

Internet of Things and the Law

Legal Strategies for Consumer-Centric
Smart Technologies

Guido Noto La Diega

First Published 2023

ISBN: 978-1-138-60479-7 (hbk)

ISBN: 978-1-032-30579-0 (pbk)

ISBN: 978-0-429-46837-7 (ebk)

6 The Internet of Things (You Don't Own) under Bourgeois Law

An Integrated Tactic to Rebalance
Intellectual Property

(CC BY-NC-ND 4.0)

DOI: 10.4324/9780429468377

 **Routledge**
Taylor & Francis Group
LONDON AND NEW YORK

6 The Internet of Things (You Don't Own) under Bourgeois Law

An Integrated Tactic to Rebalance Intellectual Property

Science, generally speaking, costs the capitalist nothing, a fact that by no means prevents him from exploiting it.

Marx, *Das Kapital* (1)

6.1 Introduction: Intellectual Property and Rentier Capitalism

It is a commonly held view that intellectual property (IP) is a policy bargain whereby exclusive rights and monopolies are granted as a reward to intellectual labour and investments in order to incentivise innovation and creativity.¹ The idea that IP rights (IPRs) would be a necessary incentive has been largely debunked.² Law and economics studies demonstrated that IP is just another product of capitalism aimed at creating new enclosures of the 'commons.'³ This notwithstanding, a number of national and international laws have kept expanding its scope and augmenting the relevant level of protection. Most IP-stemming monopolies are temporary⁴ on paper but end up producing revenues that are regarded as rents on a virtually permanent basis. The elevation of IP to perpetual rent is rendered possible by complex strategies that rely on cumulation of IPRs, factual control over data and service, contracts, and technical protection measures. Favoured by a legal environment that is 'heavily tilted in favour of IP rent-seekers,'⁵ IP has become the key ideological device of rentier capitalism. Traditionally, the phenomenon of rentiers refers to the fact that landowners would exploit their monopoly power over the land to impose a rent that was a monopoly price. As noted by Marx in *The Poverty of Philosophy*, '[r]ent, in the Ricardian sense, is patriarchal agriculture

1 Robert P Merges, *Justifying Intellectual Property* (HUP 2011).

2 Andreas Von Gunten, *Intellectual Property Is Common Property: Arguments for the Abolition of Private Intellectual Property Rights* (buch et netz 2015).

3 N Stephan Kinsella, *Against Intellectual Property* (Ludwig von Mises Institute 2008); James Boyle, 'The Second Enclosure Movement and the Construction of the Public Domain' in *Copyright Law* (Routledge 2017) 63.

4 Trade secrets and trademarks constitute the exception as they can potentially last forever as long as, respectively, they are kept secret and they are renewed.

5 Brett Christophers, *Rentier Capitalism. Who Owns the Economy, and Who Pays for It?* (Verso 2020) 178.

transformed into commercial industry, industrial capital applied to land, the town bourgeoisie transplanted into the country.⁶ Marx and Ricardo could not foresee that new forms of rent-seeking would become an essential component of capitalism: rent-seeking through IPRs.⁷ The IoT is pivotal to rentier capitalism as it generates ‘new sources of rent, new infrastructures of rentier relations, and new mechanisms of extraction and enclosure.’⁸ While the IoT is not rentier in nature, the historically existing IoT is indeed rentier also thanks to IP abuses. According to Jathan Sadowski, data extraction, capital convergence, and digital enclosure are the main mechanisms of rentier capitalism.⁹ IP is key to digital enclosure, as instantiated by the use of software licenses to control access and collecting rents over the physical world, regardless of the ownership of the underlying tangible assets.¹⁰

The IoT ushers in an era of ubiquitous computing and ubiquitous IPRs. IP is everywhere and lends itself to monopolise virtually anything.¹¹ One may be naively inclined to think that one’s own phone is one’s own property. That is not the case. One’s phone belongs to the holders of the copyright on the code running on it, the manufacturers owning its design, and the patents on how it works, as well as trademarks not only on logos but also on things such as the way one ‘swipes.’¹² What happens when being embedded with software and other IP-protected digital contents is no longer an exclusive feature of computers and phones? What happens when proprietary Things and closed systems are everywhere: in one’s bedroom, in one’s bathroom, in one’s body? Our behaviour becomes heavily restricted by the factual, legal, and technical control that IoT companies retain over their Things – and that we correspondingly lose. We have become digital tenants, not owning or controlling any of the objects around us and data about us.¹³ To the point that, one can argue, we no longer own: *we are owned*.¹⁴

This chapter will present the main IP issues in the IoT and concentrate on one of them that has been framed as ‘death of ownership’ by Joshua Fairfield in

6 Karl Marx, *The Poverty of Philosophy. Answer to the Philosophy of Poverty by M. Proudhon (1847)* (Herr 1913) 174. On the relationship between Marx and David Ricardo see Giovanni A Caravale, ‘On Marx’s Interpretation Of Ricardo: A Note’ (1989) 17 *Atlantic Economic Journal* 6.

7 David Harvey, *Marx, Capital and the Madness of Economic Reason* (Profile 2017) 37.

8 Jathan Sadowski, ‘The Internet of Landlords: Digital Platforms and New Mechanisms of Rentier Capitalism’ (2020) 52 *Antipode* 562, 564.

9 *ibid* 570.

10 *ibid* 576.

11 Gustavo Ghidini, ‘Prospettive “Protezioniste” Nel Diritto Industriale’ [1995] *Rivista di diritto industriale* 73; Marco Ricolfi, ‘Il Futuro Della Proprietà Intellettuale Nella Società Algoritmica’ [2019] *Giur it* 10.

12 *Match Group, LLC v Bumble Trading Inc.*, No. 6:18-cv-00080 (W.D. Tex, Mar. 16, 2018). The dispute was settled in June 2020.

13 Zeynep Tufekci, ‘We Are Tenants on Our Own Devices’ [2019] *Wired* <www.wired.com/story/right-to-repair-tenants-on-our-own-devices/>.

14 Christina Mulligan, ‘Personal Property Servitudes on the Internet of Things’ (2015) 50 *Georgia Law Review* 1121; Joshua AT Fairfield, *Owned: Property, Privacy, and the New Digital Serfdom* (CUP 2017). This book has been consulted as an e-book, and since its digital pages were not numbered, pinpointing was not possible.

Owned,¹⁵ a germinal book that will provide an initial framework to understand this issue. Ownership (of Things) is dying either because of the shift from sale to subscription or because users only formally own their Things but they cannot exercise any of the powers traditionally associated to property as IoT companies control every layer of the Thing. This ‘tethered economy’¹⁶ has been seen as an attack on the concept of property reminiscent of feudal times, when ‘serfs of feudal Europe . . . lacked rights in the land they worked.’¹⁷ Similarly, users of Things would not own them but simply manage them on behalf of the IoT overlords – in this sense, they would be digital serfs. In reality, as will be argued in this chapter, the death of ownership – and IP abuses in the IoT more generally – has its roots in the individualistic outlook of ‘bourgeois’ law under capitalism, rather than resembling the medieval legal system.

Alongside desk-based research of EU laws, UK laws will be taken into account when national implementations can shed light on whether it is possible to rely on IP’s internal and external limitations to protect the IoT user affected by the death of ownership. This will be complemented by qualitative research, namely, text analysis of some ‘legals’ that are deemed representative of IoT-typical contractual practices.

With this in mind, this chapter will answer the following subquestion: *can IP and antitrust counter the death of ownership?*

6.2 An Overview of the IP Issues and Themes in the IoT

A review of the relevant literature and case law identifies the following themes and issues at the intersection of IP and IoT:

- (i) Death of ownership and digital serfdom;
- (ii) Antitrust control over standard essential patent (SEP) licensing to achieve a standardised and interoperable IoT;
- (iii) The ‘Internet of Secrets’;
- (iv) Patentability of IoT inventions;
- (v) The ‘Internet of Digital Locks’;
- (vi) Data ownership;
- (vii) Smartness and distinctiveness;
- (viii) Overcoming Western-centrism; and
- (ix) Commons for an open IoT.

Points i and ii will be the main focus of this chapter and therefore will be expanded upon in the next sections; point iii refers to the legal, technical, and organisational secrecy that we have analysed in the previous chapter.

15 Fairfield (n 14).

16 Chris Jay Hoofnagle, Aniket Kesari and Aaron Perzanowski, ‘The Tethered Economy’ (2019) 87 *George Washington Law Review* 783.

17 Fairfield (n 14).

Patentability of IoT inventions. The IoT challenges the identification of the subject pattern that is excluded from patentability (hereinafter also ‘excluded subject matter’).¹⁸ The European Patent Convention excludes software as such from patentability.¹⁹ As shown in the *travaux préparatoires* to the Convention, the rationale of the exclusion is that ‘patent protection is reserved for creations in the technical field’²⁰ and that software is already protected by copyright. The exclusion of software only ‘as such’ means that the latter is patentable if it has a technical character, that is, if it produces a further technical effect when run on a computer or other Thing.²¹ *HTC v Apple*²² provides some useful signposts to understand what this technical effect is: (a) whether the claimed technical effect has a technical effect on a process which is carried on outside the computer; (b) whether it operates at the level of the architecture of the computer; (c) whether it results in the computer operating in a new way; (d) whether it makes the computer run more efficiently or effectively; or (e) whether the perceived problem is overcome by the invention rather than merely circumvented. A common way to circumvent the software exclusion is to frame the invention as a computer-implemented invention. This is seen as distinct from a computer program because it refers to ‘computers, computer networks or other programmable apparatus wherein at least one feature is realised by means of a computer program.’²³ Unlike software inventions, they cannot be objected ‘as any method involving the use of technical means (e.g. a computer) and any technical means itself (e.g. a computer or a computer-readable storage medium) have technical character.’²⁴ By issuing guidance on computer-implemented inventions and examples of ‘further technical effect,’ the European Patent Office has made it easier to apply for software patents, including IoT patents.²⁵ Moreover, a competent draftsman ‘can usually present a claim as a computer-implemented method . . . rather than as a “computer program.”’²⁶ Even before the IoT, the exclusion of software ‘as such’ from patentability had done little to slow down the monopolisation of software innovation. The situation risks worsening with the IoT. Indeed, the European Patent Convention’s exclusion is based on the hardware-software dichotomy, but as argued in this book, the IoT disrupted this dichotomy. The same applies to the North-American exclusion of

18 Patent issues that I will not deal with include joint infringement, connected to the interactive nature of the IoT, and patent quality. On them, see W Keith Robinson, ‘Patent Law Challenges for the Internet of Things’ (2015) 15 *Wake Forest Intellectual Property Law Journal*.

19 Art 52(2)(c) and 52(3).

20 Administrative Council, ‘Basic Proposal for the Revision of the EPC (MR/2/00)’ (2000) 43. For the debate around the reform of this exclusion, see President of the European Patent Office, ‘Revision of EPC: Article 52(1)-(3)’ (1999) CA/PL 6/99.

21 European Patent Office, *Guidelines for Examination* (EPO 2019) [G, II, 3.6].

22 *HTC Europe v Apple* [2013] EWCA Civ 451.

23 European Patent Office (n 22) [G, II, 3.6].

24 *ibid.*

25 See Yahong Li, ‘The Current Dilemma and Future of Software Patenting’ (2019) 50 *IIC* 823.

26 Mateo Abov and others, ‘How Does Emerging Patent Case Law in the US and Europe Affect Precision Medicine?’ (2019) 37 *Nature Biotechnology* 1118.

abstract ideas,²⁷ whose historical rationale is that patents were intended to cover devices and things.²⁸ Although the inclusion of a Thing in a software claim does not necessarily make it admissible, and even though software claims may still fail for lack of inventive step,²⁹ there is the undeniable risk that the overcoming of the hardware-software dichotomy will lead to the factual overcoming of the software exclusion.³⁰ When all software becomes embedded in a Thing – in other words, when no software is purely software, software ‘as such’ – we must be alert and prevent IoT companies from monopolising software innovation at the expenses of smaller businesses, consumers, and society at large. An ambitious solution could be a software treaty that would provide for a limited scope and length of software protection, ‘allowing only the means of implementation but not the function to be patented; and granting 10 years of utility-model-type or sui generis protection.’³¹ Or even, perhaps more radically, to exclude all software inventions from patentability – removing the ‘as such’ proviso – and to rely exclusively on the copyright protection of software.³² Indeed, although the duration of copyright is excessive for a rapid market such as the software one, I would argue that pure copyright protection would instantiate a more balanced approach to the legal protection of software as, unlike patents, copyright is not a monopoly right which allows for independent creations and thus encourages follow-on innovation.

The Internet of Digital Locks. Technological protection measures and digital rights management (DRM),³³ exemplified by the digital locks that prevent gamers from running counterfeit games on their consoles, are problematic for at least three reasons. First, they leave it to the IP owner to decide whether a use is permitted by one of the exceptions, with no or limited possibility for the user to argue otherwise. This goes hand in hand with the de facto privatization of internet governance – and ultimately of justice – that is a recent trend in digital regulation.³⁴ For example, under the Copyright

27 The leading cases are *Alice v CLS*, 573 U.S. 208 (2014) and *Mayo v Prometheus*, 566 U.S. 66 (2012).

28 Miriam Bitton, ‘Patenting Abstractions’ (2014) 15 NCJL & Tech 153, 162.

29 Indeed, features that fall within Art. 52(2) categories (e.g. software) ‘can contribute to the assessment of non-obviousness only if they contribute to the technical character’ (Aboy and others (n 27) 1124).

30 This was my main thesis in Guido Noto La Diega, ‘Software Patents and the Internet of Things in Europe, the United States and India’ (2017) 39 EIPR 173.

31 Li (n 26) 823.

32 ‘Member States shall protect computer programs, by copyright, as literary works’ (Software Directive, art 1(1)). The TRIPS Agreement is often referred to as the legal basis of the alleged obligation for contracting states to protect software patents as it provides that ‘patents shall be available for any inventions . . . in all fields of technology’ (art 27). However, software is a type of technology, not a field and software patentability under TRIPS ‘remains an open question’ (Robert Tomkiewicz, *Intellectual Property Overlaps: Theory, Strategies and Solutions* (Routledge 2012) 45).

33 Infosoc Directive, art 6; DMCA, s 1201.

34 Alongside the provision at hand, one need only think of the proposed Digital Services Act that provides a mixed public-private system of oversight and enforcement where platforms and users themselves are called to an active role in policing compliance and handling complaints (arts 6, 8, 17, and 19).

in the Digital Single Market Directive,³⁵ online content-sharing providers have to prevent the sharing of infringing material (so-called upload filter). In doing so, they have to ‘put in place an effective and expeditious complaint and redress mechanism.’³⁶ Thus, not only it is up to the IoT company to deploy technological locks and filters to pre-empt ex ante potentially infringing behaviour, but they are also judges in the disputes arising therefrom. This is likely to lead to a further compression of the user freedoms enshrined in IP exceptions and limitations. This can be inferred by the fact that this directive openly provided that ‘Member States shall ensure that users have access to a court or another relevant judicial authority to assert the use of an exception or limitation to copyright and related rights.’³⁷ Traditional judicial process is better positioned to account for the conflicting interests at play and understand whether the digital lock regarded as infringing activities that would fall within the scope of IP exceptions and limitations. However, in a fast-paced, opaque, and asymmetrical environment such as the IoT, it is unlikely that end users will resort to legal action to open the digital locks. This is regrettable as IP exceptions and limitations are pivotal to achieving a fair balance between the rightsholders’ and the users’ interest. As the US Supreme Court put it, copyright ‘protection has never accorded the copyright owner complete control over all possible uses of (the) work.’³⁸ Conversely, DRM may accord complete control. Second, digital locks delegate to automated or partly automated systems complex assessments that do not lend themselves to being translated into code – e.g. how is one to translate the concepts of ‘fairness’ and ‘substantiality’?³⁹ Third, the circumvention of DRM measures is unlawful even when there is no proof of underlying copyright infringement.⁴⁰ In this sense, DRM gives rise to forms of over-protective ‘paracopyright’⁴¹ and runs counter to fundamental use freedoms, including freedom of expression. With the IoT, copyright works such as software and databases become embedded in virtually any object that surrounds us; with multimedia products becoming commonplace and with every layer of a Thing being locked, ‘the effect of DRM systems in economic and social processes may be pervasive.’⁴² There is little, if

35 C-DSM Directive, art 17.

36 C-DSM Directive, art 17(9).

37 C-DSM Directive, art 17(9).

38 *Sony v Universal Studios*, 464 U.S. 417, 432 (1984).

39 Léo Pascault and others, ‘Copyright and Remote Teaching in the Time of Covid-19: A Study of Contractual Terms and Conditions of Selected Online Services’ (2020) 42 EIPR 548. cf Niva Elkin-Koren, ‘Fair Use by Design’ (2017) 64 UCLA Law Review 22.

40 The DMCA, and arguably the Infosoc Directive, forbid ‘these circumventions regardless of the purpose of the circumvention’ (Lawrence Lessig, *Code* (Version 2.0, Basic Books 2006) 186.) Whilst circumventing a DRM system does not involve copyright infringement, it is less clear whether the circumventions need to have some relationship to copyright infringement.

41 Guido Westkamp, ‘Code, Copying, Competition: The Subversive Force of Para-Copyright and the Need for an Unfair Competition Based Reassessment of DRM Laws after Infopaq’ (2010) 58 Journal of the Copyright Society of the USA 665.

42 Michèle Finck and Valentina Moscon, ‘Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0’ (2019) 50 IIC 77.

any,⁴³ recourse against IoT companies that implement DRM systems to prevent ‘users and the government from ever finding out what data is collected and how it is used by device manufacturers.’⁴⁴ As the Internet of Digital Locks rises, the postsale control over our Things throughout their life cycle is a threat not only to our property but also to our autonomy.

Data ownership. Trade secrets do not, strictly speaking, instantiate a property right: they implement a tort law approach that outlaws certain specific uses of the confidential information.⁴⁵ Therefore, they have been seen as suitable to protect firms in the data economy whilst balancing the potentially conflicting interests in data protection and in the free flow of information.⁴⁶ Their widespread use to protect IoT data, coupled with factual control over data, supported by DRM-like measures, corroborates the thesis that the case for a new property right on the data as such has not been convincingly made.⁴⁷ Such a proposal – dubbed ‘data producer’s right’ – is contained in the European Commission’s Free Flow of Data initiative.⁴⁸ On the debatable assumption that the Database Directive’s sui generis right⁴⁹ would not be fit for machine-generated data and that new incentives are needed for the data economy to thrive,⁵⁰ the Commission proposed a data ownership right, that is, a ‘right to use and authorise the use of nonpersonal data’⁵¹ granted to the data producer, that is, ‘the owner or long-term user (i.e. the lessee) of the device.’⁵² Thus, users would ‘utilise their data and thereby contribute to unlocking machine-generated data.’⁵³ However, law and economics studies have abundantly proved that big data is generated despite the absence of proprietary incentives.⁵⁴ Moreover, the unfitness of the sui generis right for IoT data can be called into question.⁵⁵ More on this will be said later in the chapter, when dealing with the exceptions to the sui generis right. For the purposes of this

43 As seen in the previous chapter, data protection laws can prevail on IP, with limited exceptions regarding the rights to access and portability.

