judgement’)
- Case 53/87, *CICCRA v. Renault* [1988] ECR 6039 (‘*Renault* judgement’)
- Case 311/84, *Cenbtre belge d’études du marché*, [1985] ECR 3261 (‘*Telemarketing* judgement’)
- Case 85/76 *Hoffman- La Roche & Co AG v Commission* [1979] ECR 461, (1979) 3 CLR 211
- Case 22/78, *Hugin Kassaregister AB and Hugin Cash Registers Ltd v. EC Commission* [1979] ECR 1869
- Case 27/76 *United Brands v Commission* [1978] ECR 207 (‘*United Brands* judgement’)
- Joined Cases 6, 7/73, *Commercial Solvents v. Commission* [1974] ECR 223 (‘*Commercial Solvents* judgement’)
- Joined cases C-241/91 P and C-242/91 P, Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission [1995] ECR I-743, [1995] 4 CMLR 718 (‘*Magill* judgement’)

EPO Cases

- Case T 258/03, Auction Method/HITACHI [2004] OJ 2004, 575

United States

- *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 US 585 (1985)
- *Atari Corp. and Tengen Inc. v. Nintendo of America Inc. and Nintendo Co. Ltd.,* 975 F.2d 832, (Fed. Cir. 1990) ('*Nintendo* judgement')
- *Nintendo Co Ltd and others v PC Box Srl*, Case C-355/12, (23 January 2014) ('*Nintento* preliminary ruling')
- *Verizon Telecommunications Inc.* v. *Law Offices of Curtis V. Trinko*, LLP 540 U.S. 398, 2004 ('*Trinko* judgement')
- *United States v. Microsoft Corp.*, 87 F. Supp. 2d 30, 36 (D.D.C. 2000)
- *Sega Enterprises Ltd. v. Accolade, Inc*., 977 F.2d1510 (9th Cir. 1992)
- *United States v Terminal Railroad Association* 224 US 383 (1912)

Books and Chapters

- Anderman, S. and Schmidt, H. *EU Competition Law and Intellectual Property Rights: The Regulation of Innovation* (2nd edn, OUP 2011)
- Anderman, S. D. and Kallaugher, J. *Techonology Transfer and The New EU Competition Rules - Intellectual Property Licensing after Modernisation* (OUP 2006)
- Anderman, S. D. *EC Competition Law and Intellectual Property Rights: The Regulation of Innovation* (Clarendon Press 1998)
- Balkin, J. M., 'Information Power: The Information Society from an Antihumanist Perspective' in Ramesh Subramanian and Eddan Katz (eds.), *The Global Flow of Information: Legal, Social, and Cultural Perspectives* (New York University Press 2011) 232-249

- Band, J. and Katoh, M. *Interfaces on Trial 2.0* (The MIT Press 2011)
- Bauer, J. M., Weijnen, M. P. C., Turk, A. L. and Herder, P. M. 'Delineating the Scope of Convergence in Infrastructures' in W. A. H. Thissen and P. M. Herder (eds), *Critical Infrastructures State of the Art in Research and Application* (Kluwer Academic Publishers 2003) 209-232
- Benkler, Y., *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006)
- Boyle, J., *The Public Domain: Enclosing the Commons of the Mind* (Yale University of Press 2008)
- Coates, K., *Competition Law and Regulation of Technology Markets* (OUP 2011)
- Cornish, W., Llewelyn, D. and Aplin, T. *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (8th edn, Sweet & Maxwell 2013)
- Daly, A., *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart Publishing 2016)
- De Streel, A., 'Efficient Regulation of Dynamic Telecommunications Markets and the New Regulatory Framework in Europe' in R. Dewenter and J. Haucap (eds), *Access Pricing: Theory and Practice* (Elsevier B.V, 2007) 327-372
- Eagles, I. and Longdin, L. *Refusals to License Intellectual Property: Testing the Limits of Law and Economics* (Hart Publishing 2011)
- Efroni, Z., *Access-Right: The Future of Digital Copyright Law* (OUP 2011)

- Eisemann, T. R., 'Geoffrey Parker and Marshall Van Alstyne, Opening platforms: how, when and why?' in Annabelle Gawer (eds), *Platforms, Markets and Innovation* (Edward Elgar 2009) 131-162
- Elkin-Koren, N., 'It's all about control: Rethinking copyright in the new information landscape' in N. Elkin-Koren and N. Weinstock Netanel (eds.), *The Commodification of Information* (Kluwer Law International 2002) 79-106
- Fehling, C., Leymann, F., Retter, R., Schupeck, W. and Arbitter, P., *Cloud Computing Patterns: Fundamentals to Design, Build, and Manage Cloud Applications* (Springer, 2014)
- Finkelstein, R., 'Legal protection of business research and development: can it harm competition?' in M. Pittard, A. L. Monotti and J. Duns (eds) *Business, Innovation and the Law: Perspectives from Intellectual Property, Labour, Competition and Corporate Law* (Edward Elgar 2013) 244-267
- Fransman, M., *The New ICT Ecosystem: Implications for Policy and Regulation* (Cambridge University Press 2010)
- Frischmann, B. and Selinger, E., *Re-Engineering Humanity* (Cambridge University Press 2018)
- Gardler, R., 'Open Source and Governance' in Noam Shemtov and Ian Walden (eds), *Free and Open Source Software* (OUP 2013)
- Ghidini, G. and Arezzo, E., 'One, none, or a hundred thousand: how many layers of protection for software innovations?' in J Drexl (eds), *Research Handbook on Intellectual Property and Competition* (Edward Elgar 2008) 346-372

- Ghosh, R., ‘An Economic Basis for Open Standards’ in Laura DeNardis (eds), *Opening Standards: The Global Politics of Interoperability* (The MIT Press 2011) 75-96
- Goyder, J. and O’Regan, M., ‘Market Conduct’ in L. Garzaniti and M. O’Regan (eds), *Telecommunications, Broadcasting and the Internet: EU Competition Law and Regulation* (3rd edn, Sweet & Maxwell 2010) 1-73
- Helberger, N., *Controlling Access to Content - Regulating Conditional Access in Digital Broadcasting*, Kluwer Law International, 2005
- Henten, A. and Tadayoni, R., ‘The dominance of the IT industry in a converging ICT ecosystem’ in H. Mitomo, H. Fuke and E. Bohlin (eds), *The smart revolution towards the sustainable digital society: Beyond the era of convergence* (Edward Elgar 2015) 15-34
- Hoffman, S. G., *Regulation of Cloud Services under US and EU Antitrust, Competition and Privacy Laws* (PL Academic Research 2017)
- Hon, W. K. and Millard, C., ‘Control, Security and Risk in the Cloud’ in Christopher Millard (eds), Cloud Computing Law (OUP 2013) 18-36
- Hwang, K., Fox, G. C. and Dongarra, J. J., ‘Distributed and Cloud Computing: Form Parallel Processing to the Internet of Things’ (Elsevier, 2012) 191-206
- Jacob, R., Alexander, D. and Fisher, M., *Guidebook to Intellectual Property* (6th edn, Hart Publishing 2013)
- Jacobs, K., ‘Corporate standardization, management and innovation’ in Richard Hawkins, Knut Blind, Robert Page (eds), *Handbook on Innovation and standards* (Edward Elgar 2017) 377-397.

- Jaina, S. and Jain, R. K., *Patents: Procedures and Practices with Examples of Complete Specifications and Important Judgements* (Universal Law Publishing Co. Pvt. Ltd. 2011)
- Janevski, T., *NGN Architectures, Protocols and Services* (John Wiley & Sons, Ltd. 2014)
- Jones, A. and Sufrin, B., *EU Competition Law: Text, Cases and Materials* (5th edn, OUP 2014).
- Jones, A. and Sufrin, B., *EC Competition Law: Text, Cases and Materials* (4th edn, OUP 2011)
- Jütte, B. J., *Reconstructing European Copyright Law for the Digital Single Market: Between Old Paradigm and Digital Challenges* (Hart Publishing 2017)
- Karapapa, S. and McDonagh, L., *Intellectual Property Law* (OUP 2019)
- Kariyawasam, R., *International Economic Law and the Digital Divide: A New Silk Road* (Edward Elgar 2007)
- Kariyawasam, R., 'Interconnection, Access and Peering: Law and Precedent' in I. Walden and J. Angel (eds), *Telecommunications Law* (Blackstone Press Limited 2001) 135-223
- Katsoulacos, Y. and Ulph, D., 'Optimal Enforcement and Decision Structures for Competition Policy: Economic Considerations' in Federico Etro and Ioannis Kokkoris, *Competition Law and the Enforcement of Article 102* (OUP 2010) 73-82
- Korah, V., *Intellectual Property Rights and the EC Competition Rules* (Hart Publishing 2006)

- Laidlaw, E. B., *Regulating Speech in Cyberspace; Gatekeepers, Human Rights and Corporate Responsibility* (Cambridge University Press 2015)
- Laffont, J. and Tirole, J., *Competition in Telecommunications* (4th edn, The MIT Press 2002)
- Larouche, P., *Competition Law and Regulation in European Telecommunications* (Hart Publishing 2000)
- Leslie, C. R., *Antitrust Law and Intellectual Property Rights: Cases and Materials* (OUP 2011)
- Lessig, L., *Code; version 2.0* (Basic Books 2006)
- Malcolm, B. 'Patents and FOSS' in Noam Shemtov and Ian Walden (eds), *Free and Open Source Software* (OUP 2013)
- Marsden, P., 'Some Outstanding Issues from the European Commission's Guidance on Article 102 of the TFEU: Not-so-faint Echoes of Ordoliberalism' in F. Etro and Ioannis Kokkoris (eds), *Competition Law and the Enforcement of Article 102* (OUP 2010) 53-72
- Mazhelis, O., Luoma, E. and Warma, H., 'Defining an Internet-of-Things Ecosystem' in S. Andreev, S. Balandin and Y. Koucheryavy (eds), *Internet of Things, Smart Spaces, and Next Generation Networking* (Springer 2012) 1-14
- Melody, W. H., *Telecom Reform: Principles, Policies and Regulatory Practices* (Private Ingeniørfond, Technical University of Denmark 1997)
- Nihoul, P and Rodford, P. *EU Electronic Communications Law: Competition and Regulation in the European Telecommunications Market* (OUP 2004)
- Norman, H., *Intellectual Property Law* (OUP 2011)

- Nuechterlein, J. E. and Weiser, P. J., *Digital Crossroads: Telecommunications Law and Policy in the Internet Age* (2nd edn, The MIT Press 2013)
- Otero, B. G., 'Compelling disclosure of software interoperability information: A risk for innovation or a balanced solution?' in G. B. Dinwoodie (eds), *Intellectual Property and General Legal Principles: Is IP a Lex Specialis*? (Edward Elgar 2015) 69-90
- Palfrey, J. and Gasser, U., *Interop: The promise and perils of highly interconnected systems* (Basic Books 2012)
- Petrovčič, U. *Competition Law and Standard Essential Patents: A Transatlantic Perspective* (Kluwer Law International BV 2014)
- Psygkas, A., *From the "Democratic Deficit" to a "Democratic Surplus": Constructing Administrative Democracy in Europe* (OUP 2017)
- Schilling, M. A., 'Protecting or diffusing a technology platform: tradeoffs in appropriability, network externalities, and architectural control' in Annabelle Gawer, (eds) *Platforms, Markets and Innovation* (Edward Elgar 2009) 192-218
- Schneider, V. and Bauer, J. M., 'A network science approach to the Internet' in J. M. Bauer and M. Latzer (eds), Handbook on the Economics of the Internet (Edward Elgar 2016) 72-90
- Shawish, A. and Salama, M., 'Cloud Computing: Paradigms and Technologies' in F. Xhafa and N. Bessis (eds), *Inter-cooperative Collective Intelligence: Techniques and Applications, Studies in Computational Intelligence* (Springer-Verlag Berlin Heidelberg, 2014) 39-67.

- Spulber, D. F., ‘Competition Policy in Telecommunications’ in M. Cave, Sumit K. Majumdar and I. Vogelsang (eds), *Handbook of Telecommunications Economics* (Elsevier Science B. V. 2002) 477-508
- Sutor, Robert S., ‘Software Standards, Openness, and Interoperability’ in Laura DeNardis (eds), *Opening Standards: The Global Politics of Interoperability* (The MIT Press 2011) 209-217
- Thomas, G., *How to do your case study* (2nd edn, Sage 2016)
- Tight, M. *Understanding Case Study Research: Small-scale Research with Meaning* (Sage 2017).
- Tsilas, N. L., ‘Open Innovation and Interoperability’ in L. DeNardis (eds), *Opening Standards: The Global Politics of Interoperability* (The MIT Press 2011)
- Uckelmann, D., Harrison, M. and Michahelles, F., ‘An Architectural Approach Towards the Future Internet of Things’ in D. Uckelmann, M. Harrison and F. Michahelles (eds), *Architecting the Internet of Things* (Springer 2011)
- Vaidhyanathan, S., *Copyright and Copywrongs: The rise of Intellectual Property and How It Threatens Creativity* (New York University Press 2001)
- Van Eechoud, M., Hugenholtz, P. B., Van Gompel, S. Lucie Guibault and Helberger, N. *Harmonizing European Copyright Law: The Challenges of Better Lawmaking* (Kluwer Law International 2009)
- Van Rooijen, A. *The Software Interface Between Copyright and Competition Law: A Legal Analysis of Interoperability in Computer*