44 Lidiya Mishchenko, ‘The Internet of Things: Where Privacy and Copyright Collide’ (2016) 33 Santa Clara High Technology Law Journal 90, 90.

45 cf Mark A Lemley, ‘The Surprising Virtues of Treating Trade Secrets as IP Rights’ (2008) 61 Stanford Law Review 311.

46 Josef Drexl, ‘Designing Competitive Markets for Industrial Data. Between Propertisation and Access’ (2017) 8 JIPITEC 257 [183].

47 *ibid.*

48 European Commission, ‘SWD on the Free Flow of Data And Emerging Issues of the European Data Economy’ (2017) COM(2017) 9 final.

49 Directive 96/9/EC of 11 March 1996 on the legal protection of databases [1996] OJ L 77/20, arts 7 ff.

50 A majority of studies tend to agree on this. See Andrea Ottolia, *Big Data e Innovazione Computazionale* (Giappichelli 2017).

51 European Commission, ‘SWD on the Free Flow of Data and Emerging Issues of the European Data Economy’ (n 50) 13.

52 *ibid.*

53 *ibid.*

54 ‘[N]o incentives are needed for generating and commercialising data’ (Drexl (n 47) [183]).

55 Guido Noto La Diega, ‘Artificial Intelligence and Databases in the Age of Big Machine Data’ (2019) 25 AIDA 2018 93.

section, suffice it to say that this right provides some protection to IoT data. With this in mind – and considering the protection already afforded by trade secrets, factual control, and DRM – one can hardly say that the production of data needs further incentives. This said, we are still far from reaching a consensus on critical questions, such as whether and how IoT data can be (and should be) the subject of property, how trade secrets and sui generis right interact in governing IoT data, and whether ownership should rest with the owner of the Thing, its user, its manufacturer, or the manufacturer of the relevant sensor.⁵⁶ It seems, however, that scholars and policymakers are shifting their focus from issues of ownership to questions of access – which in the IoT are closely connected to interoperability. Pragmatically, it would appear more useful to take account of the fact that IoT companies already treat data like property, regardless of their formal qualification. Accordingly, we should endeavour and find ways to govern access to IoT data flows in a transparent, fair, and balanced way.⁵⁷

Smartness and distinctiveness. The only EU ruling that expressly deals with the IoT is the trademark case *Bosch v EUIPO*.⁵⁸ In recent years, Bosch has been making investments to become an IoT leader. This effort resulted in Bosch IoT Suite, an open-source-based platform for IoT solutions with over ten million sensors, devices, and machines connected to it.⁵⁹ Bosch launched its ‘*Simply. Connected.*’ series of ‘smart’ tools that can be controlled via a mobile app – and attempted to register the relevant logo as an EU trademark (Figure 6.1)

For the purposes of this book, it is sufficient to focus on two aspects of the case. The application regarded a wide range of goods and services, from sensors through sanitary devices to products that were either directly connected



Figure 6.1 Figurative mark at issue in *Bosch v EUIPO*.

56 See e.g. Stacy-Ann Elvy, ‘Commodifying Consumer Data in the Era of the Internet of Things’ (2018) 59 *Boston College Law Review* 423; Mehmet Bilal Ünver, ‘Turning the Crossroad for a Connected World: Reshaping the European Prospect for the Internet of Things’ (2018) 26 *International Journal of Law and Information Technology* 93.

57 See e.g. Martina Barbero and others, *Study on Emerging Issues of Data Ownership, Interoperability, (Re-)Usability and Access to Data, and Liability* (European Commission 2018); Thomas J Farkas, ‘Data Created by the Internet of Things: The New Gold without Ownership?’ [2017] *Revista La Propiedad Inmaterial* 5.

58 Cases T-251/17 and T-252/17 *Bosch v EUIPO* (CJEU, 28 March 2019).

59 ‘Bosch IoT Suite’ <www.bosch-iot-suite.com/>.

to a network or embedded into connected objects.⁶⁰ EUIPO's Board of Appeal rejected the application as the sign was deemed devoid of any distinctive character. Indeed, the words 'simply connected' were seen as a mere slogan meaning 'just connected,' and the figurative elements were considered customary and nondistinctive. The Board, in particular, referred to the concept of IoT, which they defined as 'the interconnection of physical objects in a network comparable to the Internet, so as to allow them to be controlled at a distance or to make them capable of communicating and exchanging information.'⁶¹ In light of this, 'simply connected' meant 'just connected to a network' or 'above all connected to a network'; as such, it was to be regarded as '*desirable characteristic*'⁶² and a '*laudatory indication*'⁶³ for Things, as such nondistinctive. Therefore, IoT companies attempting to register connectivity-related signs should be aware that their signs may be regarded as descriptive and devoid of distinctiveness.

A second aspect that is of relevance from this book's perspective has to do with the examiners' discretion when it comes to considering signs that are applied to a diverse range of IoT products. Bosch attempted to demonstrate that, even if the relevant public would understand 'Simply.Connected.' as just connected to a network, this would be meaningless in relation to the majority of the products to which the sign referred. In particular, whereas consumers know that laptops, mobile phones, tablets, and earphones can be connected to the internet – and therefore the sign may be descriptive with regard to these products – they would not be aware that other, everyday objects or their components (e.g. antennas for radios and television receivers, batteries, etc.) can be connected to a network.⁶⁴ Moreover, the defence went on arguing that a number of services (e.g. training and instruction services) were not limited to connectivity. In principle, when assessing distinctiveness, examiners should look at each good and service separately. Conversely, the Board of Appeal assessed jointly products that were *prima facie* diverse – this was at the core of Bosch's appeal. However, the CJEU confirmed that examiners do have the power to use the same general reasoning for a group of products if 'goods and services . . . are interlinked in a sufficiently direct and specific way, to the point where they form a *sufficiently homogenous category*.'⁶⁵ The concept of IoT provided this homogenizing factor. Indeed, the court stated that:

In view of the development of the Internet of Things, the Board of Appeal was correct to state that the relevant public would see the signs at issue as

60 *Bosch* (n 59) [4], [81].

61 *ibid* [43].

62 *ibid*.

63 *ibid* [45].

64 *ibid* [71], [72].

65 *ibid* [50]. Italics added.

indicating the ability of the goods at issue to be connected and would perceive the services at issue as relating to such connections.⁶⁶

Therefore, the existence and pervasiveness of the IoT makes the examiners' work easier as they can assess jointly all the 'smart' goods and services, and it renders connectivity-related signs nondistinctive well beyond the realm of traditionally connected objects to encompass all Things.

Overcoming Western-centrism. Reflecting a road-to-Damascus moment in legal scholarship, it has occurred to some authors that Western-centric IP studies do not reflect the socio-economic, cultural, and legal importance of Eastern and Southern countries (the 'global South').⁶⁷ This is particularly the case with China. Once an imitator, China has for some time taken on the role of innovator.⁶⁸ The country has an established manufacturing industry, and many IoT start-ups rely on it. Much of the value of these start-ups is in their IP; nonetheless, they do not properly assess the IP risks and opportunities of having their Things manufactured in China. Some scholars have been studying ways in which IP law can be leveraged to strengthen the position of foreign IoT start-ups in China.⁶⁹ The Chinese information economy is now as important as its manufacturing; this is evidenced by its being a top IP holder and by the gradual strengthening of its IP laws.⁷⁰ This can be seen in the latest statistics of the European Patent Office, where China is the fastest-growing patent applicant in the world (+9.9%).⁷¹ In light of the growth of China-based IoT and of the modernisation of its laws on innovation, IP scholars and practitioners should avoid their Western-centric habits. China is no longer a mere rule-taker in global lawmaking,⁷² including in the field of internet regulation and IT law. The awareness of China's rulemaking power should permeate contemporary legal scholarship. In turn, consumers should be aware that at least some components of their Things are provided by China-based companies, which can leverage their national IP laws to control the Thing's software, hardware, service, and data, thus affecting the Thing as a whole.

Commons for an open IoT. While IP excesses tend to create a closed and noninteroperable IoT, there are many attempts to open the IoT to make it more socially just and user-centric. Some of these attempts revolve around the concept of 'commons.' Information is a common and a public good because it is difficult 'to exclude people from knowledge once someone had made a discovery. One person's use of knowledge . . . does not subtract from another person's capacity to use

66 *ibid* [80].

67 Yun Zhao and Michael HK Ng, *Chinese Legal Reform and the Global Legal Order Adoption and Adaptation* (CUP 2018).

68 Jingxi Ding and others, 'From Imitation to Innovation: A Study of China's Drug R&D and Relevant National Policies' (2011) 6 *Journal of Technology Management & Innovation* 1.

69 Carr and Harris (n 68).

70 Li (n 68).

71 'Patent Index 2020' (*European Patent Office*, 2021) <www.epo.org/about-us/annual-reports-statistics/statistics.html#patentees>.

72 Peter K Yu, 'The Middle Kingdom and the Intellectual Property World' (2011) 13 *Oregon Review of International Law* 209.

it.⁷³ Information is a nonrivalrous and nonexclusionary good. The status of data as a commons *extra commercium* has been recently convincingly argued.⁷⁴ New technologies, including the IoT, make the commons more vulnerable due to their 'ability to capture the previously uncapturable.'⁷⁵ In the field of software, the commons increasingly take the form of free and open-source licenses.⁷⁶ Some studies focused on the importance of free and open-source software (FOSS) and hardware to ensure a fully-functioning, inclusive, and interoperable IoT.⁷⁷ IoT software is increasingly developed under open-source innovation models and combined with proprietary ones, giving rise to hybrid business models. IoT commons are instantiated amongst other things by open patent strategies, such as patent pools and patent pledges.⁷⁸ Around the knowledge commons, including open software and hardware, forms of antiproprietary collective resistance can develop.⁷⁹ In the next chapter, I will expand on how the commons can provide a solution to many of the problems of the IoT in two senses: on the one hand, as a practice of collective resistance to new extractive practices; on the other hand, as the foundation for free and open-source software, hardware, standards, data, and platforms.

Current IP scholarship tends to focus on the practical question of how to govern the IoT as in how to protect its components and the related inventions. However, I felt it was more urgent to explore whether IP laws can be leveraged to re-empower IoT users who, increasingly affected by the death of ownership, struggle to cope with their diminished status as digital tenants. This chapter aims to fill this gap.

6.3 Death of Ownership: To Strengthen Property Rights and Empower IoT Users-Digital Peasants or to Counter Bourgeois Property?

By selling consumers hardware while retaining ownership of software, service, digital content, and data, IoT companies 'are treating users like digital tenants.'⁸⁰

73 Charlotte Hess and Elinor Ostrom, 'Introduction: An Overview of the Knowledge Commons' in Charlotte Hess and Elinor Ostrom (eds), *Understanding Knowledge as a Commons. From Theory to Practice* (MIT Press 2007).

74 Chiara Angiolini, *Lo statuto dei dati personali: uno studio a partire dalla nozione di bene* (Giapichelli 2020).

75 Hess and Ostrom (n 74) 10.

76 Shubha Ghosh, 'How to Build a Commons: Is Intellectual Property Constrictive, Facilitating, or Irrelevant?' in Charlotte Hess and Elinor Ostrom (eds), *Understanding Knowledge as a Commons: From Theory to Practice* (MIT Press 2007).

77 Ovidiu Vermesan and Peter Friess (eds), *Building the Hyperconnected Society* (River 2016).

78 Mariateresa Maggolino and Maria Lilla Montagnani, 'From Open Source Software to Open Patenting – What's New in the Real of Openness?' (2011) 42 IIC 804; Natacha Estèves, 'Open Models for Patents: Giving Patents a New Lease on Life?' (2018) 21 The Journal of World Intellectual Property 2.

79 Peter Levine, 'Collective Action, Civic Engagement, and Knowledge Commons' in Charlotte Hess and Elinor Ostrom (eds), *Understanding Knowledge as a Commons* (MIT Press 2007).

80 Jathan Sadowski, 'Landlord 2.0' (*OneZero*, 4 April 2019) <<https://onezero.medium.com/landlord-2-0-techs-new-rentier-capitalism-a0bfe491b463>>.

These companies are the new prophets of 'rentier capitalism' as they are monopolising access to property (including IP) to extract value from users often without providing any actual service, let alone innovating or contributing to society.⁸¹ Being demoted to tenants of one's own Things has practical consequences. E.g. in the UK there is an implied term that the purchaser of a good, as opposed to its tenant, will enjoy its quiet possession.⁸² This means that a trader who transfers ownership over a good promises the owner that the possession and use will be uninterrupted.⁸³ Owners can avail themselves of this implied term when the trader transfers IPRs on the Thing to third parties⁸⁴ as well as to counter the deletion of software that makes the Thing inoperable.⁸⁵ Conversely, digital tenants cannot invoke such legal protections.

The concept of 'death of ownership' originated in the 'new servitudes'⁸⁶ that Molly Shaffer Van Houweling described in her study on the usage restrictions that courts recognise on software-embedded goods. The 'death of ownership' transforms end users into digital tenants in a twofold way. First, IoT traders may retain ownership of the Thing as such. This trend sees the shift from the contract of sale to a mere subscription: in the tethered economy,⁸⁷ we have a right to access the 'device-as-a-service'⁸⁸ as opposed to outright owning it. Cost saving is not the only justification for this phenomenon. IoT users may lease the Thing under the condition that, at the end of the life cycle, the Thing be returned to them for them to dispose of it responsibly. Perhaps surprisingly, the 'green' imperatives of the circular economy could contribute to the death of ownership.⁸⁹ Second – and this is the focus of this section – the death of ownership can be caused by IoT companies retaining control over the Thing by factual, legal (IPRs and contracts), and technological means. IoT users remain owners, though only formally, as they cannot exercise the powers that are traditionally associated to property. These two forms of death of ownership are not mutually exclusive. For example, in June 2021 owners of smart treadmill Tread+, which retails for thousands of dollars, were notified that if they wanted to keep having access to the smart functionalities of the product, they had to pay a monthly

81 Guy Standing, *Corruption of Capitalism* (Biteback 2016); Carlo Vercellone, 'Il Ritorno Del Rentier. Salario, Rendita, Profitto Nel Capitalismo Cognitivo' (2006) *Autunno Posse* 97.

82 CRA, s 17(2)(c).

83 Christopher Millard, W Kuan Hon and Jatinder Singh, 'Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities' [2017] *IC2E* 286.

84 *Microbeads v Vinhurst* [1975] 1 *WLR* 218.

85 *Cox v Riley* (1986) 83 *Cr App Rep* 54, [1986] *Crim LR* 460.

86 Molly Shaffer Van Houweling, 'The New Servitudes' (2007) 96 *Georgetown Law Journal* 885.

87 Hoofnagle, Kesari and Perzanowski (n 17).

88 See e.g. the subscription plans offered by Microsoft to lease devices certified for Teams meetings. 'What's New in Microsoft Teams' (*Microsoft TechCommunity*, 2 March 2021) <<https://techcommunity.microsoft.com/t5/microsoft-teams-blog/what-s-new-in-microsoft-teams-microsoft-ignite-2021/ba-p/2118226>>.

89 Sean Thomas, 'Law, Smart Technology, and Circular Economy: All Watched Over by Machines of Loving Grace?' (2018) 10 *Law, Innovation and Technology* 230.

subscription fee.⁹⁰ Nonetheless, the focus of this chapter is on the second type of death in its pure form, while the issues of the subscription economy will be the subject of future research.

IoT companies factually, technologically, and legally control the Thing – and ultimately its users – by controlling virtually each of its components and layers.

Factual control regards mostly data and services: they do not lend themselves to being appropriated through IPRs but are de facto subject to the jurisdiction of the IoT overlord. The latter can factually prevent access to one's own data and roll back services at its discretion. A telling illustration of factual control was provided in the previous chapter, where I showed that although in theory we have a right to access our data under the GDPR, Amazon does not grant meaningful access to the data subject's profile, including the inferences that the company makes about one's preferences, biases, and vulnerabilities.

IoT companies also retain technological control over the Thing. This is exemplified by the aforementioned issue of the 'Internet of Digital Locks.' A group of farmers was surprised to find out that they did not have a right to repair their own tractors, purchased from John Deere, a heavy equipment manufacturer. The service could only be provided by John Deere-approved technicians.⁹¹ John Deere argued to the Copyright Office that because the tractor was equipped with software and the copyright on the software was merely licensed to the farmer, it was within the manufacturer's powers to prevent farmers from modifying or even repairing their own equipment.⁹² Any independent repair would have qualified as an illegal DRM circumvention. This led to widespread criticism and some emphatic calls not to let IoT companies 'eviscerate the notion of ownership.'⁹³ As such, the evisceration of ownership does not necessarily harm IoT users; the loss of control does.

'Legal control' refers to a combination of contracts and IPRs. As seen in Chapter 2, the user of as simple a Thing as a speaker would hardly expect to be confronted with a mountain of hundreds of terms of service, privacy policy, warranties, etc. These 'legals' are often used to affect those exclusive rights that are quintessential to the property right, at least in its traditional, i.e. tangible, form.⁹⁴

90 Ax Sharma, 'Peloton's \$3,000 Treadmill Now Comes with Surprise "Subscription Fee"' (*Bleeping-Computer*, 22 June 2021) <www.bleepingcomputer.com/news/technology/pelotons-3-000-treadmill-now-comes-with-surprise-subscription-fee/>.

91 Kit Walsh, 'John Deere Really Doesn't Want You to Own That Tractor' (*Electronic Frontier Foundation*, 20 December 2016) <www.eff.org/deeplinks/2016/12/john-deere-really-doesnt-want-you-own-tractor>.

92 Laura Sydell, 'DIY Tractor Repair Runs Afoul Of Copyright Law' (*NPR.org*, 17 August 2015) <www.npr.org/sections/alltechconsidered/2015/08/17/432601480/diy-tractor-repair-runs-afoul-of-copyright-law>.

93 Kyle Wiens, 'We Can't Let John Deere Destroy the Very Idea of Ownership' (*Wired*, 21 April 2015) <www.wired.com/2015/04/dmca-ownership-john-deere>.

94 This exacerbates a phenomenon that was already taking place previously, e.g. in the field of cloud contracting. See Guido Noto La Diega, 'Il Cloud Computing. Alla Ricerca Del Diritto Perduto Nel Web 3.0' (2014) 2 *Europa e diritto privato* 577.

The analysis of Echo's contractual quagmire also shed light on how a number of IPRs protect Amazon's speaker. Echo is protected by 84 patents and 427 trademarks that monopolise virtually any aspect of the Thing.⁹⁵ On top of this, IoT companies can leverage a rich portfolio of unregistered and registered IPRs from trade secrets through copyright to database rights. A perspicuous illustration of the death of ownership caused by the incorporation of numerous IP works in all 'our' Things is provided by the recent *Tom Kabinet* case,⁹⁶ which dealt with the legality of a virtual market for second-hand e-books. The resale of IP-protected products without the rightsholder's permission is allowed by the principle of exhaustion. This principle applies to all IPRs,⁹⁷ and it provides that, once an IP-protected product has been lawfully put on the market within the European Economic Area by the rightsholder or with their consent, the rights conferred by that IPR in relation to the commercial exploitation of the good become exhausted.⁹⁸ This means that, once exhaustion occurs, the rightsholder can no longer invoke the IPR in question to prevent the further resale (including parallel imports), rental, lending, or other forms of commercial exploitation of the product by third parties.⁹⁹ In the EU, exhaustion can be regarded as a limitation on IP imposed by the fundamental freedom of movement of goods.¹⁰⁰ The right to distribution – the right to issue copies of the work to the public, i.e. to put the work into circulation – is one of the copyright owner's exclusive rights to which exhaustion applies.¹⁰¹ Conversely, the right to communication to the public – that is, the right to make the works available to the public in such a way that the public may access them from a place and at a time individually chosen by them – is not subject to exhaustion. The key question in *Tom Kabinet* was whether the supply by downloading, for permanent use, of an e-book was covered by the concept of 'communication to the public' or by that of 'distribution to the public.' In the former event, the IP holder could prevent the resale of the e-book; in the latter, the resale would be lawful as exhaustion applied. As stated by the CJEU in *UsedSoft*,¹⁰² the right to distribution of a computer program is subject to exhaustion regardless of whether it is incorporated in

95 I sourced the data from WIPO's Patentscope and Global Brand Database on 1 June 2021.

96 Case C-263/18 *Nederlands Uitgeversverbond v Tom Kabinet* [2020] Bus LR 983.

97 Infosoc Directive, art 4(2), and other references in Guido Noto La Diega, 'Can the Law Fix the Problems of Fashion? An Empirical Study on Social Norms and Power Imbalance in the Fashion Industry' (2019) 14 *JIPPL* 18.

98 See Irene Calboli and Edward Lee (eds), *Research Handbook on Intellectual Property Exhaustion and Parallel Imports* (Edward Elgar 2016).

99 IPO and Government Digital Service, 'Exhaustion of IP Rights and Parallel Trade from 1 January 2021' (2020) Guidance <www.gov.uk/guidance/exhaustion-of-ip-rights-and-parallel-trade-after-the-transition-period>.

100 Guido Westkamp, 'Intellectual Property, Competition Rules, and the Emerging Internal Market: Some Thoughts on the European Exhaustion Doctrine' (2007) 11 *Marquette Intellectual Property Law Review* 291.

101 Berdien BE van der Donk, 'CJEU Rules the Right to Distribution Only Applies to Tangible Digital Works – UsedSoft Doctrine of Exhaustion Does Not Apply to e-Books CJEU C-263/18 (*Tom Kabinet*)' (2020) 42(8) *EIPR* 516, 517.

102 Case C-128/11 *UsedSoft v Oracle* [2012] 3 *CMLR*. 44.

a tangible medium. Accordingly, lawfully downloaded software may be resold.¹⁰³ In *Tom Kabinet*, the CJEU considerably narrowed the scope of the *UsedSoft* doctrine by arguing that:

- (i) The right to distribution of computer programs is indeed subject to exhaustion regardless of the existence of a tangible medium. However, the concept of 'computer program' does not include e-books, which can be regarded as digital copyright products governed by the Infosoc Directive as opposed to the Software Directive.¹⁰⁴
- (ii) Unlike the Software Directive, the Infosoc Directive would rely on the tangible-intangible divide; therefore, tangible items distributed by tangible means are covered by the right to distribution and can be resold without the rights-holder's permission under the principle of exhaustion. Conversely, intangible copyright products such as e-books are not distributed; they are communicated to the public, and since this right is not subject to exhaustion, the resale of used e-books requires the copyright holder's permission.¹⁰⁵

This decision is open to a twofold criticism. First, the growth of IoT and converged devices has led to an erosion of the distinction between software and digital products. Arguably, an e-book – similar to the digital content and the service embedded in a Thing (e.g. e-sport played on a 'smart' console) – falls within the commonly accepted definition of software, that is, a collection of instructions that can be executed by a computer to perform a specific task.¹⁰⁶ With *Tom Kabinet*, it is unclear when a set of instruction leaves the realm of computer programs and enters that of digital product. Second, perhaps more importantly, given the amalgam of hardware, software, service, and data in the IoT, the *Tom Kabinet* doctrine risks leading to an 'exhaustion of exhaustion.' Things are sold intact with software preinstalled and not removable or changeable under the license agreement – software is not bundled separately anymore. To predicate that the exhaustion of IPRs depends on the tangible-intangible divide may reflect the wording of the Infosoc Directive and, in particular, of Recital 28, whereby '(c)opyright protection under this Directive includes the exclusive right to control distribution of the work incorporated in a tangible article.' However, it is an outdated approach that is at odds with the smart reality we live in. Such binary doctrine may be exploited by IoT companies that own the IPRs on the intangible components of the Thing to prevent further resale or other commercial exploitation despite the exhaustion of the right to distribution, ultimately breaching the fundamental freedom of movement of goods in the EU. This is in line with other attacks on the principle

103 This rule comes with two provisos: (i) the licence is for an unlimited period of time, and (ii) the acquirer has paid a fee that responds to the economic value of the copy of the work.

104 *Tom Kabinet* (n 97) [53]–[59].

105 *ibid* [42], [56].

106 See e.g. JB Dixit, *Fundamentals of Computer Programming and Information* (Firewall Media 2005) 59.

of exhaustion, as exemplified by *Coty v Akzente*.¹⁰⁷ In this case, a luxury brand was allowed to impose restrictive distribution agreements excluding third-party e-commerce platforms. De lege ferenda, two recommendations can be made. First, the Software Directive should be amended to expressly define computer programs in line with commonly accepted computer science ontologies, while providing that every time software is involved, this directive will prevail on general copyright rules. Second, in light of the right to communication to the public becoming ubiquitous (most recently in *VG Bild*¹⁰⁸ about ‘framing’), copyright law should be amended to provide that this right too – not just the right to distribution – be subject to exhaustion. Otherwise, as most Things include content that is communicated to the public, there is the risk of reducing the principle of exhaustion to irrelevance, thus sterilising a limitation to IP that would otherwise be pivotal to ensuring the free movement of Things.

The combination of these factual, technological, and legal controls that the IoT company retains over the Thing results in the death of ownership. In turn, this manifests itself in decreased user power over the Thing, whilst the IoT company increases its power over the Thing, leading to its after-sale modification throughout its life cycle, and over user-generated content. I will analyse each manifestation in turn.

Decreased User Power Over the Thing. Linking back to Echo’s scenario, its legalists warn that ‘Service, Software and the Digital Content embody intellectual property that is protected by law.’¹⁰⁹ Virtually any aspect of Amazon’s apps and Things is covered by patents, trademarks, copyright, trade secrets, and other IPRs.¹¹⁰ Amazon’s control over Echo’s IP-embedding components prevents users from exercising their proprietary prerogatives. Under Alexa Terms of Use, e.g. users can utilise it only for personal and noncommercial purposes.¹¹¹ Under Amazon’s Conditions of Use and Sale, users can only share content via ‘their’ Thing to the limited extent that they ‘own or otherwise control all of the rights.’¹¹² This begs the question whether they can share contents by relying on IP exceptions or defences.¹¹³ The question is of crucial importance because Amazon can suspend and terminate those accounts that they deem to carry out infringing activities.¹¹⁴

107 Case C-230/16 *Coty Germany v Parfümerie Akzente* [2018] 4 CMLR 9.

108 Case C-392/19 *VG Bild-Kunst v Stiftung Preußischer Kulturbesitz* [2021] ECDR 9, criticised for its ‘dangerous extension of the right to communication to the public’ (Roberto Caso, ‘Diritto d’autore, Comunicazione al Pubblico e Misure Tecnologiche Di Protezione Contro Il Framing: VG Bild-Kunst e l’ultimo Cioccolatino Della Corte Di Giustizia’ (2021) 45 Trento Law and Technology Research Group Research Papers 1.).

109 Amazon Prime Video Terms of Use, last updated 27 May 2020, 6f.

110 Inter alia Amazon App Suite Legal Notices; Amazon App Legal Notice; Alexa Built-In Trademark Usage Guidelines; Works with Alexa – Trademark Usage Guidelines; etc.

111 Alexa Terms of Use, last updated on 31 January 2020, 1.2.

112 Conditions of Use & Sale, last updated on 29 January 2020, 8.

113 Similar problems, in the context of distance learning platforms, have been observed by Pascault and others (n 40).

114 Amazon Intellectual Property Policy.

Amazon's approach is clearly against allowing users to exercise their fundamental freedoms as conveyed by the copyright exceptions. This can be seen in the Additional Amazon Software Terms that prohibit to 'copy, modify, reverse engineer, decompile or disassemble, or otherwise tamper'¹¹⁵ with Echo's software. This provision is likely to qualify as 'null and void'¹¹⁶ under the Software Directive as it is contrary to the study and decompilation exceptions.¹¹⁷ More on the potential of IP exceptions to tackle the death of ownership will be said in the next section.

This cumulation of IPRs affects the degree of control that we have over the Thing as a whole and signals a shift from ownership to tenancy. Indicative of this shift are also those provisions whereby users do not own the digital content embedded in Echo: users have only a 'non-exclusive *right to view*'¹¹⁸ the content. Indeed, the latter is merely 'licensed, not sold, to you.'¹¹⁹ Amazon exercises a form of techno-legal power that is epitomised by its use of Microsoft PlayReady,TM a copy prevention technology embedded in software and hardware that allows control over the video content displayed on Amazon's Things.¹²⁰ Users remain owners of the Thing, but their right does not even resemble that absolute power over goods that is at the core of the traditional concept of property.

Increased Corporate Power Over the Thing. The death of ownership is not limited to the reduced power that users can exercise over 'their' Things. It is also connected to the IoT companies' increased contractual power that leads to the possibility to modify the Thing unilaterally throughout its life cycle. Users must be aware that their Thing may vary over time and possibly become radically different to what it was when they purchased it. This is evidenced by the fact that the services and the digital content provided through Echo may become unavailable over time and contain errors, without Amazon being liable for it.¹²¹ This can be seen with even more clarity in that contractual provision that allows Amazon to cease providing Echo's software and to terminate the user's right to use the software at any time: '[y]our rights to use the Amazon Software will automatically terminate without notice from us if you fail to comply with any of these Software Terms, the Conditions of Use or any other Service Terms.'¹²² The unavailability of the software makes the Thing as a whole unusable, including its hardware, service, digital content, and data components.

Increased Corporate Power Over User-Generated Content. Alongside decreased user power over the Thing – and, correspondingly, increased corporate power over it – the death of ownership manifests itself through IoT companies claiming control over the content generated by users via the Things. Users typically retain

115 Additional Amazon Software Terms, last updated on 29 January 2020, 3.

116 Software Directive, art 8.

117 Software Directive, arts 6 and 5(3).

118 Kindle Store Terms of Use, last updated on 22 May 2018, 1. Similar provisions apply to the video content under Amazon Prime Video Terms of Use, 4h.

119 Kindle Store Terms of Use, 1.

120 Third Party Software, last updated on 26 July 2019.

121 *ibid* 13; Amazon Prime Video Terms of Use, 4i and 6d.

122 Additional Amazon Software Terms, 1.

ownership over the contents they generate, but they effectively lose control over them by granting Amazon a worldwide sublicensable, royalty-free license over that content.¹²³ This can only partly be countered through the exercise of moral rights and image rights, but their protection is, in practice, weak and piecemeal.¹²⁴ The shift from ownership to control is a feature of contemporary IP that goes beyond the IoT. We have seen it occur in the context of the platformisation of education during the COVID-19 pandemic, when most universities adopted third-party proprietary platforms that de facto dispossessed teachers and students of their data.¹²⁵ The IoT brings the irrelevance of formal ownership to the physical world and renders it ubiquitous.

The power dynamics that underpin the death of ownership result in a fundamental shift in ‘the traditional conceptions of ownership’¹²⁶ that goes beyond Echo’s case study: it is a core characteristic of the IoT as a whole, as noted in a significant and comprehensive book on ownership in a ‘smart’ world: *Owned* by Joshua Fairfield.¹²⁷ Previous research had already underlined how the dematerialisation of traditional goods was leading to a shift in the concepts of ownership and property.¹²⁸ Conversely, less explored had been the opposite move, that is, when goods remain tangible but are embedded with software, service, and data. This is the gap filled by *Owned*, which shows that IP law has usurped a role traditionally delegated to property law when it comes to governing Things. Through IP-enabled postsale control over the Things – and ultimately over their ‘owners’ – IoT companies are responsible for a system that Fairfield sees as reminiscent of the feudal times, when people would only manage property subject to the ruler’s will. The feudal lord’s power was exemplified by the infamous *ius primae noctis*, the right to have sexual intercourse with his peasants’ brides on the night of the wedding. While there is no hard evidence that the *ius primae noctis* actually existed,¹²⁹ *Owned* refers to it as a powerful metaphor: ‘as the owner of the intellectual property embedded in the device, and as the drafter of clauses buried deep within its license agreement,’¹³⁰ IoT companies may be

123 Conditions of Use & Sale, 8.

124 See e.g. Huw Beverley-Smith, Ansgar Ohly and Agnes Lucas-Schloetter, *Privacy, Property and Personality: Civil Law Perspectives on Commercial Appropriation* (CUP 2005) esp 207.

125 Pascault and others (n 40).

126 Natasha Tusikov, ‘Precarious Ownership of the Internet of Things in the Age of Data’ in Blayne Haggart, Kathryn Henne and Natasha Tusikov (eds), *Information, Technology and Control in a Changing World* (Springer International Publishing 2019) 140. Tusikov’s main contention is that ‘companies that own the knowledge integral to the IoT’s functionality (the software) control that knowledge through intellectual property laws, especially copyright, and the ubiquitous surveillance of their customers.’

127 Fairfield (n 14).

128 M Scott Boone, ‘Ubiquitous Computing, Virtual Worlds, and the Displacement of Property Rights’ (2008) 4 ISJLP 91; Aaron Perzanowski and Jason M Schultz, *The End of Ownership: Personal Property in the Digital Economy* (The MIT Press 2016).

129 Jörg Wettlaufer, ‘The Jus Primae Noctis as a Male Power Display. A Review of Historic Sources with Evolutionary Interpretation’ (2000) 21 *Evolution and Human Behavior* 111.

130 Fairfield (n 14). No pinpointing is provided as this e-book’s pages are not numbered.

regarded as digital lords who blatantly invade the property and privacy of the users, who are demoted to digital peasants.

Fairfield goes as far as to claim that '[l]ike the serfs of feudal Europe who lacked rights in the land they worked, without digital property rights, we aren't owners – *we're owned*.'¹³¹ The solution to the death of ownership is found in the extension of the property rights that people have traditionally enjoyed over their things. Alongside the rights to modify, sell, use, and exclude – traditionally associated to 'ordinary' property – Fairfield claims that we should have the rights to hack, sell, run, and ban.¹³² To some extent, this has been already recognised by the Library of Congress's Copyright Office, which has introduced new exemptions to the Digital Millennium Copyright Act in order to recognise a right to hack one's own Thing without the fear of being liable for copyright infringement for the unauthorised use of the software embedded in the Thing.¹³³ These include exemptions to 'unlock' the Thing to connect it to alternative wireless networks and to 'jailbreak' it to make the Thing interoperable. It also includes more specific, IoT-friendly exemptions for purposes of diagnosis, repair, and lawful modification of motorised land vehicles.¹³⁴ Whilst stronger IP exceptions may play a role as part of a strategy to re-empower IoT users, they are not as such sufficient. More importantly, their revitalisation can be hindered by a strengthening of the property right over the Thing. IP exceptions are not grounded in the right to property: they reflect the public interest to ensure freedom of expression and information, as well as the right to self-determination. Extended property rights do not achieve much; they inherently foster the private interest, whose all-absorbing character in the IoT threatens the public and collective interests.

The parallel between IoT and feudalism, whilst a potent metaphor, does not fully account for the power dynamics at play in feudal times and today. In the current stage of capitalistic development, IoT companies leverage their IP and data power to impose their private interests on the end users' rights and freedoms – not only on their property, but also on their fundamental freedoms that is in the public interest to protect e.g. expression and information. Under medieval law, the lord could not wield property as a weapon: the power over the land depended on – and could be limited in view of – the collective interest, mainly to 'a more abundant and higher-quality agricultural harvest,'¹³⁵ which would ultimately bind both the lord and the peasants. As revolutionary Paul Lafargue put it, the feudal landlord 'has obligations and is *far from enjoying the liberty of the capitalist – the right to use and abuse*. The land is not marketable; it is burdened with conditions.'¹³⁶ In

131 *ibid.*

132 *ibid.*

133 US Copyright Office, Library of Congress, 'Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (83 FR 54010)' (26 October 2018).

134 *ibid.*

135 Paolo Grossi, *A History of European Law* (Laurence Hooper tr, Wiley-Blackwell 2010) 17.

136 Paul Lafargue, *The Evolution of Property from Savagery to Civilization (1890)* (New Park 1975) 48.

a sense, the public interest could be seen as able to limit private power, that is, the opposite to what appears to be happening under IoT capitalism.¹³⁷ Property, the private interest, and IP become the real protagonists of the market dynamics with the passage from feudal society to bourgeois society.¹³⁸ That was the moment when the ownership of goods started to be branded as ‘natural,’ as if it emanated from the ownership over oneself.¹³⁹ Thus, property became the most significant contributor to a person’s individuality, and the bourgeoisie, by accumulating ‘sacred’¹⁴⁰ property, reorientated society towards profit and accumulation of wealth. I would posit that the individualist outlook of bourgeois society – as opposed to medieval property – is the real precursor of the current state of things. The death of ownership is not the death of property: in the IoT, property thrives in the forms of IP, data power, contractual and technical control. Under their weight, citizens’ freedoms, their collective interests, and the public interest risk succumbing. Compared to this, the feudal communities, based on collective property and the feudal hierarchy where everyone ‘from the serf upwards to the king . . . were bound by the ties of reciprocal duties,’¹⁴¹ become a rather alluring prospect.

Even though the metaphor of digital serfdom has its drawbacks, it is possible to trace a parallel between feudalism and IoT economy. It has been noted that the ‘most distinctive feature of villein tenures was *labour rent*, i.e. the obligation to perform unpaid labour-service’¹⁴² on the manorial demesne. The demesne was the land that the lord retained for his own use and under his own management. From this viewpoint, an echo of this unpaid labour is present in the increasingly widespread practices of digital labour that see IoT users becoming unwitting workers. E.g. to extract value from images, companies need to annotate them, namely, they need to add tags that say, ‘This image contains a cat, a person, etc.’ In this way, image datasets can be used to train image-recognition AI models. However, manual annotation is slow and expensive. The solution Facebook came up with was to use user-generated hashtags as a proxy to human annotations for training purposes.¹⁴³ Thus, by ‘using a dataset comprised of 3.5 billion Instagram photos, Facebook was able to achieve an all-time record-high score of 85.4 percent on

137 This statement comes with the caveat that in medieval times, larger parts of society were marginalised, and therefore their interests would be unlikely to be subsumed under the public interest.