Programs (Kluwer Law International, Information Law Series, Vol. 20, 2011)

- Van Schewick, B., *Internet Architecture and Innovation* (The MIT Press 2012)
- Walden, I., 'Open Source as Philosophy, Methodology, and Commerce: Using Law with Attitude' in N. Shemtov and I. Walden (eds), *Free and Open Source Software* (OUP 2013)
- Walden, I., 'Access and Interconnection' in I. Walden (eds), *Telecommunications Law and Regulation* (4th edn, OUP 2012)
- Walden, I., 'Access and Interconnection' in I. Walden and J. Angel (eds), *Telecommunications Law and Regulation* (eds), (2nd edn, OUP 2005)
- Whish, R., *Competition Law* (5th edn, Butterworths 2003)
- Yin, R. K., *Case Study Research and Applications: Design and Methods* (6th edn, Sage 2018)

Journal Articles, Reports and Web Sources

- Abbott, J. 'Reverse Engineering of Software: Copyright and Interoperability' [2003] 14 Journal of Law and Information Science, 7-49
- Ahlborn, C., Evans, D. S. and Padilla, A. J. 'The Logic & Limits of the "Exceptional Circumstances Test" in Magill and IMS Health' [2005] 28 Fordham International Law Journal, 1109-1156
- Ahmed, M. Z. 'How Cloud Computing Application Architecture is Different from Traditional Application Architecture?' (2015)

<https://www.linkedin.com/pulse/how-cloud-computing-application-architecture-different-muhammad-ahmed/> accessed 9 October 2020

- Alberro, J. and Shcwabe, R. 'The Theory of Contestable Markets and its Legacy in Antitrust Practice' [2016] 16(1) Economics Committee Newsletter, 20-28
- Alexiadis, P. 'Forging a European Competition Policy Response to Online Platforms' [2017] 18(2) Business Law International, 91-154
- Alexiadis, P. 'Balancing the Application of ex post and ex ante Disciplines under Community Law in Electronic Communications Markets: Square Pegs in Round Holes?' (2012) <https://www.gibsondunn.com/wp-content/uploads/documents/publications/Alexiadis-BalancingtheApplicationofExPostandExAnteDisciplines.pdf> accessed 9 October 2020
- Alexiadis, P. and De Streel, A., 'Designing an EU Intervention Standard for Digital Platforms' (EUI Working Paper RSCAS 2020/14) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544694> accessed 9 October 2020
- Aliprandi, S. 'Interoperability and Open Standards: The Key to True Openness and Innovation' [2015] 3(1) International Free and Open Source Software Law Review, 5-24
- Arnold Porter, European Telecommunications Practice Group, 'Introduction to the New EU Regulatory Framework for Electronic Communications', (2002)
- Bagnoli, V. 'The big data relevant market as a tool: For a case by case analysis at the digital market' 12th Ascola Conference (Competition Law

for the Digital Economy) 12 June 2017) <https://ssrn.com/abstract=3064795> accessed 9 October 2020

- Ballon, P. and Van Heesvelde, E. 'ICT platforms and regulatory concerns in Europe' [2011] 35 Telecommunications Policy, 702-714
- Ballon, P. 'The Platformisation of the European Mobile Industry', [2009] 75 3rd Q Communications & Strategies, 15-34
- Bartolini, C., Santos, C. and Ullrich, C. 'Property and the cloud' [2018] 34 Computer Law and Security Review, 358-390
- Barzilai-Nahon, K. 'Gatekeeping: A critical review' 2009 43(1) Annual Review of Information Science and Technology 1-79
- Barzilai-Nahon, K. 'Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control' [2008] 59(9) Journal of the American Society for Information Science and Technology, 1493-1512
- Bauer, J. M. 'Governing the Mobile Broadband Ecosystem' [2015] 22(2) International Telecommunications Policy Review, 1-26
- Bauer, J. M. 'Platforms, systems competition, and innovation: Reassessing the foundations of communications policy' [2014] 38 Telecommunications Policy, 662-673
- Bauer, J. M. 'The Evolution of the European Regulatory Framework for Electronic Communications' (2013) IBEI Working Papers Telefonica Chair Series, 2013/41
- Belli, L. and Zingales, N. 'How Platforms are Regulated and How They Regulate Us' Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility (United Nations Internet Governance Forum, 2017)

- BEREC, Report Enabling the Internet of Things (BoR (16) 2016) 41 (BEREC Report) <http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things> accessed 9 October 2020
- Besen, S. M. and Sadowsky, G., 'The economics of Internet standards' in Johannes M. Bauer and Michael Latzer (eds), *Handbook on the Economics of the Internet* (Edward Elgar 2016) 211-228
- Biegel, A., Ganske, R. and Jurgovan, J. 'Broadened Antitrust Liability for Abusing Standards-Setting Process' [2006] 18(12) Intellectual Property & Technology Law Journal, 4-6
- Björkroth, T. 'Loyal or Locked-in – And Why Should We Care?' [2013] 10(1) Journal of Competition Law & Economics, 47-62
- Blackman, C. and Srivastava, L. *Telecommunications Regulation Handbook* (10th Anniversary edn, International Bank for Reconstruction and Development / World Bank, Infodev and ITU, 2011) <https://www.itu.int/pub/D-PREF-TRH.1-2011> accessed 9 October 2020
- Brown, I. 'Regulations and the Internet of Thing (IoT)', (2015) GSR15 discussion paper, <http://www.itu.int/en/ITU-D/Conferences/GSR/Pages/GSR2015/GSR15-discussion-paper.aspx> accessed 9 October 2020
- Cambridge Dictionary, 'Meaning of interoperability in English' <https://dictionary.cambridge.org/dictionary/english/interoperability> accessed 9 October 2020