138 Grossi (n 136) esp 63.

139 James Tully, *A Discourse on Property: John Locke and His Adversaries* (Re-issued, Cambridge University Press 2006).

140 Declaration of the Rights of Man [1789], art 17.

141 Lafargue (n 137) 48.

142 Chris Middleton, ‘Peasants, Patriarchy, and the Feudal Mode of Production in England: A Marxist Appraisal: 1 Property and Patriarchal Relations within the Peasantry’ (1981) 29 *The Sociological Review* 105, 109.

143 Manohar Paluri and others, ‘Advancing State-of-the-Art Image Recognition with Deep Learning on Hashtags’ (*Facebook Engineering*, 2 May 2018) <<https://engineering.fb.com/ml-applications/advancing-state-of-the-art-image-recognition-with-deep-learning-on-hashtags/>>.

image recognition accuracy.¹⁴⁴ I would argue that this free labour that Instagram users provide resembles the unpaid labour provided by the peasant on the manorial demesne. As data is the main commodity in the IoT market and it is produced in large quantities by IoT users, the latter necessarily qualify as unwitting workers and should therefore be protected both in their individual and collective dimension.

Private property, by definition, will always be a means to protect the capitalist's private interest. Part of the capitalist strategy has been presenting IP as a form of nearly absolute property, as opposed to a policy bargain between the public and the rightsholders.¹⁴⁵ Against this backdrop, extending property rights is a dangerous path to take. By contrast, an answer may be found in the limitations to property. These can be intra-IP (exceptions), extra-IP (competition), and even extralegal limitations (the commons). The next sections will critically assess whether intra-IP limitation can be at the centre of a strategy to re-empower IoT users affected by the death of ownership.

6.4 Intra-IP Limitations: IP Exceptions or the Piecemeal Protection of Public Interest

Our Things being protected by a plurality of IPRs and embedding of a variety of IP works, combined with the strategic use of contractual, technical, and factual controls, leads to an imbalanced relationship between the IoT company/rightsholder and the end user. The death of ownership is the epitome of this imbalance. The principle of exhaustion is a key way IP law ensures a fair balance is achieved. However, we have seen that the principle is itself 'exhausted' in light of the *Tom Kabinet* doctrine with its outdated tangible-intangible divide, arbitrarily narrow interpretation of 'software,' and expansion of the right of communication to the public. Therefore, it becomes even more important to assess whether IP law provides effective tools to maintain a balance between public interest and private interest, as well as between the rightsholders' interest and the end user's ones: this is the realm of IP exceptions, also known as permitted acts or defences.¹⁴⁶ These exceptions allow users of IP works to carry out certain activities without the permission of the rightsholder. They can be invoked by the defendant in infringement proceedings and can be regarded as a way to inject public interest into IP, albeit in a piecemeal way.¹⁴⁷ As held in *Deckmyn*,¹⁴⁸ it is in the public interest to

144 Paige Tsai, 'Image Recognition at Facebook' (*HBS Digital Initiative*, 13 November 2018) <<https://digital.hbs.edu/platform-rctom/submission/image-recognition-at-facebook-how-machine-learning-is-helping-computers-and-people-who-are-blind-see-digital-photos/>>.

145 David Bollier, *Viral Spiral: How the Commoners Built a Digital Republic of Their Own* (New Press 2008) esp 49.

146 cf Laurence R Helfer, 'The New Innovation Frontier – Intellectual Property and the European Court of Human Rights' (2008) 49 *Harvard International Law Journal* 1.

147 Ruth L Okediji, 'Le Système International de Droit d'Auteur. Restrictions, Exceptions et Considérations En Matière d'Intérêt Public Pour Les Pays En Développement' (2006) *ICTSD* 15.

148 Case C-201/13 *Johan Deckmyn and Vrijheidsfonds VZW v Helena Vandersteen and Others* [2014] *Bus L R* 1368.

protect freedom of expression, and this includes the unauthorised use of IP works for parody purposes.¹⁴⁹ The role of exceptions as devices inject the public interest into IP has become more evident in parallel to the increased awareness of the importance of a commitment to sustainability in a time of climate emergency. To adopt a more flexible and balanced approach to exceptions, as epitomised by the fair use doctrine, would ‘*préservé pour les pays la flexibilité de continuer à élaborer des limitations et exceptions selon leurs besoins, dans leur propre contexte local.*’¹⁵⁰ Sustainable – and, more generally, fair – IP needs to have strong in-built limitations.

My starting point is that, regardless of the manifold ways IoT users attempt to neutralise the end users’ proprietary prerogatives, the latter could still use their Things without the former’s permission as long as the relevant activity falls within the scope of one of the IP exceptions. On the face of it,¹⁵¹ the IP exceptions that more clearly lend themselves to give back (some) control to the end user in the context of the IoT are:

- (i) Observation, study, and test of the functioning of a computer program;¹⁵²
- (ii) The decompilation (or reverse engineering) exception;¹⁵³
- (iii) Private copy of copyright works;
- (iv) Insubstantial extraction and reutilisation of databases protected by the *sui generis* right;
- (v) Use of a trade secret for freedom of information purposes;¹⁵⁴
- (vi) Use of a trademark not ‘in the course of trade’¹⁵⁵ and with ‘due cause’;¹⁵⁶
- (vii) Acts done privately and for noncommercial purposes in respect of objects protected by design rights.

An IoT user with some IT skills may want to inspect the Thing’s software to understand how it works, e.g. to comprehend the logic of the black box algorithm that runs in the Thing. In principle, this falls within the scope of exception that the Software Directive sets forth ‘to observe, study or test the functioning of the program.’¹⁵⁷ However, to successfully invoke it, the defendant must meet

149 Christophe Geiger and others, ‘Limitations and Exceptions as Key Elements of the Legal Framework for Copyright in the European Union: Opinion of the European Copyright Society on the CJEU Ruling in Case C-201/13 Deckmyn’ (2015) 46 IIC 93.

150 Okediji (n 148) 52.

151 This selection is, by its nature, discretionary. Other exceptions may play a role in consumer empowerment, see, e.g. Rossana Ducato and Alain Strowel, ‘Limitations to Text and Data Mining and Consumer Empowerment: Making the Case for a Right to “Machine Legibility”’ (2019) 50 IIC 649.

152 Software Directive, art 5(3).

153 Software Directive, art 6.

154 TS Directive, art 5(a).

155 TM Directive, art 10(2).

156 TM Directive, art 10(2)(c).

157 Software Directive, art 5(3).

the following requirements: (a) they must be a lawful acquirer, that is, a 'person having a right to use a copy of a computer program';¹⁵⁸ (b) the purpose has to be the determination of the 'ideas and principles which underlie any element of the program';¹⁵⁹ (c) the activity must be carried out 'while performing any of the acts of loading, displaying, running, transmitting or storing the program which (they are) entitled to do.'¹⁶⁰ The first requirement has to be interpreted broadly as encompassing anyone having a right to use the program based on a license or otherwise.¹⁶¹ This is straightforward as the owner of a Thing is likely to qualify as a lawful user despite being a mere licensee of the embedded software, unless the Thing as a whole is held under a subscription contract. The second requirement can constitute more of a hurdle because it can be interpreted as excluding activities that go beyond the mere understanding of the ideas to e.g. repair or improve the software. The third requirement is the most problematic because it might be construed as meaning that the IoT company can use the EULA or one of the other 'legals' to restrict the types of acts that end users can put in place while studying, testing, etc. the program. Even though this is a grey area, IoT companies cannot go as far as to exclude this exception altogether, directly or indirectly. Indeed, under Article 8 of the Software Directive, any contractual provision contrary to this exception is null and void. Arguably, this should extend also to those technical measures aimed at restricting user freedoms in the 'Internet of Digital Locks.'

The right to decompile the embedded software is a complementary exception that IoT users affected by the death of ownership can trigger.¹⁶² Decompilation is a method of reverse engineering whereby a program's code is analysed and the program is translated from a low level of abstraction to a higher level. Reverse engineering is a more general concept that goes beyond software (hardware can be reverse engineered) and has to do with the extrapolation of the underlying logic of a system based on the observation of its visible behaviour. Like the observation exception, the right to decompile cannot be overridden contractually; therefore, it can be useful to counter the power imbalance between IoT companies and end users by neutralising the contractual quagmire seen in Chapter 2. Decompilation is particularly important from this book's perspective given the vital role interoperability plays in preventing the Internet of Silos. Practically, this right gives IoT users the power to reproduce and translate the software's code to obtain

158 Software Directive, art 5(3).

159 Software Directive, art 5(3).

160 Software Directive, art 5(3).

161 The concept of lawful acquirer has been interpreted broadly as a 'purchaser, licensee, renter, or a person authorized to use the program on behalf of one of the above' (European Commission, 'Report on the Implementation and Effects of Directive 91/250/EEC' (2000) COM(2000)199 final para 10.) *UsedSoft* (n 103) included in the concept of lawful acquirer those who use a computer program based on a license resold by the original licensee. Moreover, national implementations (e.g. UK Copyright, Designs, and Patents Act 1988 (CDPA), s 50A) often refer to 'user' rather than 'acquirer.'

162 Software Directive, art 6.

the information necessary to achieve the interoperability of an independently created computer program. Defendants will have to prove:

- (i) To be a lawful user (typically a licensee);¹⁶³
- (ii) That the information necessary to achieve interoperability had not been previously made readily available;¹⁶⁴
- (iii) That reproduction and translation of the code are confined to the parts of the original program which are necessary in order to achieve interoperability;¹⁶⁵
- (iv) That the three-step test is made out, namely, that the exception does not unreasonably prejudices the rightsholder's legitimate interests or conflicts with a normal exploitation of the computer program.¹⁶⁶

The main limitation of this exception is that reverse engineering is possible only to obtain interoperability-related information. This is likely to require skills that most users will not have. It could nonetheless benefit them indirectly by allowing developers to design interoperable Things. Additionally, in the case of complex software, reverse engineering 'does not provide a viable means for achieving interoperability,'¹⁶⁷ and this will usually be the case with IoT software, due to its intrinsic complexity and its being fused with hardware.¹⁶⁸ A more IoT-friendly copyright and patent law would entail a positive obligation for developers to disclose the interoperability information.¹⁶⁹

Whilst the embedded software falls clearly within the scope of that subcategory of copyright that is regulated by the Software Directive, other components of our Things are covered by 'general' copyright law, as enshrined in the Info-soc Directive and the Copyright in the Digital Single Market Directive, which was transposed by member states in June 2021. Under *Nintendo v PC Box*,¹⁷⁰ complex multimedia products fall within the scope of both general copyright and software copyright when the CJEU interprets the provisions on the rightsholder's rights and remedies. The law of complex multimedia products is far from settled, however. *Tom Kabinet*¹⁷¹ is indicative of this issue as the court held

163 Software Directive, art 6(1)(a).

164 Software Directive, art 6(1)(b).

165 Software Directive, art 6(1)(c).

166 Software Directive, art 6(3); Berne Convention, art 9(2). The third step is that exceptions should be provided in 'special cases,' which is usually interpreted as meaning that they should be statutorily listed; decompilation instantiates such special case.

167 Ulla-Maija Mylly, 'An Evolutionary Economics Perspective on Computer Program Interoperability and Copyright' (2010) 41 IIC 284, 315.

168 See Zhi-Kai Zhang and others, 'IoT Security: Ongoing Challenges and Research Opportunities' 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications (IEEE 2014).

169 Mylly (n 168).

170 Case C-355/12 *Nintendo v PC Box* [2014] 1 WLUK 506; cf Dan L Burk, 'Owning E-Sports: Proprietary Rights in Professional Computer Gaming' (2013) 161 University of Pennsylvania Law Review 1535.

171 (n 97).

that e-books are attracted under 'general' copyright as opposed to 'special' software copyright. Whilst the code of the embedded program is covered by 'literary' copyright, the original interface of the Thing, should the Thing have one, may be protected as an artistic work.¹⁷² The original sounds emitted by the Thing, either downloaded or streamed, may qualify as musical works.¹⁷³ Accordingly, the IoT company's exclusive rights are limited by a number of exceptions to 'general' copyright. In particular, the private copy exception appears to be the most suitable to re-empower the IoT user who is affected by the death of ownership. Under the Infococ Directive, member states may allow the unauthorised reproduction of copyright material for private and noncommercial use, by natural persons, on condition that the rightsholders receive fair compensation, unless the prejudice caused to them is minimal.¹⁷⁴ Positively, this exception applies to the reproduction on any medium.¹⁷⁵ Therefore, e.g. a Thing's user could make a copy of the Thing's digital content accessed through the cloud and save it on a computer or other device.¹⁷⁶ However, the private copy exception has three shortcomings. First, it is optional. Unlike the aforementioned exceptions to software copyright and unlike the new exceptions under the Copyright in the Digital Single Market Directive, member states have discretion when it comes to the implementation of most of the exceptions under the Infococ Directive.¹⁷⁷ This explains why the UK does not provide the private copy exception¹⁷⁸ and the Republic of Ireland only partly implemented it.¹⁷⁹ Second, unlike the Software Directive, the exception can be overridden by means of contracts and technological protection measures.¹⁸⁰ Therefore, IoT companies can contract it out and technologically exclude it. Third, the CJEU interprets the concept of communication to the public broadly, thus leading to the excessive monopolisation of intangible assets and, ultimately,

172 Case C-393/09 *BSA v Ministerstvo Kultury* [2010] 12 WLUK 773. Conversely, the graphic user interfaces are not protected under the Software Directive.

173 Nigel Davies, 'The Digital Music Revolution – How Will Traditional Rights Operate in the on-Line Music World?' (2005) 16 *Entertainment Law Review* 137.

174 Infococ Directive, art 5(2)(b) and recital 35; Case C-463/12 *Copydan Båndkopi v Nokia Danmark* [2015] 3 WLUK 142 [96(4)].

175 Infococ Directive, art 5(2)(b).

176 Case C-265/16 *VCAST v RTI* [2017] 11 WLUK 694.

177 Apart from the exception for transient and incidental inclusion, all the exceptions under the Infococ Directive are optional.

178 The High Court quashed the Copyright and Rights in Performances (Personal Copies for Private Use) Regulations 2014 because of a defect in the consultation process (*BASCA and others v Secretary of State for Business, Innovation and Skills* [2015] EWHC 2041 (Admin)). See Guido Noto La Diega, 'In Light of the Ends. Copyright Hysteresis and Private Copy Exception after the British Academy of Songwriters, Composers and Authors (BASCA) and Others v Secretary of State for Business, Innovation and Skills Case' in Alberto M Gambino (ed), *Studi giuridici europei 2014* (Giappichelli 2016).

179 Copyright and Related Rights Act 2000, ss 101–102.

180 Estelle Derclaye and Marcella Favale, 'Copyright and Contract Law: Regulating User Contracts: The State of the Art and a Research Agenda The Relationship between Copyright and Contract Law' (2010) 18 *Journal of Intellectual Property Law* 65.

the death of ownership.¹⁸¹ The *Vcast* case¹⁸² well illustrates the point. The dispute regarded an online recording service of television broadcasts in which Vcast captured the television signal by its own antennas and recorded the time slot of the selected broadcast signal in the user's cloud storage. The private copy exception applies to the right of reproduction and not to the right of communication to the public.¹⁸³ The CJEU argued that the concept of communication to the public must be interpreted broadly as 'covering any transmission or retransmission of a work to the public by wire or wireless means, including broadcasting.'¹⁸⁴ Since the 'active involvement' of Vcast in the realization of the private copies required some form of transmission – and hence, according to the court, of communication to the public – it followed that the private copy exception would not apply. This links back to the aforementioned issue of the 'exhaustion of exhaustion': since Things are interactive objects that are embedded with content that is often transmitted and retransmitted, there is the risk that the private copy exception will not be available to IoT users. De lege ferenda, alongside being subject to the principle of exhaustion, the private copy exception should be rendered mandatory and binding.

IP, however, is not only about the protection of intangible assets. After some recent jurisprudential developments at the EU level, three-dimensional copyright is of growing importance. Traditionally, the only three-dimensional works to be protected by copyright were artistic works, and in particular sculptures, works of architecture, and works of artistic craftsmanship.¹⁸⁵ Arguably, most Things cannot be regarded as any of these 'works.' Sculptures are protected irrespective of artistic quality, but the UK Supreme Court interpreted narrowly the concept of 'sculpture' in *Lucasfilm v Ainsworth*.¹⁸⁶ There, the Imperial Stormtrooper's helmet (Figure 6.2) was deemed not to fall within the scope of copyright protection because it was a mere prop, not a sculpture.¹⁸⁷

It is fair to say that most Things are closer to props than they are to sculptures. Works of architecture, e.g. buildings, may be embedded with Things, but they are not a Thing as such, following this book's approach. Finally, works of artistic craftsmanship refer to things such as handcrafted jewellery and hand-knitted mittens. Regardless of the fact that most Things are industrially produced and cannot be regarded as a work of artistic craftsmanship, they are unlikely to meet the additional requirements of being of artistic quality and of craftsmanship.¹⁸⁸

181 See Giancarlo Frosio, 'It's All Linked: How Communication to the Public Affects Internet Architecture' (2020) 37 *Computer Law & Security Review* 105410.

182 (n 177).

183 Infosoc Directive, art 5(3).

184 *VCAST* (n 177) [40].

185 CDPA, s 4.

186 [2011] UKSC 39.

187 The Supreme Court underlined the importance to refer to the ordinary use of the word 'sculpture' and observed that not every three-dimensional representation of a concept qualifies (ibid [36], [37]).

188 *Hensher v Restawile Upholstery* [1976] AC 64.



Figure 6.2 Imperial Stormtrooper helmet. Copy created from the original mouldings used in the first Star Wars film *A New Hope*.

Source: RS Prop Masters.

This approach is consistent with the traditional assumption that copyright protects only an exhaustive list of ‘works,’ namely, literary, dramatic, musical, artistic works, films, sound recordings, typographical arrangements, and broadcasts.¹⁸⁹ This theory of the *numerus clausus* (closed number) has been arguably abandoned by the CJEU notably in *Levola Hengelo*¹⁹⁰ and *Cofemel*.¹⁹¹ In the former case, regarding the taste of cheese, it was held that for something to be a work, it must be original and it must be expressed in a manner which makes it identifiable with

189 *Creation Records v News Group Newspapers* [1997] EMLR 444.

190 Case C-310/17 *Levola Hengelo v Smilde Foods* [2018] 11 WLUK 155.

191 C-683/17 *Cofemel – Sociedade de Vestuário v G-Star Raw* [2019] 9 WLUK 110.

sufficient precision and objectivity.¹⁹² In *Cofemel*, a case about the protection of the design of a line of jeans, the court applied *Levola Hengelo* and further clarified that all works that are original and identifiable with precision and objectivity are protected by copyright: no additional and subjective requirements are allowed.¹⁹³ This means that the tangible components of the Things may be protected even though they do not fall under any of the categories of ‘works’ as long as they are the author’s own intellectual creation and if the subject matter of protection can be identified with precision and objectivity. If that is the case, the aforementioned considerations on the private copy exception apply.

The tangible components of a Thing may be protected as well by means of patents, trademarks, and design rights. For the purposes of this book, it is possible to ignore patents since they – and their exceptions – have not been harmonised at the EU level. Trademarks need only touching upon because, although one can register a shape as a trademark, the vast majority of these applications fail because consumers are unlikely to think of a shape as being indicative of a particular undertaking’s goods.¹⁹⁴ Moreover, applications for three-dimensional marks have to overcome three absolute grounds for refusal that before the 2015–2017 reform applied only to shapes:¹⁹⁵ it will not be possible to register a shape that depends on the nature of the goods, is necessary to achieve a technical result, or adds substantial value to the good.¹⁹⁶ The latter would most likely apply here. Indeed, as Advocate General Szpunar noted in *Hauck*,¹⁹⁷ the rationale of this exclusion is to demarcate the protection conferred by trademarks and that conferred by industrial designs and copyright, which are usually seen as better suited for the external features of goods that ‘substantially enhance (their) attractiveness . . . and strongly influence consumer preferences.’¹⁹⁸ I would argue that the shape of the Things influences consumer preferences and thus cannot be registered as a trademark as it adds substantial value to the Thing. There is evidence that consumer purchase Things based on emotional factors rather than rational ones related to the functionalities of the Thing as such.¹⁹⁹ Design plays a key role in eliciting consumer emotions based on a product’s attractiveness.²⁰⁰ I would conclude that

192 *Levola Hengelo* (n 191) [37], [40].

193 *Cofemel* (n 192) [35].

194 ‘Average consumers are not in the habit of making assumptions about the origin of goods based on the shape’ (Case C-218/01 *Henkel KGaA v Deutsches Patent- und Markenamt* [2004] ECR I-1725 [52]). Recently, the General Court has held that the shape of a lipstick can be distinctive in Case T-488/20 *Guerlain v EUIPO* (General Court, 14 July 2021).

195 The EU reform of trademark extended the absolute grounds for refusal that once applied only to shape marks to ‘another characteristic’ (TM Directive, art 4(1)(e)).

196 TM Directive, art 4(1)(e); Case T-508/08 *Bang & Olufsen v OHM* [2011] ECR II-6975.

197 Case C-205/13 *Hauck v Stokke* [2014] 9 WLUK 444, Opinion of AG Szpunar.

198 *ibid* [80].

199 Luis Hernan Contreras Pinochet and others, ‘The Influence of the Attributes of “Internet of Things” Products on Functional and Emotional Experiences of Purchase Intention’ (2018) 15 *Innovation & Management Review* 303.

200 Ravindra Chitturi, ‘Emotions by Design: A Consumer Perspective’ (2009) 3 *International Journal of Design* 7.

the fact that the design of a Thing affects the decision to purchase it suggests that IoT companies are unlikely to be successful in registering the shape of their Things as a trademark as that shape would add substantial value to the goods. Nonetheless, should a Thing's shape be registered as a trademark, its private use would not constitute infringement because 3D mark owners can only prevent uses 'in the course of trade.'²⁰¹ A trademark is used in the course of trade if it performs one of functions of trademarks, mainly, if it acts as a 'badge of origin'²⁰² of the good or service. Most private uses of IoT shape marks will not qualify as infringement because a private use of a Thing is unlikely to signal to third parties a claim that the Thing originates from the end user. Moreover, in line with ECtHR jurisprudence, freedom of expression can operate as an external limit to trademark law.²⁰³ Some have argued that it is not necessary to introduce external freedom-of-expression limits because 'EU trade mark law itself provides for limits that guarantee respect of the freedom of expression.'²⁰⁴ This applies especially to well-known marks, such as Amazon's arrow. Their protection is stronger than ordinary marks, but their unauthorised use does not constitute infringement if it is supported by 'due cause.'²⁰⁵ There is no definition of *due cause*, but as held in *Leidseplein v Red Bull*,²⁰⁶ it includes ante-registration uses and uses that are in good faith. The CJEU underlined that the concept of due cause is intended to strike a balance between the proprietor's interests and either objective or subjective interests of a third party using the identical sign. Although the court does not couch this as freedom of expression, it is not unfounded to see the concept through this lens. Whilst it is contested whether freedom of expression creates an autonomous defence to trademark infringement, it is clear that existing exceptions must be interpreted broadly. Indeed, the new Trade Marks Directive and the EU Trade Marks Regulation,²⁰⁷ for the first time, provide that their application must ensure 'full respect for fundamental rights and freedoms, and in particular the freedom of expression.'²⁰⁸ Accordingly, in the unlikely event that the shape of a Thing is registered as a trademark, freedom of expression will breathe life into the

201 TM Directive, art 10(2); Regulation (EU) 2017/1001 of 14 June 2017 on the European Union trade mark ('EUTM Regulation') [2017] OJ L 154/1, art 9.

202 *Unilever v Griffin* [2010] EWHC 899 (Ch) [11]-[14].

203 *Österreichische Schutzgemeinschaft für Nichtraucher v Austria*, App no 17200/90 (Eur. Comm'n on H.R., 2 December 1991) as interpreted by Christophe Geiger and Elena Izyumenko, 'The Constitutionalization of Intellectual Property Law in the EU and the Funke Medien, Pelham and Spiegel Online Decisions of the CJEU: Progress, But Still Some Way to Go!' (2020) 51 IIC 282, 63.

204 Michal Bohaczewski, 'Conflicts Between Trade Mark Rights and Freedom of Expression Under EU Trade Mark Law: Reality or Illusion?' (2020) 51 IIC 856.

205 TM Directive, art 10(2)(c).

206 Case C-65/12 *Leidseplein Beheer v Red Bull* [2014] Bus LR 280.

207 TM Directive, recital 27; EUTM Regulation, recital 21.

208 No such reference was present in the previous directive (Directive 2008/95/EC of 22 October 2008 to approximate the laws of the Member States relating to trade marks ('Second TM Directive')) [2008] OJ L 299/25).

aforementioned defences and most acts carried out by IoT users will not qualify as infringement.

Design rights²⁰⁹ appear to be the most suitable form of IP protection for the shape of a Thing and, more generally, its tangible components.²¹⁰ *Design* means the ‘appearance of the whole or a part of a product resulting from the features of, in particular, the lines, contours, colours, shape, texture and/or materials of the product itself and/or its ornamentation.’²¹¹ In light of the composite nature of most Things, many of them will likely qualify as ‘complex products,’ which design law defines as products ‘composed of multiple components which can be replaced permitting disassembly and reassembly of the product.’²¹² If a Thing’s design – or the design of its visible component parts if we are dealing with a complex product²¹³ – is novel²¹⁴ and has individual character,²¹⁵ the rightsholder can prevent anyone, including the IoT user, from using the product.²¹⁶ However, although the ‘delineation of rights is not restricted to commercial uses,’²¹⁷ design rights cannot be exercised in respect of acts done for private and noncommercial purposes.²¹⁸ This exception – that applies also to Community Design Rights²¹⁹ – is mandatory, and therefore, member states must provide it in their national laws.²²⁰ It is unclear whether the exception can be overridden by means of a contract, e.g. via the terms of service linked to the purchase of a Thing. On the one hand, the Design Directive is without prejudice of other forms of protection, including civil liability and unfair competition, whilst contract law is not mentioned.²²¹ On

209 Design rights can be registered or unregistered, but this chapter will only consider the former because there has been no harmonisation of unregistered designs in the EU.

210 Design rights can also protect two-dimensional articles. The unregistered design right has not been harmonised; therefore, some countries, e.g. the UK, apply unregistered design rights only to two-dimensional articles. See CDPA, s 213.

211 Directive 98/71/EC of 13 October 1998 on the legal protection of designs (‘Design Directive’) [1998] OJ L 289/28, art 1(a).

212 Design Directive, art 1(c).

213 Design Directive, art 3(3).

214 A design is novel if no identical design has been made available to the public before the date of filing of the application or if the variant differs only in immaterial details (Design Directive, art 4).

215 A design has individual character if the ‘overall impression it produces on the informed user differs from the overall impression produced on such a user by any design which has been made available to the public before the date of filing of the application’ (Design Directive, art 5).

216 Design Directive, art 12(1).

217 Lionel Bently and others, *Intellectual Property Law* (5th edn, OUP 2018) 797.

218 Design Directive, art 13(1)(a). Some unauthorised commercial uses are lawful as well. E.g. the citation exception refers to commercial citation (Community Design Regulation, art 20(1)(c); Joined Cases C-24/16, C-25/16 *Nintendo Co Ltd v BigBen Interactive GmbH* [2018] Bus LR 1245).

219 Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs (‘Community Design Regulation’) [2002] OJ L 3/1, art 20(1)(a).

220 This can be inferred by the use of ‘shall’ in art 13 of the Design Directive. E.g. in the UK, the Intellectual Property Act 2014 introduced a series of exceptions which mirror patent and copyright exceptions, including the private and noncommercial defence under the CDPA, s 244A.

221 Design Directive, art 14.

the other hand, no specific provision on the contractual overridability is made. The exception is further narrowed by national laws imposing requirements of (i) no undue prejudice to the normal exploitation of the design, (ii) compatibility with fair trade practices, and (iii) acknowledgement of the source.²²² However, the interpretation of design law and of its exceptions should never lead to a disproportionate interference of freedom of expression, as the ECtHR held in *Plesner v Louis Vuitton*.²²³ This should empower the IoT user to utilise their Things as freely as possible regardless of their design protection. Moreover, design rights should not be used to stifle innovation and suppress competition. This was made clear by the CJEU in *Nintendo v BigBen*,²²⁴ where the citation exception – hitherto regarded as narrowly applicable – was ‘transformed into a far more expansive right for third-party competitors to re-produce designs to explain or demonstrate product compatibility.’²²⁵ These human rights–orientated interpretations of the exceptions are fit for the IoT and should be welcomed as a positive approach to balancing IP and competing interests.²²⁶

It is of little doubt that the value of the IoT is intrinsically linked to the value of the big data produced by our Things, also known as machine data or industrial data.²²⁷ Whilst data as such and in isolation is not covered by IP, it can be protected under certain circumstances by an oft-forgotten right, namely, the sui generis right under the Database Directive (also known as ‘the database right’).²²⁸ This is of particular relevance in the context of machine-generated datasets that are at the core of the IoT. The sui generis right is not confined to physical databases where documents are systematically archived (e.g. the Wiener Holocaust Library) and to online databases (e.g. WestLaw). Under this directive, a database is any collection of ‘independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.’²²⁹ In principle, an air company’s website that allows users to search and book flights can be regarded as a database.²³⁰ The collection of voice recordings of the users’ interactions with Google Home could be an example of IoT database.

222 CDPA, s 244A(c)(i), (ii).

223 *Plesner v Louis Vuitton* [2011] E.C.D.R. 14.

224 (n 218) [86].

225 Jane Cornwell, ‘Nintendo v BigBen and Acacia v Audi; Acacia v Porsche: Design Exceptions at the CJEU’ (2019) 14 *JIPPL* 51, 53.

226 Natalia Kapyrina, ‘Limitations in the Field of Designs’ (2018) 49 *IIC* 41, 58. *Contra*, David Stone, ‘Design Law Misplayed in Nintendo AG Opinion’ (2017) 12 *JIPPL* 558, 560.

227 Nastaran Hajiheydari, Mojtaba Talafidaryani and SeyedHossein Khabiri, ‘IoT Big Data Value Map: How to Generate Value from IoT Data’ *Proceedings of the 2019 the 5th International Conference on e-Society, e-Learning and e-Technologies – ICSLT 2019* (ACM Press 2019).

228 Database Directive, arts 7–11.

229 Database Directive, art 1.

230 In Case C-30/14 *Ryanair v PR Aviation* [2015] 2 All E.R. (Comm) 455, however, the database fell outside the scope of the directive because it did not meet the further requirements of originality and substantial investment. See Tatiana – Eleni Synodinou, ‘Databases and Screen Scraping: Lawful User’s Rights and Contractual Restrictions Do Not Fly Together’ (2016) 38 *EIPR* 312.

Indeed, these recordings are stored systematically and made available in an individually retrievable way.²³¹

A database may be protected by copyright or by the sui generis right. I will overlook the former as only a minority of IoT databases will attract copyright. Indeed, for a database to be copyright protected, the selection and arrangement of the contents must be original, that is, the author's own intellectual creation.²³² Copyright is not fit for IoT databases because of the prevalence of automation in selecting and arranging the contents; in other words, the setting up of these databases 'is dictated by technical considerations, rules or constraints which leave no room for creative freedom.'²³³ IoT databases, nonetheless, could be protected by the sui generis right, since the latter does not require originality. The maker of a database has the right to prevent extraction and reutilisation of the contents of the database if the investment in obtaining, verifying, or presenting its contents was substantial.²³⁴ One could object that IoT companies do not need to invest substantially to set up their databases, since they are mostly machine-generated. However, in reality, the threshold of substantiality accepted by courts throughout Europe is low. In practice, any investment is regarded as substantial as long as it is 'more than minimal.'²³⁵ IoT companies will not struggle to identify even a limited amount of 'human, technical and financial resources'²³⁶ invested in the database, and therefore, this requirement is unlikely to constitute a hurdle. An investment will be needed e.g. for human beings to label the data, especially if the database relies on supervised or semisupervised learning techniques.²³⁷

The sui generis right is often regarded as unfit for IoT data.²³⁸ The unfitness is mostly based on *British Horseracing Board v William Hill*²³⁹ and the three *Fixtures Marketing* cases,²⁴⁰ where the CJEU took the debatable decision that the investment into newly created – as opposed to already existing, 'obtained' – data does not attract sui generis protection. Many have interpreted this obtaining-creating dichotomy as an endorsement of the so-called spin-off theory, whereby 'databases which are the by-products of the main activities of an economic undertaking ('spin-off'

231 'Google – My Activity' <<https://myactivity.google.com/activitycontrols/webandapp>>.

232 Database Directive, art 3(1); Case C-604/10 *Football Dataco v Yahoo! UK* [2012] Dir com sc int 269.

233 *Football Dataco* (n 232) [39].

234 Database Directive, art 7.

235 European Commission, 'SWD "Evaluation of Directive 96/9/EC on the Legal Protection of Databases"' (2018) SWD(2018)147final 27.

236 Database Directive, recital 7.

237 Noto La Diega, 'Artificial Intelligence and Databases in the Age of Big Machine Data' (n 56).

238 Matthias Leistner, 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos 2017) 25.

239 Case C-203/02 *British Horseracing Board v William Hill* [2004] ECR I-10415.

240 Case C-338/02 *Fixtures Marketing v Svenska Spel* [2004] ECR I-10497; Case C-444/02 *Fixtures Marketing v OPAP* [2004] ECR I-1549; Case C-46/02 *Fixtures Marketing v Oy Veikkaus Ab* [2004] ECR I-10365.

databases) are in principle not protected by the *sui generis* right.²⁴¹ The example of such spin-off databases made by the Commission was ‘the automated creation of machine-generated data (e.g. Internet of Things data).’²⁴² However, the spin-off theory has no sound basis in the four aforementioned cases. Indeed, the CJEU held that the creation of a database can be ‘linked to the exercise of a principal activity in which the person creating the database is also the creator of the materials contained in the database’²⁴³ as long as the obtaining, verification, or presentation ‘required *substantial investment . . . independent of the resources used to create those materials.*’²⁴⁴ Accordingly, although most IoT databases may be regarded as spin-off databases, they could nonetheless be protected by the *sui generis* right. More generally, the CJEU cases – and their postulation of an obtaining-creating dichotomy – can be criticised for three reasons. First, *British Horseracing* and *Fixtures Marketing* overemphasise the relevance of some recitals of the Database Directive that could be invoked to reach the opposite conclusion. In particular, they can lead to conclude that databases of ‘created’ data are in fact protected by the *sui generis* right. As pointed out in Recital 9, databases are a vital tool in the development of an information market. Given that the majority of the investments made by the database makers regard data collection rather than the setting up of the database itself,²⁴⁵ this recital can be construed as providing an argument in favour of the relevance of investments in ‘created’ data for the *sui generis* right to subsist. Second, a comparative analysis of domestic case laws shows that the same data can be treated as ‘created’ in some jurisdictions and ‘obtained’ in others,²⁴⁶ with live football data deemed to be ‘created’ in Germany and ‘obtained’ in the UK.²⁴⁷ Third, the Fourth Industrial Revolution shows the untenability of the creating-obtaining dichotomy. This is well illustrated by the use of AI-powered data mining in predictive analytics: it leads to inferences, identification of patterns, and discovery of correlations between existing data; one could argue both ways, that this data is created or, as seems more reasonable, obtained.

Given that, consequently, it can be argued that the *sui generis* right provides some protection to IoT data,²⁴⁸ it becomes important to assess whether the excep-

241 European Commission, ‘SWD “Evaluation of Directive 96/9/EC on the Legal Protection of Databases”’ (n 236) 15.

242 *ibid.*

243 *British Horseracing* (n 239) [35].

244 *ibid* [35].

245 European Commission, ‘SWD “Evaluation of Directive 96/9/EC on the Legal Protection of Databases”’ (n 236) 36.

246 In the literature, there is no consensus on where to draw the line between creation and obtaining. See Estelle Derclaye, *The Legal Protection of Databases: A Comparative Analysis* (Edward Elgar 2008); Ottolia (n 51).

247 *Football Dataco Ltd v Stan James Ltd* (No 2) [2013] EWCA Civ 27; European Commission, ‘SWD “Evaluation of Directive 96/9/EC on the Legal Protection of Databases”’ (n 236) 25.

248 The *sui generis* protection will depend on a number of factors, e.g. if the learning model utilised is a supervised one (i.e. requiring human intervention), if the IoT system is created with the purpose of setting up a database, or if it produces databases serially, etc. More on this in Noto La Diega, ‘Artificial Intelligence and Databases in the Age of Big Machine Data’ (n 56).

tions to this right can be successfully invoked by IoT users who find themselves affected by the death of ownership. There are two exceptions that may come into play in these scenarios. First, database makers cannot prevent lawful users from extracting or reutilising insubstantial parts of the database's contents.²⁴⁹ Importantly, this is expressly qualified as a user right rather than an exception, and therefore, any narrow interpretation should be excluded. This is further corroborated by the generous wording of the directive, whereby insubstantial extraction and reutilisation can be carried out 'for any purposes whatsoever',²⁵⁰ therefore, commercial and mixed uses are included. It is mandatory for member states to provide this right in the national implementation measures,²⁵¹ and companies may not override it contractually.²⁵² The limit to this is that only a lawful user can exercise this right, which means that if the terms of service prevent all access and use of the database, the term will prevail on the exception. However, if the use is permitted, then the terms of service (and the other 'legals') cannot be used to prevent the insubstantial extraction of the database's contents. Conversely, the private use exception to the sui generis right is rather narrow. First, it is optional, and therefore, member states can decide not to implement it.²⁵³ Second, contracts can be used to override it,²⁵⁴ which is worrying in the IoT's contractual quagmire and associated power imbalance. Third, the private use exception applies only to the extraction (and not to the reutilisation) of the contents of nonelectronic databases, which makes it useless in an IoT context. The main weakness in any strategy that would rely on the exceptions to the sui generis right is the narrow interpretation given to this regime in *Ryanair v PR Aviation*.²⁵⁵ There, the defendant's screen scraping, i.e. the automated extraction of data from a website,²⁵⁶ was considered to be in violation of Ryanair website's terms and conditions. In particular, the low-cost airline put in place an exclusive distribution system and prevented unauthorised websites to sell Ryanair flights.²⁵⁷ The use of the website was limited to private, noncommercial purposes. The defendant's argument was

249 Database Directive, art 8.

250 Database Directive, art 8(1).

251 This is clear from the working of Article 8, especially if compared with Article 9 and the latter's use of the verb 'may.'