- Cave, J. ‘Prisoners of Our Own Device - An Evolutionary Perspective on Lock-in, Technology Clusters and Telecom Regulation’ (*SSRN*, 15 August 2009) TPRC 2009 <http://ssrn.com/abstract=1995551> accessed 9 October 2020
- CERRE ‘Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets’ (CERRE Study, 2014) <https://www.cerre.eu/sites/cerre/files/141029_CERRE_MktDefMktPwrRegInt_ECMs_Final.pdf> accessed 9 October 2020
- Cisco, *Cisco Global Cloud Index: Forecast and Methodology*, (2016–2021 White Paper, November 19, 2018) (‘Cisco 2018 Global Cloud Index’) <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html> accessed by 9 October 2020
- Claybrook, B. ‘Cloud interoperability: Problems and best practices’, (*Computerworld*, 1 June 2011) <http://www.computerworld.com/article/2508726/cloud-computing/cloud-interoperability--problems-and-best-practices.html> accessed 9 October 2020
- Cloud Standard Consumer Council, *Interoperability and Portability for Cloud Computing: A Guide* (Version 2.0, 2017) <https://www.omg.org/cloud/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf > accessed 9 October 2020
- Colomo, P. I. ‘EU Competition Law in the Regulated Network Industries’ (2016) LSE Law, Society and Economy Working Papers 08/2016, 6 <http://dx.doi.org/10.2139/ssrn.2747785> accessed 9 October 2020

- Comino, S., Manenti, F. M. and Thumm, N. 'The Role of Patents in Information and Communication Technologies (ICTs): A Survey of the Literature' (2017) Marco Fanno Working Paper N. 212
- Competition Policy International 'The Counterfactual Analysis in EU Merger Control' (21 November 2013) <https://www.competitionpolicyinternational.com/the-counterfactual-analysis-in-eu-merger-control/> accessed 9 October 2020
- Comptia, *European Interoperability Framework: ICT Industry Recommendations* (White Paper, 2004) <http://www.urenio.org/e-innovation/stratinc/files/library/ict/15.ICT_standards.pdf> accessed 9 October 2020
- Conroy, M., 'Access to Works Protected by Copyright: Right or Privilege' [2006] 18(4) South African Mercantile Law Journal, 413-422
- Cottle, G. *CDNs could help smaller OTT players disrupt the content hierarchy* (Informa, 2012)
- Cottle, R. W. 'Multiple Equilibria' (International Encyclopedia of the Social Sciences, 2008) <https://www.encyclopedia.com> accessed 9 October 2020
- Cowen, T. and Gawer, A. 'Competition in the Cloud: Unleashing Investment and Innovation within and across Platforms' [2012] 85 Digiworld Economic Journal 1st Q, 45-62
- Craig Mc Taggart 'A Layered Approach to Internet Legal Analysis' [2003] 48 McGill Law Journal, 571-625
- CREATE, EU Copyright Reform <https://www.create.ac.uk/policy-responses/eu-copyright-reform/> accessed 9 October 2020

- Crémer, J., De Montjoye, Y. and Schweitzer, H. *Competition policy for the digital era*, (2019) <http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> accessed 9 October 2020
- Cygler, J., Sroka, W., Solesvik, M. and Debkowska, K. 'Benefits and Drawbacks of Coopetition: The Roles of Scope and Durability in Coopetitive Relationships' [2018] 10(8) Sustainability, 1-24
- Da Correggio Luciano, L. and Walden, I. 'Ensuring competition in the Clouds: The role of competition law?' (*SSRN*, 7 April 2014) <http://ssrn.com/abstract=1840547> accessed 9 October 2020
- Dadhich, M. 'Regulation of vertical mergers under European Union Law: Lessons to be Learnt by Other Jurisdictions' (2015) Europea Colleg Hamburg, Study Paper No. 3/15 <https://europa-kolleg-hamburg.de/wp-content/uploads/2015/11/Study-Paper_Dadhich.pdf> accessed 9 October 2020
- De Carvalho, N. P. 'Technical Standards, Intellectual Property and Competition - An Holistic View' [2015] 47 Washington University Journal Law & Policy, 61-129
- De la Guía, E., Lozano, M. D. and Penichet, V. M. R. 'Interacting with Objects in Games through RFID Technology' (2012) Intechopen <https://www.intechopen.com/books/radio-frequency-identification-from-system-to-applications/interacting-with-objects-in-games-through-rfid-technology> accessed 9 October 2020
- De Streel, A. 'The Relationship between Competition Law and Sector Specific Regulation: The case of electronic communications' [2008]

Volume XLVII, 2008/1 Reflets et perspectives de la vie économique, 53-70

- De Streel, A. 'The New Concept of "Significant Market Power" in Electronic Communications: The Hybridisation of the Sectoral Regulation by Competition Law' [2003] 24(10) European Competition Law Review, 535-542
- Devlin, A., Jacobs, M. and Peixoto, B. 'Success, Dominance and Interoperability' [2009] 84 Indiana Law Journal, 1157-1203
- Dr2 consultants, 'The Digital Services Act – How does it affect businesses in the EU?' (14 September, 2020) <https://dr2consultants.eu/digital-services-act-how-does-it-affect-businesses-in-the-eu/> accessed 9 October 2020
- Dredge, S., 'How does Facebook decide what to show in my news feed?' (Guardian, 30 June 2014) <https://www.theguardian.com/technology/2014/jun/30/facebook-news-feed-filters-emotion-study> accessed 9 October 2020
- Drexl, J. 'Anticompetitive Stumbling Stones on the Way to a Cleaner World: Protecting Competition in Innovation Without a Market' [2012] 8(3) Journal of Competition Law and Economics, 507-543
- Easley, R., Guo, H. and Kraemer, J. 'From Network Neutrality to Data Neutrality: A Techno-Economic Framework and Research Agenda' (*SSRN*, 8 March 2017) <https://ssrn.com/abstract=2666217> accessed 9 October 2020
- ECIS 'Special paper on cloud computing: Portability and interoperability of software and data across cloud services' (27 June 2016)

<http://www.ecis.eu/2016/06/special-paper-on-cloud-computing-portability-and-interoperability/> accessed 9 October 2020

- ECORYS and TNO, *A study on future trends and business models in communication services* (Final Report: A Study prepared for the European Commission DG Communications Networks, Content & Technology, 2016) ('2016 OTT Report')
- Edwards, D. W. 'Circulation Gatekeepers: Unbundling the Platform Politics of YouTube's Content ID', [2018] 47 Computers and Composition, 61-74
- Elkhodr, M., Shahrestani, S. and Cheung, H. 'The Internet of Things: New Interoperability, Management and Security Challenges' [2016] 8(2) International Journal of Network Security & Its Applications, 85-102
- Elkin-Koren, N., 'Copyrights in Cyberspace - Rights without Laws' [1998] 73 Chicago-Kent Law Review, 1155-1201
- Elkin-Koren, N., 'Cyberlaw and Social Change: A democratic approach to copyright law in cyberspace' [1996] 14 Cardozo Arts and Entertainment Law Journal 215-296
- Elkin-Koren, N. 'Public/Private and Copyright Reform in Cyberspace' (1996) 2(2) Journal of Computer-Mediated Communication <https://doi.org/10.1111/j.1083-6101.1996.tb00059.x> accessed 9 October 2020
- EPO, 'Fundamentals of infringement' <https://e-courses.epo.org/wbts_int/litigation/FundamentalsOfInfringement.pdf> accessed 9 October 2020

- EPO, ‘Patents for software? European law and practice’ (2009) <https://tt.tecnico.ulisboa.pt/files/sites/41/PI-Pack-INPI-E-Patents-for-Software-EPO.pdf> accessed 9 October 2020
- Erdos, I. ‘A Measure to Protect Computer-Implemented Inventions in Europe’ [2004] 3 Journal of Information, Law and Technology <https://warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/erdos> accessed 9 October 2020
- ERG, Final Report on IP Interconnection, Project Team on IP - Interconnection and NGN, (2007) ERG (07) 09 <https://www.berec.europa.eu/doc/publications/erg_07_09_rept_on_ip_interconn.pdf> accessed 9 October 2020
- European Commission, ‘Digital Single Market: Bringing down barriers to unlock online opportunities’ <http://ec.europa.eu/priorities/digital-single-market_en> accessed 9 October 2020
- European Commission, ‘Digital Single Market: Electronic Communications Laws’ <https://ec.europa.eu/digital-single-market/en/telecoms-rules> accessed 9 October 2020
- European Commission, ‘Digital Single Market: Free flow of non-personal data’ <https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data> accessed 9 October 2020
- European Commission, ‘Digital Single Market: The EU copyright legislation’ (28 August 2015) <https://ec.europa.eu/digital-single-market/en/eu-copyright-legislation> accessed 9 October 2020

- European Parliament, 'Legislative Train Schedule' <http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market> accessed 9 October 2020
- European Parliament 'Review of the ePrivacy Directive' (Think Tank, 03/02/2017) <http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2017)587347> accessed 9 October 2020
- European Research Cluster on the Internet of Things, 'IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps' (2015) <http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Semantic_Interoperability_Final.pdf> accessed 9 October 2020
- European Telecommunications Standards Institute (ETSI), *Version 1.0.* (Cloud Standards Coordination, Final report, 2013) <https://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF> accessed 9 October 2020
- Faulhaber, G. R. 'Access ≠ Access1 + Access2' [2002] 3 Law Review of Michigan State University, Detroit College of Law, 677-708
- Favale, M., 'The Right of Access in Digital Copyright: Right of the Owner or Right of the User?' [2012] 15(1) The Journal of World Intellectual Property, 1-25
- Feasey, R. 'Confusion, denial and anger: The response of the telecommunications industry to the challenge of the Internet' [2015] 39(6) Telecommunications Policy, 444-449

- Fernandes, M. D. ‘Internet of Things’ (PwC Partner, 2018), <https://www.pwc.pt/pt/temas-actuais/pwc-apresentacao-iot.pdf> accessed 9 October 2020
- Fishwick, F. ‘The Definition of the Relevant Market in the Competition Policy of the European Economic Community’ [1993] 63(1) Revue D'économie Industrielle, 174-192
- Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L. and González-López, M. ‘A Review of the Internet of Things for Defense and Public Safety’ (2016) 16 Sensors <https://www.mdpi.com/1424-8220/16/10/1644> accessed 9 October 2020
- Funk, J. L. ‘Standards, critical mass, and the formation of complex industries: A case study of the mobile Internet’ [2011] 28(4) Journal of Engineering and Technology Management, 232-248
- Gandhi, V. ‘5G to become the catalyst for innovation in the IoT’ (Network World, 13 April 2018) <https://www.networkworld.com/article/3268668/internet-of-things/5g-to-become-the-catalyst-for-innovation-in-iot.html> accessed 9 October 2020
- Gasser, U. ‘Interoperability in the digital ecosystem’ (2015) GSR15 discussion paper, <http://www.itu.int/en/ITU-D/Conferences/GSR/Pages/GSR2015/GSR15-discussion-paper.aspx> accessed 9 October 2020
- George, C. and Chandak, N. ‘Issues and Challenges in Securing Interoperability of DRM Systems in the Digital Music Market’ [2006] 20/3 International Review of Law Computers & Technology, 271-285

- Geradin, D. and Layne-Farrar, A. ‘The Logic and Limits of Ex Ante Competition in a Standard Setting Environment’ [2007] 3(1) Competition Policy International, 78-106
- Geier, M. ‘United States v. Microsoft Corp.’ [2001] 16(1) Berkeley Technology Law Journal, 297-322
- Geradin, D. and Rato, M. ‘Can Standards-Setting Lead to Exploitative Abuse? A Dissonant View on Patent Hold-up, Royalty-Stacking and the Meaning of FRAND’ [2007] 3(1) European Competition Journal, 101-161
- Giannino, M. ‘The appraisal of mergers in high technology markets under the EU merger control regulation: from *Microsoft/Skype* to *Facebook/WhatsApp*’ (*SSRN*, 12 January 2015) <https://ssrn.com/abstract=2548560> accessed 9 October 2020
- Gil-Moltó, M. J. ‘Economic Aspects of the Microsoft Case: Networks, Interoperability and Competition’ (2008) University of Leicester, Working Paper No. 08/39 <http://www.le.ac.uk/economics/research/RePEc/lec/leecon/dp08-39.pdf> accessed 9 October 2020
- Ginsburg, J. C., ‘Essay: From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law’ [2003] 50 Journal of the Copyright Society of the U.S.A., 113-132
- Gleeson, N. and Walden, I. ‘‘It's a jungle out there’?: Cloud computing, standards and the law’ (2014) 5(2) European Journal of Law and Technology <http://ejlt.org/article/view/363/460> accessed 9 October 2020

- Graef, I. ‘Data as Essential Facility Competition and Innovation on Online Platforms’ (PhD Dissertation, KU Leuven Faculty of Law 2016)
- Graef, I. ‘How can software interoperability be achieved under European competition law and related regimes?’ [2011] 5(1) Journal of European Competition Law & Practice, 6-19
- Graef, I. ‘Tailoring the Essential Facilities Doctrine to the IT Sector: Compulsory Licensing of Intellectual Property Rights after Microsoft’ [2011] 7 Cambridge Student Law Review, 1-20
- Gregory G. W. ‘Connecting Antitrust Standards to the Internet of Things’ [2014] 29(1) Antitrust ABA, 62-70
- Griffin, J. G.H., ‘A call for a doctrine of “information justice”’ [2016] 1 Intellectual Property Quarterly, 44-62
- Hahn, J. ‘Nonlinear Pricing of Telecommunications with Call and Network Externalities’ (2002) <http://www.krannert.purdue.edu/centers/ijio/Accepted/1720.pdf> accessed 9 October 2020
- Harrison, H., Birks, M., Franklin, R. and Mills, J. ‘Case Study Research: Foundations and Methodological Orientations’ (2017) 18 Forum: Qualitative Social Research <http://dx.doi.org/10.17169/fqs-18.1.2655> accessed 9 October 2020
- Hart, R. ‘Interoperability Information and the Microsoft Decision’ [2006] 7 European Intellectual Property Review, 361-367
- Hau, T., Burghardt, D. and Brenner, W. ‘Multihoming, content delivery networks, and the market for Internet connectivity’ [2011] 35 Telecommunications Policy, 532-542