252 Any contractual provision that would be contrary to this right would be null and void (Database Directive, art 12).

253 This is made clear by the wording of Article 8, whereby: 'Member States may stipulate' as noted by David I Bainbridge, *Information Technology and Intellectual Property Law* (7th edn, Bloomsbury 2019) 242.

254 The Database Directive considers binding only the aforementioned right to insubstantial extraction and the right to perform those acts that are necessary to access the database and its normal use (the latter applies to original databases protected by copyright).

255 (n 230).

256 Marco Caspers and others, 'Baseline Report of Policies and Barriers of TDM in Europe' (2016) Future TDM D3.3+ 9.

257 The current version of the Terms and Conditions, as updated on 5 September 2018, no longer contains such provisions. See Ryanair General Terms & Conditions of Carriage, effective as of 9 September 2020 <www.ryanair.com/gb/en/useful-info/help-centre/terms-and-conditions>.

that what they did was covered by exceptions that contracts could not override. The CJEU held that if a database does not meet the requirements of originality or substantial investment, they are outwith the scope of the directive, and therefore the relevant exceptions cannot be invoked.²⁵⁸ This decision can be criticised on three grounds. First, the directive's scope is identified by reference to the definition of database;²⁵⁹ therefore, as long as the materials are independent, arranged systematically or methodically, and individually accessible, we are within the scope of the directive and the exceptions should be available. The assessments regarding originality and substantiality should not be conflated with the issue of the scope of protection. Second, making the exceptions unavailable to users of databases where neither substantial investment nor originality can be proved is unreasonable. Indeed, it would lead to recognising a stronger protection to those databases where the author did not put in place any intellectual effort or any meaningful investment. Finally, the main justification of the Database Directive is to stimulate investments in the database industry to bridge the gap between the US and the EU market.²⁶⁰ This goal cannot be achieved applying *Ryanair* because this ruling incentivises the database makers not to invest significantly in obtaining, verifying, and presenting contents. By reducing investments, they can circumvent the database's user rights and exceptions. The joint operation of the obtaining-creating dichotomy and the *Ryanair* jurisprudence confirms the need to revitalise the sui generis rights and, in particular, its exceptions: otherwise, IoT companies and other database makers can accumulate vast amounts of data and increase their data power by contractual and technical means, thus cementing the death of ownership.

IoT data is of tremendous value especially when used to train the algorithms that constitute the IoT's hidden architecture. Much of their value comes from being secret.²⁶¹ Indeed, as seen in the previous chapter, an increasingly important role is played by the (ab)use of trade secrets on IoT's algorithms and machine data. The Trade Secrets Directive has clarified that, for a trade secret to subsist, the information has to be (i) not generally known or readily accessible, (ii) of commercial value because it is secret, and (iii) subject to reasonable steps to keep it secret.²⁶² One may argue that the information that is embodied in a Thing, being easily accessible by third parties, can be accessed or reverse engineered and is therefore not secret.²⁶³ Accordingly, one may say, the data and the algorithms that are embodied in Things are not secret, as long as they can be easily accessed by means of reverse engineering or decrypted. However, courts have become, over

258 *Ryanair* (n 230) [49].

259 Database Directive, art 1(2).

260 Database Directive, recital 11.

261 This is not limited to IoT's algorithms. See more generally Guido Noto La Diega, 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information' (2018) 9 JIPITEC 3.

262 TS Directive, art 2(1).

263 *Saltman Engineering v Campbell Engineering* (1948) 65 RPC 203.

time, more amendable to the idea of considering Thing-embedded algorithms as secret. In *Volkswagen v Garcia*,²⁶⁴ the court e.g. granted an interim injunction to prevent the disclosure of an algorithm. This algorithm was embedded in a car's immobiliser, and the defendants had accessed it by reverse engineering a computer program that they had found online.²⁶⁵ Whilst theoretical objections can be moved to the idea of IoT algorithms and machine data as trade secrets, pragmatically one needs to take account of the fact that IoT companies do keep this information secret, and this is part of its value. For example, the algorithm that allows Alexa to be a powerful tool of the 'Internet of Personalised Things' constitutes commercially valuable confidential information.²⁶⁶

Trade secret protection is dangerous because IoT companies could keep the information secret potentially forever. Although users may counter it by invoking exceptions and GDPR rights (e.g. right to be informed),²⁶⁷ the likelihood that this happens in practice is limited due to the secrecy of these practices. Under Article 5 of the Trade Secrets Directive, user freedom can be ensured by a number of exceptions that allow the unauthorised acquisition, use, or disclosure of a trade secret. These exceptions are in place to ensure the interest of circulation of knowledge.²⁶⁸ This is particularly the case with the exception 'for exercising the right to freedom of expression and information as set out in the Charter (of Fundamental Rights of the EU).'²⁶⁹ Whilst the emphasis of the directive is on press freedom and media pluralism, these are not the only applications of freedom of expression and information that are protected as a human right in Europe. This is evidenced by the ECtHR jurisprudence that balances IP against higher values and, in particular, freedom of expression and information under Article 10 ECHR.²⁷⁰ Although this case law regards copyright,²⁷¹ the same rationale applies to all IPRs, including trade secrets.²⁷² It is not by chance that *N.V. Televizier v The*

264 [2013] EWHC 1832.

265 The court did not consider *Saltman* and ignored the issue of whether, once decrypted, the algorithms could still be regarded as secret. Moreover, a crucial role was played by the practical consideration that the disclosure may have led to mass car theft. Nonetheless, *Volkswagen v Garcia* remains an important victory for those who consider IoT-embedded data and algorithms as secret.

266 Guido Noto La Diega and Cristiana Sappa, 'The Internet of Things at the Intersection of Data Protection and Trade Secrets. Non-Conventional Paths to Counter Data Appropriation and Empower Consumers' [2020] REDC 419.

267 GDPR, arts 13–14.

268 cf Andrea Ottolia, 'Il D. Lgs n. 63/18 Di Attuazione Della Direttiva Sulla Protezione Dei Segreti Commerciali Fra Tutela e Bilanciamenti' [2019] NLCC 1091.

269 TS Directive, art 5(a).

270 Peggy Ducoulombier, 'Interaction between Human Rights: Are All Human Rights Equal?' in Christophe Geiger (ed), *Research Handbook on Human Rights and Intellectual Property* (Edward Elgar 2015) 45–46.

271 Christophe Geiger and Elena Izyumenko, 'Shaping Intellectual Property Rights Through Human Rights Adjudication. The Example of the European Court of Human Rights' (2020) Centre for International Intellectual Property Studies Research Paper No 2020–02 44.

272 The nature of trade secrets is contested; they have been considered as a 'creature of contract, of tort, of property, or even of criminal law' (Lemley (n 46)).

*Netherlands*²⁷³ – the first-ever ECHR case about the balance of IP and human rights – regarded Article 10.²⁷⁴ The first ‘balancing’ rulings in the seventies and in the nineties did not find violations of Article 10.²⁷⁵ The ‘real breakthrough’²⁷⁶ was in 2013, when the court started dealing with online copyright infringement and its impact on free flow of information in the digital environment. This change in direction started with the rulings in *Donald v France*²⁷⁷ and *The Pirate Bay*.²⁷⁸ The facts were quite different, the former dealing with the unauthorised publication of some photographs taken at a fashion show, the latter with a notorious file-sharing platform that enabled the illegal download of music, films, and computer games. Importantly, the court held that the applicants’ convictions for copyright infringement constituted an interference with Article 10. The interference was not considered disproportionate as the expression the applicants were seeking to protect had commercial character.²⁷⁹ This means that the abuse of IP, including trade secrets, to prevent an IoT user from utilising their Things for noncommercial purposes may be regarded as disproportionately interfering with freedom of expression.²⁸⁰

In considering the scope of the Trade Secrets Directive’s freedom of expression exception, one needs to account for the ECtHR’s practice to view IP ‘as an exception to freedom of expression (which) must hence be narrowly interpreted.’²⁸¹ Even more progressive in its recognition of the limits of IP is the CJEU jurisprudence, which has been balancing IP and freedom of expression – in particular, freedom of information – in a way that allows the interpreter to requalify IP exceptions as proper user rights as opposed to mere ‘exceptional’ defences available only passively, should the rightsholder claim infringement.²⁸² The CJEU has been gradually recognising the importance of a fair balance between the rightsholders’ interests and the competing rights and interests in the context of IP disputes that are examined ‘mainly from the angle of fundamental rights.’²⁸³ It follows that courts need to interpret trade secrets exceptions in a way that pursues a fair balance between the IPRs and the ‘*rights of the users* of protected subject matter.’²⁸⁴

273 App no 2690/65 [1968] Y B Eur Conv on H R 782.

274 Geiger and Izyumenko (n 272).

275 *D.G.P.N.V. v Netherlands*, App no 5178/71 (1976) 44 Eur Comm’n H R Dec & Rep 13; *Société Nationale de Programmes FRANCE 2 v. France*, App no 30262/96 [1997] Eur Comm’n on H R 15.

276 Geiger and Izyumenko (n 272) 52.

277 App no 36769/08 (ECtHR, 10 January 2013).

278 *Kolmisoppi v Sweden*, App no 40397/12 (ECtHR, 19 February 2013).

279 Geiger and Izyumenko (n 272). The other reason being that the information contained in the shared material did not contribute to the general debate of public interest.

280 cf *Akdeniz v Turkey*, App no 20877/10 (ECtHR, 11 March 2014).

281 Elena Izyumenko, ‘The Freedom of Expression Contours of Copyright in the Digital Era: A European Perspective: The Freedom of Expression Contours of Copyright’ (2016) 19 *The Journal of World Intellectual Property* 115.

282 *ibid.*

283 Case C-70/10 *Scarlet v SABAM*, Opinion of AG Cruz Villalón [5].

284 *Deckmyn* (n 148) [26], italics added.

As stated *inter alia* in *Deckmyn*²⁸⁵ and elaborated in the literature,²⁸⁶ IP and user rights should be regarded as having equal standing.

At first glance, more recent cases *Funke Medien*,²⁸⁷ *Pelham*,²⁸⁸ and *Spiegel Online*²⁸⁹ would seem to go in the opposite direction. Indeed, they deny that member states can create exceptions beyond those listed in the relevant directives. This notwithstanding, these cases have been seen as the confirmation of the ‘liberal, “*freedom-of-expression-driven*” approach of the CJEU’²⁹⁰ to IP balancing. Accordingly, the awareness that ‘freedom of expression and information give a substantive content to the rights of users’²⁹¹ must inform the understanding of the exceptions under all IP laws, including the Trade Secrets Directive. Therefore, I would opine that under the freedom of information exception, trade secrets cannot be used to prevent IoT users from handling their Things unencumbered, especially so as to allow them to understand how their Things work and to comprehend their underlying logic, including by accessing the Things’ intangible components.

The prospect of relying on a combination of exceptions-user rights to regain control over one’s Things is appealing. However, its potential to tackle the death of ownership in the IoT is thwarted by five factors. First, exceptions may counter only abuses that are perpetrated by means of IP rights. IoT companies can find ways to strategically bring their conduct outwith the scope of IP laws. If IP laws do not apply, IP exceptions will be unavailable, as was the case in *Ryanair v Aviation PR*.²⁹² In practice, most of IoT data is likely to fall outside the scope of the Database Directive, and IoT users are therefore unlikely to be able to invoke the relevant exceptions. Second, although IP law discourages rightsholders from using technological protection measures to compress the exceptions,²⁹³ however, this may prove to be immaterial in practice. Indeed, the IoT is a high-speed and low-focus environment, and therefore technical defaults can influence user behaviour more than traditional legal rules. Third, contractual abuses may be tackled only by those exceptions that expressly override contracts. *De lege ferenda*, it is crucial to streamline all IP exceptions to render them binding. Fourth, IP excep-

285 *ibid*, referring to Case C-467/08 *Padawan v SGAE* [2011] ECDR 1.

286 Lionel Bently and Tanya Aplin, *Global Mandatory Fair Use: The Nature and Scope of the Right to Quote Copyright Works* (CUP 2020).

287 Case C-469/17 *Funke Medien v Germany* [2020] 1 WLR 1573 about the unauthorised communication to the public of periodic briefing reports on the operations of the federal armed forces abroad.

288 Case C-476/17 *Pelham v Hutter* (‘Metall auf Metall’) [2019] 7 WLUK 462 about music sampling.

289 Case C-516/17 *Spiegel Online GmbH v Beck* [2019] 7 WLUK 458 about hyperlinks, news reporting, quotation, and freedom of expression.

290 Geiger and Izyumenko (n 204) 286. The authors recognise, however, that whilst freedom of expression could be used to overcome a rigid approach to the three-step test and embrace an open-ended copyright exception, the CJEU did not go as far.

291 Izyumenko (n 282) 118.

292 (n 230).

293 Infosoc Directive, art 6(4); C-DSM Directive, art 17(9).

tions can do little to empower IoT users affected by factual control over the Thing, in particular over services and data. Abuses of data power are under increased scrutiny of antitrust authorities, but competition law remains unfit for these new forms of power.²⁹⁴ The recent inquiry of the European Commission into the antitrust issues of the IoT confirmed this inadequacy.²⁹⁵ It remains to be seen whether unconventional interventions such as the Data Governance Act, the Digital Services Act, and the Digital Markets Act will be able to curb IoT power. Finally, the viability of exception-focused strategies is limited by the issue of IP overlaps. The latter predates the IoT but is exacerbated by this sociotechnological phenomenon. To test the viability of the proposed exception-focused strategy, the next section will give a closer look at IP overlaps.

6.5 IP Overlaps and the Erosion of IP Exceptions in the 'Smart' World

The IoT provides an excellent illustration of the problem of the cumulation of rights. As IPRs overlap, any strategy aimed at countering the death of ownership by leveraging the potential of IP exceptions is called into question. Indeed, what constitutes an exception under one IP subsystem (e.g. copyright) may constitute infringement under another (e.g. design rights). The IoT ushers in an era of ubiquitous computing and ubiquitous IPRs. The more these rights expand, the more user rights contract.

Despite some similarities, the exceptions analysed in the previous section are rather diverse. Some are mandatory; others are left to the discretion of member states as to whether to implement them. Some are binding; others can be overridden contractually. Some cover commercial uses; others do not. Some are regarded as user rights; others are not.²⁹⁶ The joint operation of overlapping IPRs covering virtually any aspect of a Thing and the misalignment between IP exceptions hampers any strategy to counter the death of ownership in the IoT by invoking IP exceptions.

The question of IP overlaps may be perceived as niche, but it is of great theoretical and practical importance.²⁹⁷ Countless laws have been passed – and numerous rulings have been handed in – in the 310 years of the history of copyright legislation, from the Statute of Anne to the Copyright in the Digital Single

294 The shift in focus can be seen, e.g. in Case AT.39740 *Google Search* (C(2017) 4444 final).

295 'Antitrust: Initial Findings of Consumer IoT Sector Inquiry' (*European Commission*, 9 July 2021) <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2884>.

296 Even when a limitation to an IP right is qualified as an exception and not as a right, it should nonetheless be interpreted in a way that does not undermine its effectiveness and that takes into account the exception's purpose. In this sense, *Nintendo v BigBen* (n 218) [74].

297 As shown by the following in-depth analyses: Estelle Derclaye and Matthias Leistner, *Intellectual Property Overlaps: A European Perspective* (Hart 2011); Neil Wilkof and Shamnad Basheer (eds), *Overlapping Intellectual Property Rights* (OUP 2012); Tomkowicz (n 33); Nuno de Araújo Sousa e Silva, *The Ownership Problems of Overlaps in European Intellectual Property* (Nomos 2014).

Market Directive. These laws and rulings have enlarged the types of subject matters eligible for protection (e.g. databases),²⁹⁸ widened and strengthened the owners' exclusive rights (e.g. the all-encompassing right of communication to the public),²⁹⁹ and provided discrete IPRs for their protection (e.g. the new publishers' right that adds to already-existing author rights on the same subject matter).³⁰⁰ The fact that the 'expansion of (IP) rights at the international level is more extensive than ever'³⁰¹ is at the root of this phenomenon and of the subsequent issue of overlaps. If a country wishes to be a member of the WTO, they have to accept to be bound by Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). This agreement obliges contracting states to protect all the rights covered by the treaty, that is, copyright and related rights,³⁰² trademarks,³⁰³ geographical indications,³⁰⁴ industrial designs,³⁰⁵ patents,³⁰⁶ topographies of integrated circuits,³⁰⁷ and protection of undisclosed information.³⁰⁸ The lack of adequate protection of these rights would expose the country to a breach of the TRIPS obligations falling under the jurisdiction of the WTO Dispute Settlement Body. Conversely, it is left to the states' discretion whether to introduce IP exceptions. If they do introduce them, they need to comply with the three-step test. As touched upon in the previous section, exceptions need to be limited to certain special cases, not to conflict with the normal exploitation of the work and not unreasonably prejudice the legitimate interest of the owner.³⁰⁹ Whilst a fair and balanced interpretation of the three-step test could be put forward,³¹⁰ the WTO favours a strict interpretation that regards the limbs as cumulative.³¹¹ The situation is worsened by the so-called TRIPS-plus provisions: free trade agreements that introduce stronger IP protection in exchange for trade opportunities.³¹² TRIPS-plus provisions further tilt the IP balance in favour of rightsholders, especially those based in developed countries. This is exemplified by the data exclusivity provisions that, by allowing pharmaceutical test data submitted by companies to drug regulatory

298 Database Directive (although databases were arguably protected also before the directive; see Derclaye (n 247) 45).

299 We have seen above this phenomenon as epitomised by *Tom Kabinet* (n 97).

300 C-DSM Directive, art 15(1).

301 Wilkof and Basheer (n 298) *ivii*.

302 TRIPS, arts 9 ff.

303 TRIPS, arts 15 ff.

304 TRIPS, arts 22 ff.

305 TRIPS, arts 25 ff.

306 TRIPS, arts 27 ff.

307 TRIPS, arts 35 ff.

308 TRIPS, art 39.

309 See e.g. TRIPS art 13.

310 Christophe Geiger and others, 'Declaration. A Balanced Interpretation Of The "Three-Step Test" In Copyright Law' (2010) 1 JIPITEC 119.