- Helberger, N. ‘Access to technical bottleneck facilities: the new European approach’ [2002] 46, 2nd Q Communications & Strategies, 33-74
- Helberger, N., Kleinen-von Königslöw, K. and Van der Noll, R. ‘Regulating the new information intermediaries as gatekeepers of information diversity’ [2015] 17(6) Info, 50-71
- Hoehn, T. and Lewis, A. ‘Interoperability Remedies, FRAND Licensing and Innovation: A Review of Recent Case Law’ (2013) 34(2) European Competition Law Review, 101-111
- Holm, J. ‘Regulating Network Access Prices under Uncertainty and Increasing Competition: The Case of Telecommunications and Local Loop Unbundling in the EU’ (MSc Thesis, University of Copenhagen 2000)
- House of Lords, Select Committee on Communications, *Regulating in a digital world* (2nd Report of Session 2017-19, March 2019)
- Hutchinson, T. ‘The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law’ 3 [2015] Erasmus Law Review, 130-138.
- Institute of Electrical and Electronics Engineers (IEEE), Standards Glossary, 2016 <https://www.standardsuniversity.org/article/standards-glossary/> accessed 9 October 2020
- International Telecommunications Union (ITU) Telecommunications Development Sector, *Regulatory Challenges and Opportunities in the New ICT Ecosystem* <https://www.itu.int/pub/D-PREF-BB.REG_OUT03-2018> accessed 9 October 2020
- ITU, *Overview of the Internet of Things* (ITU-T Y.4000/Y.2060. 2012) <https://www.itu.int/rec/T-REC-Y.2060-201206-I> accessed 9 October 2020

- ITU, ‘NGN Working Definition’ <http://www.itu.int/ITU-T/studygroups/com13/ngn2004/working_definition.html> accessed 9 October 2020
- Kariyawasam, R. ‘Defining Dominance for Bits and Bytes: A new Layering Theory for Significant Market Power?’ [2005] 26(10) European Competition Law Review, 581-594
- Kariyawasam, R. ‘Telecoms Regulation - Peering and Transit Over TCP/IP Networks’ [2001] 17(1) Computer Law & Security Report, 36-40
- Kartner, F. ‘Merger remedies: fostering innovation?’ [2016] 12(2-3) European Competition Journal, 298-319
- Kerber, W. and Schweitzer, H. ‘Interoperability in the Digital Economy’ [2011] 8(1) JIPITEC, 39-58
- Kesan, J. P. ‘Open Standards’ (2018) University of Illinois College of Law Legal Studies Research Paper No. 18-38 <https://ssrn.com/abstract=3260138> accessed 9 October 2020
- KPMG, Securing the benefits of industry digitisation (A Report for Vodafone, 2015) 5 <https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2017/02/vodafonewebaccess.pdf> accessed 9 October 2020
- Kutterer, C. ‘Future Models for Service Regulation - Implications for OTTs, Telcoes and Consumers’ (WIK Conference: New rules for digital networks and services?, Brussels, 18 October 2016)
- Laidlaw, E. B. ‘Private Power, Public Interest: An Examination of Search Engine Accountability’ [2009] 17(1) International Journal of Law and Information Technology, 113-145

- Larouche, P. and Van Overwalle, G. 'Interoperability standards, patents and competition policy' (2014) TILEC Discussion Paper DP 2014-050, December 2014
- Lassig, B. 'CDN Technology: How Net Neutrality Will Affect Global CDNs' (*CDNetworks Americas*, 21 February 2018) <http://nl.cdnetworks.com/en/news/how-net-neutrality-will-affect-global-cdns/6811> accessed 9 October 2020
- Leonard, J. 'Google, Microsoft, Facebook and Twitter team up on data portability project' (*Computing*, July 23, 2018) <https://www.computing.co.uk/ctg/news/3036306/google-microsoft-facebook-and-twitter-team-up-on-data-portability-project> accessed 9 October 2020
- Lynskey, O. 'Regulating 'Platform Power' (2017) LSE Law, Society and Economy Working Papers, 1/2017 <http://eprints.lse.ac.uk/73404/1/WPS2017-01_Lynskey.pdf> accessed 9 October 2020
- Mansell, R. and Steinmueller, W. E., 'Intellectual property rights: the development of information infrastructures for the information society' (A study carried out for the STOA programme of the European Parliament, Final Report, 1995) <http://eprints.lse.ac.uk/24969/> accessed 9 October 2020
- Marcus, J. S. and Elixmann, D. 'Regulatory Approaches to NGNs: An International Comparison' [2008] 69, 1st Q Communications & Strategies, 19-40

- Marini-Balestra, F. and Tremolada, R. 'Digital markets and merger control: balancing big data and privacy against competition law - a comment on the European Commission's decision in the *Microsoft/LinkedIn* merger' [2017] 38(7) European Competition Law Review, 337-345
- Markwith, J. 'Key intellectual property issues in acquisitions involving open source software' [2008] Computer and Telecommunications Law Review, 45-49
- Mc Taggart, C. 'A Layered Approach to Internet Legal Analysis', [2003] 48 McGill Law Journal, 571-625
- McMahon, K. 'Interoperability: "Indispensability" and "Special Responsibility" in High Technology Markets' [2007] 9 Tulane Journal of Technology and Intellectual Property, 123-172
- Meisel, J. B. and Needles, M. 'Voice over internet protocol (VoIP) development and public policy implications' [2005] 7(3) Info, 3-15
- Mendler, C. *CDNs, the Cloud and Carrier Ethernet: The new golden triangle* (Informa, 2012)
- Messina, M. 'Article 82 and the New Economy: Need for Modernisation?' [2006] 2(2) The Competition Law Review, 73-98
- Miller, L. L. 'The Use of Case Studies in law and Social Science Research' [2018] 14 Annual Review of Law and Social Science 381-396
- Miller, R. 'The OSI Model: An Overview' (SANS Institute Information Security Reading Room, 2019) <https://www.sans.org/reading-room/whitepapers/standards/osi-model-overview-543> accessed by 9 October 2020

- Mindel, J. L. and Sicker, D. C. 'Leveraging the EU regulatory framework to improve a layered policy model for US telecommunications markets' [2006] 30 Telecommunications Policy, 136-148
- Mintzer, E. S. and Breed, L. M. 'How to Keep the Fox Out of the Henhouse: Monopolization in the Context of Standards-Setting Organizations' [2007] 19(9) Intellectual Property & Technology Law Journal, 5-12
- Mittelstadt, B. D., et al, 'The ethics of algorithms: Mapping the debate' July-December 2016, Big Data & Society, 1-21
- National Institute for Standards and Technology (NIST), US Department of Commerce, The NIST Definition of Cloud Computing (Recommendations of the National Institute for Standards and Technology, Special publication 800-145, 2011)
- Nikolinakos, N. 'The New Legal Framework for Digital Gateways-The Complementary Nature of Competition Law and Sector-Specific Regulation' [2000] 9 European Competition Law Review, 408-414
- Noura, M., Atiquzzaman, M. and Gaedke, M. 'Interoperability in Internet of Things: Taxonomies and Open Challenges' [2019] 24 Mobile Networks and Applications, 796-809
- Ocho, R. E. 'Architectural evolution through softwarisation: On the advent of software-defined networks' (PhD Thesis, The London School of Economics and Political Science, 2016)
- OECD, *Communications Outlook 2013* (2013) <http://www.oecd.org/sti/broadband/oecd-communications-outlook-19991460.htm> accessed 9 October 2020

- OECD, *The Internet of Things: Seizing the benefits and Addressing the Challenges* (Background report for Ministerial Panel 2.2, 2016)
- Oen, H. M. 'Interoperability at the Application Layer in the Internet of Things' (MSc Thesis, Norwegian University of Science and Technology 2015)
- Olhede, S. C. and Wolfe, P. J., 'The algorithms ubiquity of algorithms in society: implications, impacts and innovations' (2018) The Royal Society Publishing <https://dx.doi.org/10.1098/rsta.2017.0364> accessed 9 October 2020.
- Open Connectivity Foundation, 10 October 2016 <https://openconnectivity.org/announcements/allseen-alliance-merges-open-connectivity-foundation-accelerate-internet-things> accessed 9 October 2020
- Otero, B. G. 'Mandating Portability as a Strategy to Achieve Interoperability between On-line Platforms: Pros & Cons', Proceedings of the 12th International Conference on Internet, Law & Politics (Universitat Oberta de Catalunya, Barcelona, 7-8 July 2016) 217-233
- Oxford Dictionaries, 'Definition of interoperability in English' <https://en.oxforddictionaries.com/definition/interoperability> accessed 9 October 2020
- Palfrey, J and Gasser, U. 'Fostering innovation and trade in the global information society: The different facets and roles of interoperability' (2011) NCCR Trade Regulation Working Paper No. 2011/39 <https://www.wti.org/media/filer_public/f7/a7/f7a7ae35-d43a-4e82-8cef-4ca26b7bb778/gasser_and_palfrey_final.pdf> accessed 9 October 2020

- Peitz, M. and Valletti, T. ‘Reassessing competition concerns in electronic communications markets’ [2015] 39 Telecommunications Policy, 896-912
- Petit, N. ‘Innovation, Competition, Unilateral Effects and Merger Control Policy’ (SSRN, 29 January 2018) <https://ssrn.com/abstract=3113077> accessed 9 October 2020
- Plantin, J., Lagoze, C., Edwards, P. N. and Sandvig, C. ‘Infrastructure studies meet platform studies in the age of Google and Facebook’ [2018] 20(1) New media & society, 293–310
- Popernik, S. B. ‘The Creation of an Access Right in the Ninth Circuit's Digital Copyright Jurisprudence’ [2013] 78(2) Brooklyn Law Review, 697-740
- Porter, M. E. and Heppelmann, J. E. ‘How Smart, Connected Products Are Transforming Competition’ (2014) Harvard Business Review, <https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition> accessed 9 October 2020
- Poudel, S. ‘Internet of Things: Underlying Technologies, Interoperability, and Treats to Privacy and Security’ [2016] 31(2) Berkeley Technology Law Journal Annual Review, 997-1022
- Reichl, W. and Ruhle, E. ‘NGA, IP-Interconnection and their Impact on Business Models and Competition’ [2008] 69, 1st Q Communications & Strategies 41-62
- Renda, A. ‘Competition, neutrality and diversity in the cloud’ 85 [2012] Digiworld Economic Journal 1st Q 23, 28-30
- Renda, A., Simonelli, F., Mazziotti, G., Bolognini, A. and Luchetta, G. *The Implementation, Application and Effects of the EU Directive on Copyright*

in the Information Society (CEPS Special Report, No. 120, November 2015)

- Ridyard, D. 'The Commission's Article 82 Guidelines: some reflections on the economic issues' [2009] 30(5) European Competition Law Review, 230-236
- Rose, K., Eldridge, S. and Chapin, L. 'The Internet of Things: An Overview' (Internet Society, 2015) <http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf> accessed 9 October 2020
- Rouse, M. 'CDN (content delivery network)' (*TechTarget*, 31 July 2014) <https://searchnetworking.techtarget.com/definition/CDN-content-delivery-network> accessed 9 October 2020
- Samuelson, P. 'The Past, Present and Future of Software Copyright Interoperability Rules in the European Union and United States' [2010] 34(3) European Intellectual Property Review, 229- 236
- Samuelson, P. 'Are Patents on Interfaces Impeding Interoperability' [2009] 93 Minnesota Law Review, 1943-2019
- Samsung, 'SmartThings – Featured Products' <https://www.smartthings.com/gb/products> accessed 9 October 2020
- Scantamburlo, T., Charlesworth, A. and Cristianini, N. 'Machine decisions and human consequences' in K. Yeung and M. Lodge Algorithmic Regulation (OUP, 2019) 49-81
- Sehgal, V. K., Patrick, A. and Rajpoot, L. 'A Comparative Study of Cyber Physical Cloud, Cloud of Sensors and Internet of Things: Their Ideology,

Similarities and Differences' (IEEE International Advance Computing Conference (IACC) 2014) 708-716