311 WTO Panel, 'United States – Section 110(5) of the US Copyright Act' (2000) WT/DS160/R.

312 S Frankel, 'Challenging Trips-Plus Agreements: The Potential Utility of Non-Violation Disputes' (2009) 12 Journal of International Economic Law 1023.

authorities to remain secret, factually and substantially extend the duration and the scope of the monopoly granted by the relevant patent.³¹³ This is one of the reasons that a COVID patent waiver may not suffice and more courageous, open innovation models should be adopted.³¹⁴ Stronger and pervasive IPRs led to their overlaps becoming commonplace. This also depends on technological development producing a 'diversity of goods and services and ever-more powerful platforms to deliver them.'³¹⁵ Existing IP laws are often claimed not to be fit for these innovations, which typically leads to additional protection being provided in legislation or case law, with judicial expansions being often crystallised in legislation.³¹⁶

The negative effects of this accumulation can be seen most clearly in the IoT, where virtually every aspect and component of even simple Things are protected by some form of IP. This risks neutralising the potential of IP exceptions because many of the acts covered by an IPR's exceptions constitute infringement of another IPR.³¹⁷ Most countries, including all EU countries, allow or even impose partial overlap and cumulation of IPRs.³¹⁸ There are three scenarios where IPRs overlap.³¹⁹ First, two (or more) rights may cover the entirety of the subject matter. Artistic works e.g. can be the domain of copyright, design, and trademarks. Second, the subject matters of the IPRs may overlap in part. This is the case with plant-related inventions that are protected by patents and plant breeders' rights.³²⁰ Third, an article may be protected by a range of IPRs, but each of them protects different aspects of the article; e.g. a product's aesthetic aspects are covered by design rights, its functional aspects by patents.³²¹ In the IoT, all three scenarios occur. There are instances where the two sets of IP laws will dictate clear rules

313 Lisa Diependaele, Julian Cockbain and Sigrid Sterckx, 'Raising the Barriers to Access to Medicines in the Developing World – The Relentless Push for Data Exclusivity' (2017) 17 *Developing World Bioethics* 11.

314 Enrico Bonadio and Filippo Fontanelli, 'Push for COVID-19 Vaccine Patent Waiver Isn't a Panacea: But It Could Nudge Companies to Share' (*The Conversation*, 12 May 2021) <<http://theconversation.com/push-for-covid-19-vaccine-patent-waiver-isnt-a-panacea-but-it-could-nudge-companies-to-share-160802>>.

315 Wilkof and Basheer (n 298) *ivi*.

316 E.g. the US Digital Millennium Copyright Act 1998 codified the approach to secondary liability of ISPs set forth in *Religious Technology Center v Netcom Online Communications Services* 907 F Supp 1361 (ND Cal, 1995) as noted by Chris Reed (ed), *Computer Law* (7th edn, OUP 2012) 460.

317 Derclaye and Leistner (n 298) 92.

318 Estelle Derclaye, 'Overlapping Rights' in Rochelle Dreyfuss and Justine Pila (eds), *The Oxford Handbook of Intellectual Property Rights* (OUP 2018) 629.

319 This distinction is adapted by Wilkof and Basheer (n 298).

320 The overlap is partial because patent protection is geared towards the methods to breed the plants, and the patentability of plants as such is excluded unless 'the technical feasibility of the invention is not confined to a particular plant or animal variety' (Directive 98/44/EC of 6 July 1998 on the legal protection of biotechnological inventions ('Biotech Directive') [1998] OJ L 213/13, art 4(2)).

321 David Musker, 'The Overlap between Patent and Design Protection' in Neil Wilkof and Shamnad Basheer (eds), *Overlapping Intellectual Property Rights* (OUP 2012) 23.

on mutual exclusion. This is not a common occurrence. Usually, interplay and demarcation rules are unclear and more than one IP law will apply.³²² The resulting overlaps can be criticised due to their leading to uncertainty and overprotection.³²³ Indeed, when overlaps occur – and in the IoT they are the rule rather than the exception – the ‘strictest regime overrides the more generous one.’³²⁴ In a context where the exceptions to the IPRs vary so greatly from one IP subsystem to another, this renders any strategy that centres on these exceptions unlikely to be successful, especially in an IoT world.

An in-depth analysis of IP overlaps is beyond the scope of this chapter. Three examples will suffice: (i) the cumulation of copyright and patents in protecting software, (ii) the troubled relationship between general copyright and special copyright in complex multimedia products, and (iii) the copyright-design interface.³²⁵ They are, at once, the most relevant from an IoT perspective and the most topical in current IP jurisprudence. A particularly fitting scenario regards the copyright-patent interface in the protection of software.³²⁶ At an international, European, and national level, attempts to draw a clear line between the domain of software copyright and software patents have not led to clarity.³²⁷ In Europe, software is excluded from patentability only ‘as such.’³²⁸ This criterion of prevention of overlaps becomes irrelevant in an IoT world, where the boundaries between software and hardware are blurred.³²⁹ In Europe, whilst there is a harmonized right to reverse engineer that users can invoke without the copyright holder’s permission,³³⁰ IoT companies may block it by qualifying it as patent

322 Araújo Sousa e Silva (n 298).

323 G Moschini and O Yerokhin, ‘The Economic Incentive to Innovate in Plants: Patents and Plant Breeders’ Rights’ in Jay P Kesan (ed), *Agricultural Biotechnology and Intellectual Property: Seeds of Change* (CAB International 2007) 161.

324 Derclaye (n 319) 622.

325 However, similar considerations apply to the other overlaps. E.g. most countries do not have rules to resolve the issue in the copyright-trademark overlap, and since these regimes diverge (trademark law providing more limited exceptions), the stricter regime will prevail over the other, whose exceptions will be practically unavailable (see Ellen Gredley and Spyros Maniatis, ‘Parody: A Fatal Attraction’ (1997) 19 EIPR 339.).

326 Although patent law has not been harmonised at the EU level, it will be analysed because the lack of harmonisation is a key factor to consider when analysing the problem created by IP overlaps. EU harmonisation of patent law, including the streamlining of exceptions, would benefit the IoT.

327 Andrew P Bridges, ‘Navigating the Interface Between Utility Patents and Copyrights’ in Neil Wilkof and Basheer (eds), *Overlapping Intellectual Property Rights* (OUP 2012) 6.

328 European Patent Convention, art 52(2)(c). ‘As such’ means that computer programs that produce a further technical effect and have therefore technical character are not excluded. In Europe, software patents claims are typically drafted as claims to a computer-implemented invention, that is, a method performed by a computer, computer network, or other programmable apparatus where one or more of the features of the invention is realised by means of a computer program. European Patent Office (n 22) G, II, 3.6.

329 Noto La Diega, ‘Software Patents and the Internet of Things in Europe, the United States and India’ (n 31).

330 Software Directive, art 6.

infringement³³¹ since the relevant defences have not been harmonised.³³² E.g. in the UK there is no reverse engineering defence in patent infringement proceedings.³³³ Equally, copyright holders' power to control derivative software is at odds with the right to patents derivative nonobvious inventions.³³⁴ More generally, there are fewer and divergent exceptions in patent law, and this allows patent law to override copyright exceptions.³³⁵ It has been noted that, consequently, software patent holders are in a stronger position compared to companies that hold copyright.³³⁶ However, it has been overlooked that IoT companies may at the same time be patent holders and copyright holders; accordingly, they can leverage their multiple IPRs to neutralise IP exceptions. Law and economics studies have shown that the copyright-patent overlap is overprotective, anticompetitive, and undesirable,³³⁷ with some commentators convincingly arguing for a resolution of the conflict by abolishing software copyright or significantly limiting its scope.³³⁸ More moderate proposals³³⁹ include a call for reconsidering the balance between freedom of use and protection of the right owner via a patent fair use defence that could be invoked irrespective of commercial motivations. A reform that would be necessary from an IoT perspective would be to make sure that patents and copyright provide for the same exceptions and that these are qualified as user rights.

The second scenario has to do with the relationship between software copyright and general copyright in multimedia products. The composite nature of Things has been mainly explored with regard to its amalgam of software, hardware,

331 When copyright and patents overlap, the infringement of the former will normally constitute an infringement also of the latter. Indeed, 'since copying copyright expressions includes copying the underlying ideas, the patent will typically be infringed' (Derclaye and Leistner (n 298) 93.).

332 In the UK e.g. there is a private use defence in patent infringement proceedings, but there is no homologous defence in copyright infringement proceedings (Patents Act 1977, s 60(5)(a); *BASCA* (n 179)). Conversely, in Austria there is no private use defence in patent infringement proceedings, but a copyright private use defence is available (Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Austria's Copyright Act), §§ 42, 42a, 42b; WIPO Standing Committee on the Law of Patents, 'Certain Aspects of National/Regional Patent Laws. Revised Annex II of Document SCP/12/3 Rev.2: Report on the International Patent System' (2020).).

333 Joachim Weyand and Heiko Haase, 'Patenting Computer Programs: New Challenges' (2005) 36 *IIC* 647, 653.

334 Gustavo Ghidini and Emanuela Arezzo, 'One, None or a Hundred Thousand: How Many Layers of Protection for Software Innovations?' in Josef Drexl (ed), *Research Handbook on Intellectual Property and Competition Law* (Edward Elgar 2008) 358.

335 Derclaye (n 319) 644.

336 Bridges (n 328) 16.

337 Christian Le Stanc, Gustavo Ghidini and Luis Mariano Genovesi, 'Logiciels Entre Droit d'Auteur et Brevet: Implications Juridiques et Economiques' in *Intellectual Property and Market Power* (Eudeba 2008) 309. However, there is no consensus on this, see Robert Hart, Peter Holmes and John Reid, 'The Economic Impact of Patentability of Computer Programs. Report to the European Commission' (2000) Intellectual Property Institute Study Contract ETD/99/B5-3000/E/106.

338 Le Stanc, Ghidini and Genovesi (n 338) 295; Ghidini and Arezzo (n 335) 372.

339 Martin Senftleben, 'Overprotection and Protection Overlaps in Intellectual Property Law – the Need for Horizontal Fair Use Defences' in Annette Kur and Vytautas Mizaras (eds), *The Structure of Intellectual Property Law: Can One Size Fit All?* (Edward Elgar 2011) 21.

service, and data. However, it goes beyond it. The analysis of *Tom Kabinet* has already shown that as e-books are composite products – computer programs and digitised literary works – the stronger protection afforded by general copyright law prevails, in that case rendering de facto irrelevant the principle of exhaustion on the basis of a non-IoT-friendly tangible-intangible dichotomy and an unjustifiably narrow interpretation of the concept of software.

Tom Kabinet is no isolated incident. In *Nintendo v PC Box*,³⁴⁰ for the claimant's video games and consoles to work, they would have to exchange encrypted information, thus 'recognising' each other and confirming that the game was not counterfeit. Although the nature of this pairing mechanism was contested, Nintendo regarded it as a form of technological protection measures. Their circumvention is forbidden under the Infosoc Directive.³⁴¹ The defendant manufactured devices that enabled video games other than Nintendo and Nintendo-licensed games to be played on the claimant's consoles. The latter accused the former of thusly circumventing their technological protection measures. The defendant put forward two contentions. First, Nintendo's 'locks' could not be regarded as a technological measure because they were present both in the hardware of the console and in the video games. This argument was rejected by the CJEU that accepted the advocate general's broad interpretation of technological protection measure as including the application of an access control or protection process, such as encryption, scrambling, or other transformation of the work or other subject matter or a copy control mechanism.³⁴² Importantly, this interpretation was supported by the observation that 'the principal objective of (the Infosoc Directive) is to establish a high level of protection in favour, in particular, of authors, which is crucial to intellectual creation.'³⁴³ Such an approach is at odds with a key tenet of copyright law, whereby copyright is a policy bargain, a delicate balance between the rightsholder's interests and competing private and public interests.³⁴⁴ The second contention that PC Box put forward was that Nintendo's true purpose was to prevent the use of independent software and to compartmentalise markets by rendering games purchased in one geographical zone incompatible with consoles purchased in another.³⁴⁵ The referring court itself had found that the effect of Nintendo's protective measures was not limited to allowing only Nintendo and Nintendo-licensed games to be played on Nintendo consoles; it 'prevented such games from being played on any other console, thus restricting interoperability and consumer choice.'³⁴⁶ Accordingly, PC Box's devices would favour independent software and the internal market in a way that was lawful under the Software Directive and

340 (n 171).

341 Art 6.

342 *Nintendo v PC Box* (n 171) [27].

343 *ibid* [27]

344 See e.g. Rebecca Tushnet, 'Intellectual Property as Public Interest Mechanism' in Rochelle Dreyfuss and Justine Pila, *The Oxford Handbook of Intellectual Property Law* (OUP 2018) 95.

345 *Nintendo v PC Box* (n 171) [24].

346 AG Sharpston in *Nintendo v PC Box* (n 171) [25].

aligned to the principle of free movement of goods. In particular, the defendant was relying on the decompilation exception;³⁴⁷ the decompilation was ‘confined to the parts of the programme strictly necessary in order to ensure interoperability between Nintendo consoles and “homebrew” games which did not infringe any copyright or related right.’³⁴⁸ The advocate general rejected this argument, and the CJEU followed suit. The starting point was that video games are complex multimedia products. Indeed, they constitute ‘complex matter comprising not only a computer program but also graphic and sound elements.’³⁴⁹ Since a video game is not (only) a computer program but is also a complex multimedia work, the Software Directive – and, with it, the decompilation exception – was seen as inapplicable. The advocate general argued that the Software Directive would take precedence over the Infosoc Directive ‘only where the *protected material falls entirely within the scope* of the former.’³⁵⁰ Such prevalence was justified by saying that, by reason of its exceptions, the protection afforded by the Software Directive is ‘slightly less generous’³⁵¹ than that which the Infosoc Directive affords. From this, the controversial inference was that where ‘complex intellectual works comprising both computer programs and other material are concerned – and where the two cannot be separated – . . . the *greater, and not the lesser, protection* should be accorded.’³⁵² Therefore, users of most Things could not rely on the Software Directive’s exceptions because Things are composite and cannot fall exclusively within the scope of this directive.

The prevalence of stronger proprietary regimes over weaker, user-focused regimes in the event of overlaps is open to criticism. The propertarianism that underpins this approach is incompatible with the public interest dimension of IP. The CJEU recognises that technological protection measures must be proportionate and that their circumvention cannot be invoked to ‘prohibit devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection.’³⁵³ However, the court bases this conclusion on the need to protect competitors’ private interests rather than on the public interest. Although *Nintendo v PC Box* illustrates the prevalence of stronger general copyright on weaker special regimes, whose exceptions are neutralised, it also indicates that external considerations – the imperatives of free market – can play a role in limiting IP excesses, at least in principle. The next section will delve into the drawbacks of the reliance on external limitations.

Similar overprotection issues can be seen when reflecting on the copyright-design interface. As seen in the preceding passages, Things may be protected by

347 Software Directive, art 6.

348 AG Sharpston in *Nintendo v PC Box* (n 171) [32].

349 *Nintendo v PC Box* (n 171) [23].

350 AG Sharpston in *Nintendo v PC Box* (n 171) [32].

351 *ibid* [35].

352 *ibid*.

353 *Nintendo v PC Box* (n 171) [30].

both rights. This is all the more true after recent EU cases *Cofemel*³⁵⁴ and *Brompton*.³⁵⁵ In the former,³⁵⁶ the court observed that the Berne Convention left it to the contracting parties to decide whether to exclude cumulative protection of designs under both copyright and registered designs (or industrial designs).³⁵⁷ However, the CJEU opined that ‘the EU legislature opted for a system in which the protection reserved for designs and the protection ensured by copyright are not mutually exclusive.’³⁵⁸ This conclusion is inferred from both the Design Directive and the Community Design Regulation, whereby a registered design can also be protected in other ways, including copyright.³⁵⁹ The court does not adequately account for the fact that design law leaves it to member states to decide the conditions under which this cumulation should operate, ‘including the level of originality required.’³⁶⁰ As to the Infosoc Directive, the argument appears even less convincing because it is based on Article 9, whereby this directive ‘shall be without prejudice to provisions concerning . . . design rights.’³⁶¹ Being without prejudice does not necessarily mean that EU law provides, let alone mandates, a cumulation of IPRs.

Even more recently, in the *Brompton Bicycle* case,³⁶² the CJEU held that copyright protects original functional shapes. This case is in line with the rise of the role of copyright in protecting the three-dimensional aspect of Things, as seen in prior paragraphs.³⁶³ Commentators have warned that ‘cumulation may have adverse effects if it is absolute and unrestricted in such a way as to become the norm.’³⁶⁴ With the IoT, cumulation is indeed becoming the norm. This is problematic because, on the one hand, IoT companies will be able to rely on copyright’s longer protection; on the other hand, copyright exceptions may be overridden by relying on design rights. Indeed, as there are far fewer exceptions in the design right regimes, this mismatch can adversely affect the public interest that permeates copyright exceptions. This was the case, e.g. in a decision of the Tribunal de Grande Instance of Paris,³⁶⁵ where the parody exception to copyright was deemed

354 (n 192).

355 C-833/18 *SI v Chedech/Get2Get* [2020] 6 WLUK 135.

356 (n 192).

357 Berne Convention, art 2(7).

358 *Cofemel* (n 192) [43].

359 Design Directive, art 17; Community Design Regulation, art 96.

360 Design Directive, art 17; Community Design Regulation, art 96(2).

361 Infosoc Directive, art 9.

362 (n 356).

363 We have seen the limits traditionally encountered by copyright when protecting 3D objects. A reflection on the impact of *Brompton Bicycle* (n 356) on the category of works of artistic craftsmanship is proposed by Neil Wilkof, ‘The CJEU *Brompton Bicycle* Case: A UK View’ (*The IPKat*, 5 July 2020) <<https://ipkitten.blogspot.com/2020/07/the-cjeu-brompton-bicycle-case-uk-view.html>>.

364 Daniel Inguanez, ‘A Refined Approach to Originality in EU Copyright Law in Light of the ECJ’s Recent Copyright/Design Cumulation Case Law’ (2020) 51 IIC 797.

365 TGI Paris, 18 March 2005 [2005] Propriétés Intellectuelles 339.

unavailable because of the cumulation with design rights. Thus, design law ends up overriding 'the public-regarding aspects of copyright law.'³⁶⁶

The problems created by IP overlaps to exception-focused strategies are exacerbated in the IoT, where the overlaps become ubiquitous. *De lege ferenda*, this brings further evidence to support a change in IP laws to better govern the relationships between IP subsystems and ensure convergence between the regimes of exceptions.³⁶⁷ Such convergence would be consistent with international law and, in particular, TRIPS and WTO case law.³⁶⁸ An open-ended exception along the lines of fair use – as opposed to enumerated and rigid exceptions – may provide an effective way to prevent clashes and avoid overprotection of IP.³⁶⁹ A study of the drafting history of the three-step test – whose narrow interpretation has led to the current EU approach to copyright exceptions – shows that the test can and ought to be regarded as a 'flexible formula (with) its roots in the Anglo-American copyright tradition.'³⁷⁰ Properly understood, based on the *travaux préparatoires* of the WIPO Copyright Treaty,³⁷¹ the three-step test would allow states to devise new exceptions that are fit for the IoT and for the digital environment more generally.³⁷² A new international treaty establishing a core of minimum mandatory IP exceptions would provide further guarantees, compared to an approach that relies on judicial interpretation of existing provisions. In this sense, I would welcome as a positive effort the International Instrument on Permitted Uses in Copyright Law,³⁷³ a project launched by the Max Planck Institute for Innovation and Competition in February 2021. If adopted, this treaty would counterbalance the traditional 'minimum protection' approach of international copyright law, and it would constitute a model that should be followed in other IP fields, else the problem of overlaps would not be resolved. A second-best and perhaps more pragmatic solution may be to retain the current approach and its reliance on exhaustive lists of exceptions, but either to provide the same exceptions across the board or to provide that the overlap will not prevent the application of all the exceptions that

366 Derclaye (n 319) 630.

367 Annette Kur, 'Harmonization of the Trademark Laws in Europe. An Overview' (1997) 28 IIC 1; Irene Calboli, 'Betty Boop and the Return of Aesthetic Functionality: A Bitter Medicine Against "Mutant Copyrights"?' (2014) 36 EIPR 80; Derclaye (n 319).