- Sharron, S. and Tuckett, N. 'The Internet of Things: Evaluating the Interplay of Interoperability, Industry Standards and Related IP Licensing Approaches' [2016] The Licensing Journal, 8-19
- Shilawat, S. 'Cloud Interoperability and Portability' (*Forbes*, 22 June 2018) <https://www.forbes.com/sites/forbestechcouncil/2018/06/22/cloud-interoperability-and-portability/#5512c41f4577> accessed 9 October 2020
- Sicker, D. and Mindel, J. 'Refinements of a layered model for telecommunications policy' [2002] 1 Journal on Telecommunications and High Technology Law, 69-94
- Sicker, D. C. and Blumensaadt, L. 'Misunderstanding the Layered Model(s)' [2006] 4 Journal of Telecommunications and High Technology Law, 299-320
- Singh, J. and Powles, J. 'Why the internet of things favours dominance' (Guardian, 24 July 2015) <https://www.theguardian.com/technology/2015/jul/24/internet-of-things-centralisation-dominance> accessed 9 October 2020
- Sluijs, J. P., Larouche, P. and Sauter, W. 'Cloud Computing in the EU Policy Sphere: Interoperability, Vertical Integration and the Internal Market' [2012] 3 JIPITEC, 12-32
- Staniszewski, P. 'The interplay between IP rights and competition law in the context of standardization' [2007] 2(10) Journal of Intellectual Property Law and Practice, 666-681

- Stocker, V. ‘Interconnection and Capacity Allocation for all-IP Networks: Walled Gardens or Full Integration?’ (43rd TPRC Conference, Arlington, September 2015)
- Stocker, V., Smaragdakis, G., Lehr, W. and Bauer, S. ‘The growing complexity of content delivery networks: Challenges and implications for the Internet ecosystem’ [2017] 41(10) Telecommunications Policy, 1003-1016
- The Open Group, ‘Cloud Computing Portability and Interoperability’ <http://www.opengroup.org/cloud/cloud_iop/p3.htm> accessed 9 October 2020
- United Nations Conference on Trade and Development (UNCTAD) (Trade and Development Board Commission on Investment, Technology and Related Financial Issues), *Competition Policy and the Exercise of Intellectual Property Rights* (Report by the UNCTAD Secretariat, 2008) <http://unctad.org/en/Docs/c2clpd68_en.pdf> accessed 9 October 2020
- Unver, M. B. ‘What cloud interoperability connotates for EU policy making: Recurrence of old problems or new ones looming on the horizon?’ [2019] 43 Telecommunications Policy, 154-170
- Unver, M. B. ‘Turning the crossroad for a connected world: reshaping the European prospect for the Internet of Things’ [2018] 26(2) International Journal of Law and Information Technology, 93-118
- Unver, M. B. ‘Is a fine-tuning approach sufficient for EU NGA policy? A global review around the long-lasting debate’ [2015] 11(39) Telecommunications Policy, 957-979

- Unver, M. B. ‘Essential Facilities Doctrine under EC Competition Law and Particular Implications of the Doctrine for Telecommunications Sectors in EU and Turkey’ (MS Thesis, Middle East Technical University 2004)
- Usher-Layser, Nikki., ‘Newsfeed: Facebook, Filtering and News Consumption’ (2016) 96(3) Phi Kappa Phi Forum, 18-21
- Van den Bulck, P. ‘Patentability of Software’ (*ULYS Net*), <https://www.ulys.net/upload/conferences/doc/Patentability%20of%20Software.pps> accessed 21 August 2018
- Van Dijck, J. and Nieborg, D. and Poell, T., ‘Reframing platform power’ (2019) 8(2) Internet Policy Review, 4 <DOI: 10.14763/2019.2.1414> accessed 9 October 2020
- Van Rooijen, A. ‘Devising Ex ante Interoperability Rules: Lessons from the Court of First Instance’s Microsoft Judgment’, [2011] 14 International Journal of Communications Law & Policy, 1-37
- Vanberg, A. D. ‘The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?’ [2018] 21(7) Journal of Internet Law, 11-20
- Vanberg, A. D. and Unver, M. B. ‘The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?’ (2017) 8(1) European Journal of Law and Technology <http://ejlt.org/article/view/546> accessed 9 October 2020
- Vezzoso, S. ‘Copyright, Interfaces, and a Possible Atlantic Divide’ [2012] 2 Jipitec, 153-161

- Walley, K. Coopetition: An Introduction to the Subject and an Agenda for Research [2007] 37(2) International Studies of Management & Organisation, 11-31
- Watts, S. 'SaaS vs PaaS vs IaaS: What's the difference and how to choose?' (BMC Blog, 22 September 2017) <https://www.bmc.com> accessed 9 October 2020
- Weiser, P. 'Networks Unplugged: Towards A Model of Compatibility Regulation Between Information Platforms' (29th TPRC Conference, Washington, September 2001)
- Welbers, K., 'Gatekeeping in the Digital Age' (PhD Thesis, Vrije Universiteit Amsterdam 2016)
- Werbach, K. 'Breaking the Ice: Rethinking Telecommunications Law for the Digital Age' [2005] 4 Journal on Telecommunications and High Technology Law, 59-96
- Werbach, K. 'A Layered Model for Internet Policy' [2002] 1 Journal on Telecommunications & High Technology Law, 37-68
- Weston, S. 'Improving interoperability by encouraging the sharing of interface specifications' [2017] 9(1) Law, Innovation and Technology, 78-116
- Weston, S. E. 'The Legal Regulation of Interoperability in an Oligopolistic Market' (PhD thesis, Bournemouth University 2015)
- Whitt, R. S. 'A horizontal leap forward: formulating a new public policy framework based on the network layers model' [2003] 56(3) Federal Communications Law Journal, 587-672

- Wilding, D. and King, I. ‘Reviewing the Layered Model’ [2018] 46(1) InterMEDIA, 13-17
- World Intellectual Property Organisation (WIPO) ‘What is a Trade Secret?’ <https://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm> accessed 9 October 2020
- Wrobel, G. G. ‘Connecting Antitrust Standards to the Internet of Things’ [2014] 29(1) Antitrust ABA, 62-70
- Yeung, K., ‘Why worry about decision-making by machine?’ in K. Yeung and M. Lodge (eds) Algorithmic Regulation (OUP, 2019) 21-48
- Yoo, C. ‘Protocol Layering and Internet Policy’ [2013] 161 University of Pennsylvania Law Review, 1707-1771
- Yoo, C. S. ‘Cloud Computing: Architectural and Policy Implications’ [2011] 38 Review of Industrial Organization, 405-421
- Zhang, S. ‘How have network effects affected the European Commission’s enforcement of competition law in technology enabled markets?’ [2015] 36 European Competition Law Review, 82-92
- Zhou, J., Leppänen, T., Harjula, E., Ylianttila, M., Ojala, T., Yu, C., Jin, H., Tianruo, L. and Huazhong, Y. ‘CloudThings: A Common Architecture for Integrating the Internet of Things with Cloud Computing’ (2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design, 27-29 June 2013) 651-657
- Zingales, N. ‘Of Coffee Pods, Videogames, and Missed Interoperability: Reflections for EU Governance of the Internet of Things’ (2016) TILEC Discussion Paper (DP 2015-026)