368 Senftleben (n 340).

369 A pragmatic solution may be to recognise that European fair use would lead to remuneration at least in some cases, as argued *ibid* 138.

370 *ibid* 8. The author refers to the observations submitted by the United Kingdom, Doc. S/13, *Records of the Intellectual Property Conference of Stockholm*, 11 June – 14 July 1967, Geneva: WIPO 1971, 630.

371 Agreed Statements concerning the WIPO Copyright Treaty adopted by the Diplomatic Conference on 20 December 1996, art 10.

372 The degree to which the three-step is flexible is contested because a fair use system is regarded as contrary to the first step of the test, namely, 'certain special cases.' See Herman Cohen Jehoram, 'Restrictions on Copyright and Their Abuse' (2005) 27 EIPR 359.

373 Reto M Hilty and others, 'International Instrument on Permitted Uses in Copyright Law' (2021) 52 IIC 62.

may come into play.³⁷⁴ A third option would be the clarification that, despite the divergence, each IP subsystem safeguards the other subsystems' exceptions. This was the approach of the proposed Directive on Computer-Implemented Inventions.³⁷⁵ This proposal is now defunct, but the IoT shows that a harmonised and balanced approach to the propertisation of software calls urgently for an EU intervention to prevent clashes and protect the public interest. Such an intervention should ensure the convergence between the regimes of exceptions so as to cover similar acts as well as being mandatory, binding, and include both commercial and noncommercial uses as long as they are fair. Since these processes of legislative harmonisation are slow, my hope is that human rights-infused interpretations of IP exceptions as proper user rights will prevail, thus achieving a more balanced and open approach to innovation governance.

This analysis shows the drawbacks of any attempts to find a solution to IP abuses within IP itself. Looking through the looking glass, external limitations could play a role in resolving the overlaps or at least reducing the clashes. We have seen above the slow and steady rise of freedom of expression to rebalance IP.³⁷⁶ Other external limitations may come from the principle of free competition, including free movement of goods and services.³⁷⁷ Whilst exceptions – as in-built

374 With regards to the copyright-patent interface in the protection of software, Gustavo Ghidini and Emanuela Arezzo, 'Dynamic Competition in Software Development: How Copyrights and Patents, and Their Overlapping, Impact on Derivative Innovation' (2013) 3 *Queen Mary Journal of Intellectual Property* 278. Similarly, with a call for a 'network of corresponding fair use limitations in different IP domains', Senfleben (n 340) 30.

375 Proposal for a Directive on the Patentability of Computer-Implemented Inventions (COM(2002)92 final – 2002/47(COD)) [23]: 'the exercise of a patent covering a computer-implemented invention should not interfere with the freedoms granted under copyright law to software developers by the provisions of the (Software) Directive.'

376 Although freedom of expression does not constitute, as such, a separate, open-ended defence in civil law, member states under *Funke Medien* (n 288), *Pelham* (n 289), and *Spiegel Online* (n 290). In the UK, alongside the statutory defences that mirror the Infosoc Directive and the Copyright in the Digital Single Market, there is an open-ended public interest defence whereby copyright infringement – and a breach of confidence – will not be enforced if the unauthorised use of the work or disclosure of the information was in the public interest, which includes freedom of expression. When freedom of expression is involved, interim injunctions are unlikely to be granted under *Kennard v Lewis* [1983] FSR 346. However, English courts tend to deny that the Human Rights Act 1998, implementing the ECHR, imposes a different interpretation of the CDPA (*Ashdown v Telegraph Group Ltd* [2001] RPC 34). Whilst they accept that they must have particular regard for freedom of expression, they interpret the limit as not necessarily meaning that 'injunctive or any other relief in respect of the copyright claim should be refused' (*Imutran Ltd v Uncaged Campaigns Ltd* [2002] FSR 2 [33]). Some commentators thought that the Infosoc Directive had killed the public interest defence in copyright infringement proceedings (William Cornish and David Llewelyn, *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (5th edn, Sweet & Maxwell 2003) [13.5].) However, there is evidence that the defence is alive and well (Alexandra Sims, 'The Public Interest Defence in Copyright Law: Myth or Reality?' (2006) 28 *EIPR* 335.), and the potential conflict with EU law has become less relevant with the UK's withdrawal from the EU.

377 Derclaye (n 319) 650. The author notes that other external mechanisms include the misuse doctrine (US), the theory of abuse of rights (civil law countries), and the doctrine of public interest (UK).

limitations to the powers of the IP holder – are of little help, a more successful strategy may rely on the EU fundamental freedoms of movement. A good illustration of this point can be found in *Parfums Christian Dior SA v Evora BV*,³⁷⁸ where the CJEU held that if the commercialisation of a product was lawful due to the exhaustion of the relevant trademarks, copyright could not be invoked to undermine the objectives of the single market.

I will therefore venture to test the potential of external limitations – and in particular of competition law – to curb IP excesses and counter the death of ownership in the IoT. Such potential, or lack thereof, is well illustrated by the antitrust control over the licensing of SEPs. This will be the focus of the next section.

6.6 Extra-IP Limitations: Are Standard Essential Patents on Fair, Reasonable, and Nondiscriminatory Terms IoT-FRANDly?

For IoT (inter)connectivity to work, standardisation is necessary. Standardisation bodies such as the European Telecommunications Standards Institute ('ETSI') require their members to commit to license their patents on fair, reasonable, and nondiscriminatory (FRAND) terms if they are essential to one of ETSI's standards. This mechanism is of utmost importance because it reduces the risk of litigation, thus incentivising the sharing of technologies and the growth of open, standardised, and interoperable innovation. For this system to work, it needs to be assisted by antitrust interventions to prevent SEP holders that are in a dominant position from abusing it by suing their technologies' implementers, despite their FRAND commitment. From this book's perspective, the reference to technology implementers is to be construed as referring to companies wanting to enter the IoT market. To untangle this complex issue, this section will focus on *Huawei v ZTE*³⁷⁹ and its aftermath, including the 2020 decision of the UK Supreme Court in *Unwired Planet International v Huawei*.³⁸⁰

A SEP is a patent that protects technology that is essential to a standard.³⁸¹ The anticompetitive relevance of licensing practices in the field of SEPs is the currently most-debated area of friction between IP and competition law as well as the most relevant competition law issue in IoT regulation.³⁸² Although, in general,

378 Case C-337/95 [1997] ECR I-6013 [58].

379 Case C-170/13 *Huawei Technologies Co Ltd v ZTE Corp* [2015] Bus LR 1261.

380 *Unwired Planet International Ltd and another v Huawei Technologies (UK) Co Ltd and another* [2020] UKSC 37.

381 European Commission, 'Communication "Setting out the EU Approach to Standard Essential Patents"' (2017) COM/2017/712 final 1.

382 Jason R Bartlett and Jorge L Contreras, 'Rationalizing FRAND Royalties: Can Interpleader Save the Internet of Things' (2017) 36 *Review of Litigation* 285; Beatriz Conde Gallego and Josef Drexler, 'IoT Connectivity Standards: How Adaptive Is the Current SEP Regulatory Framework?' (2019) 50 *IIC-IIC* 135; Luke McDonagh and Enrico Bonadio, 'Standard Essential Patents and the Internet of Things' (2019) *European Parliamenti (JURI)*; Rupperecht Podszun, 'Standard Essential Patents and Antitrust Law in the Age of Standardisation and the Internet of Things: Shifting

it is still 'controversial whether the (IP)-antitrust interface should be viewed as a conflict or a finalistic convergence,'³⁸³ it would seem that from the viewpoint of SEP abuses, IP and competition law diverge. Engaging with SEPs is pivotal to understanding the economic relevance of patents more generally, as SEPs are the most valuable type of patents. Indeed, they are more frequently traded, more frequently litigated, more frequently renewed, and more frequently cited as prior art compared to non-SEP patents.³⁸⁴

If SEPs are not adequately governed, IoT standardisation cannot be achieved. It is not an exaggeration to say that '[w]ithout access to SEPs the whole IoT would not work.'³⁸⁵ European organisations play an active role in the development of standards. As seen in Chapter 1, standardisation is a form of self-regulation of the IoT. European standard setting 'may serve to ameliorate the problems of overlapping IPRs in those industries in which IP is most problematic for innovation, particularly semiconductors, software, and telecommunications,'³⁸⁶ that is, the sectors that are key to the IoT. Under the EU Standardisation Regulation, a standard consists of technical specifications, 'adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory.'³⁸⁷ A technical specification, in turn, is a document that prescribes technical requirements to be fulfilled by a product, process, service, or system.³⁸⁸ The most important of these requirements, especially from an IoT perspective, is the laying down of the characteristics required of a product and of a service, including levels of quality, performance, and interoperability.³⁸⁹ There are several standard-developing organisations, from the international level through the European level to the national one.³⁹⁰ The European standardisation organisations are the European Committee for Standardisation (CEN), the European Committee

Paradigms' (2019) 50 IIC 720; Francesca Gennari, 'Internet Protocol Standards for IoT Interoperability in the House. Open Issues in EU Competition Law' in Carlos A Iglesias and others (eds), *Intelligent Environments 2020* (IOS 2020) 95.

383 Giuseppe Colangelo and Roberto Pardolesi, 'Intellectual Property, Standards, and Antitrust: A New Life for the Essential Facilities Doctrine? Some Insights from the Chinese Regulation' in Gustavo Ghidini, Hanns Ullrich and Peter Drahos (eds), *Kritika: Essays on Intellectual Property*, vol 2 (Edward Elgar 2017).

384 Tim Pohlmann and Knut Blind, 'Landscaping Study on Standard Essential Patents (SEPs)' (2016) IPlytics GmbH and TU Berlin 2.

385 Podszun (n 385) 730.

386 Mark A Lemley, 'Intellectual Property Rights and Standard-Setting Organizations' (2002) 90 California Law Review 1889, 1892.

387 Regulation (EU) No 1025/2012 of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC [2012] OJ L 316/12, art 2(1).

388 Standardisation Regulation, art 2(4).

389 Standardisation Regulation, art 2(4)(a), (c).

390 'International standardisation body' means the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunication Union (ITU). The UK's national standardisation body is the British Standards Institution (BSI).

for Electrotechnical Standardisation (Cenelec), and the ETSI.³⁹¹ The focus of this section will be on the latter because *Huawei v ZTE*³⁹² – the leading EU authority on SEPs – regards a standard adopted by ETSI.

In their ensuring interoperability, connectivity, and safety of technologies, standards are pivotal to the IoT.³⁹³ These standards frequently refer to technologies that are protected by patents. A patent is essential to a standard ‘if it is not possible on technical grounds to make equipment which complies with the standard without infringing the intellectual-property right.’³⁹⁴ Examples of SEPs that are instrumental to the IoT include patents on Wi-Fi and Bluetooth. More than 23,500 patents have been declared essential to GSM and 3G.³⁹⁵ Thanks to the 5G standard, currently being developed, users will enjoy interoperable, high-performance, and affordable Things.³⁹⁶ The share of declared SEPs from Chinese and Korean companies has been growing over time, reflecting their role in the telecommunications sector and the global economy more generally.³⁹⁷ With currently 334,680 SEPs,³⁹⁸ standardised patented technologies make interconnectivity, and therefore the IoT, a reality.

IoT companies face a dilemma. In order to maximise the potential for value extraction, they may be inclined to exclude everyone from their closed proprietary systems. This strategy risks transforming the IoT into a noninteroperable ‘Internet of Silos’; without seamless data flows and interoperability, the IoT will fail – and proprietary IoT companies will fail with it. However, the prospect of licensing patents that are essential to standards on an industry-wide scale provides an incentive for patent holders not to leverage their monopolies to prevent the standards from being available to all for public use.³⁹⁹ To this end, ETSI and other standard setting organisations develop IP policies, demanding that their members declare whether their patented invention is essential to a standard and commit to licensing it on FRAND terms.⁴⁰⁰ Other standard-developing organisations do not require their members to commit to a license at all; others require default license commitments under royalty-free terms or non-assertion agreements. A limited number

391 Annex I to the Standardisation Regulation.

392 (n 380).

393 CEN and Cenelec, ‘Standard Essential Patents and Fair, Reasonable and Non-Discriminatory (FRAND) Commitments’ (2016); European Commission, ‘Communication “Setting out the EU Approach to Standard Essential Patents”’ (n 384).

394 ETSI IPR Policy, Clause 15.6.

395 Alison Jones, ‘Standard Essential Patents: FRAND Commitments, Injunctions and the Smartphone Wars’ (2014) 10 *European Competition Journal* 5.

396 Frederik Nilsson, ‘Appropriate Base to Determine a Fair Return on Investment: A Legal and Economic Perspective on FRAND’ [2017] *GRUR International* 1017.

397 Pohlmann and Blind (n 387) 1.

398 ETSI’s database <<https://ipr.etsi.org/>>.

399 Chryssoula Pentheroudakis and Justus A Baron, ‘Licensing Terms of Standard Essential Patents. A Comprehensive Analysis of Cases’ (2017) *RC Science for Policy Report EUR 28302 EN* 10.

400 See e.g. ETSI Intellectual Property Rights Policy, Annex 6 to Rules of Procedure, 4 December 2019.

of organisations rely on patent pools.⁴⁰¹ The focus of this section is on the ETSI model. Once a standard is established and the holders of the relevant SEPs commit to license them on FRAND terms, the technology included in the standard should be available to any potential user of the standard. What is FRAND – especially which royalties are fair and reasonable – is open to debate. The vagueness of these concepts made commentators observe that '[w]ithout some idea of what those terms are, reasonable and non-discriminatory licensing loses much of its meaning.'⁴⁰² Whilst SEP holders allege that technology users free ride on their innovation, there is evidence that the former charge excessive licensing fees based on weak patent portfolios and use litigation threats as a negotiation tool.⁴⁰³ This conflict is worsened in the IoT in light of the relational black box as presented in Chapter 1. As noted in a European Commission report, the evolution of the IoT, with its need for wider connectivity, has led to a variety of SEP owners and implementers with different business models and to greater diversity of licensing practices.⁴⁰⁴ The IoT's diversity is exemplified by the large numbers of alliances and consortia that try to shape IoT standardisation, e.g. the Industrial Internet Consortium, Open Interconnect, Thread, and Allseen.⁴⁰⁵ This diversity is making it 'more difficult to identify a consensual interpretation of FRAND licensing principles,'⁴⁰⁶ which is in turn leading to a proliferation of disputes that can be framed as patent holdup. *Patent holdup* refers to the practice of waiting for a company to include a standardised technology in their products and either seeking remedies or imposing a settlement because, once the technology has been implemented, 'it is too late for the company to change course.'⁴⁰⁷ The most common form of patent holdup is when patent holders that had made FRAND commitments seek injunctive relief to exclude willing licensees.⁴⁰⁸ Another IoT-related issue is that it is not clear whether SEP holders can decide to demand that the licensee be the end-product manufacturer as opposed to the supplier of the relevant component. In November 2020, the Düsseldorf Regional Court asked this question to the CJEU in *Nokia v Daimler*,⁴⁰⁹ as Nokia refused to license its SEP to the suppliers of connectivity components for connected cars and required to license it only to car manufacturer

401 Pohlmann and Blind (n 387) 2.

402 Lemley (n 389) 1891.

403 European Commission, 'Communication "Setting out the EU Approach to Standard Essential Patents"' (n 384) 2.

404 Pentheroudakis and Baron (n 403) 10.

405 Aref Meddeb, 'Internet of Things Standards: Who Stands out from the Crowd?' (2016) 54 IEEE Communications Magazine 40.

406 Pentheroudakis and Baron (n 403) 10.

407 Colleen V Chien, 'Holding Up and Holding Out' (2014) 21 Michigan Telecommunications & Technology Law Review 1.) In other words, holdup arises when a patent owner extracts 'a larger royalty ex post than it could have obtained in an arm's length transaction ex ante' (Thomas F Cotter, Erik Hovenkamp and Norman Siebrasse, 'Demystifying Patent Holdup' (2019) 76 Washington & Lee Law Review 1501.).

408 Sonia Kuester Pfaffenroth, Peter J Levitas and Dylan S Young, 'DOJ Changing Its Antitrust Approach to FRAND and SEPs' (2019) 31 IP & Technology Law Journal 1.

409 LG Düsseldorf, 26 November 2020–4c O 17/19 [2021] MMR 276.

Daimler. As Things are inherently composite, and in light of the relational black box, it is to be hoped that the CJEU decides in favour of Daimler. Indeed, to allow SEP holders to require a license at every level of the supply chain would be in violation of both the principle of exhaustion and Article 102 TFEU.

In the US, the prevalent approach is that SEP enforcement – including patent holdup and injunctions against technology users – should not be regarded as an antitrust violation.⁴¹⁰ There seems to be some divergence between the Department of Justice, against antitrust interventions in these scenarios, and the Federal Trade Commission (FTC), more open to them.⁴¹¹ However, *FTC v Qualcomm*,⁴¹² a case that the FTC was using to affirm the antitrust relevance of SEP abuses, has been adjudicated in favour of the modem chips monopolist.⁴¹³ Although in theory in the EU the antitrust relevance of SEP abuses is not contested, in practice the reasons of property tend to prevail. This means that the distance between the US and the EU is more apparent than real. This also means that the death of ownership does not equate to the death of property. The right to property is as strong as it has always been, as illustrated by *Huawei v ZTE*.⁴¹⁴

Huawei v ZTE deserves a closer look for a twofold reason. First, it is the leading EU authority in the field of antitrust control over SEP licensing.⁴¹⁵ Second, it exemplifies the CJEU's habit to, on the one hand, declare that IP must be balanced with other fundamental rights under the Charter of Fundamental Rights of the EU and the ECHR and, on the other hand, to refer to fundamental rights as a mere rhetoric device to strengthen 'already strong IP protection.'⁴¹⁶ This ruling directly

410 See Terrell McSweeney, 'Holding the Line on Patent Holdup: Why Antitrust Enforcement Matters' (*FTC*, 21 March 2018) <www.ftc.gov/public-statements/2018/03/holding-line-patent-holdup-why-antitrust-enforcement-matters>.

411 Kuester Pfaffenroth, Levitas and Young (n 412).

412 *Federal Trade Commission v Qualcomm Incorporated*, No 19–16122, D.C. No 5:17-cv-0020-LHK (9th Cir., August 11, 2020).

413 The FTC contended that Qualcomm violated the Sherman Act, 15 U.S.C. §§ 1, 2, by unreasonably restraining trade in and unlawfully monopolising the code division multiple access (CDMA) and premium long-term evolution (LTE) cellular modern chip markets. The breach of the SEP commitments played an important role in this conduct.

414 (n 380); Roberto Grasso, 'Selected Issues in SEP Licensing in Europe: The Antitrust Perspective' in Ashish Bharadwaj, Vishwas H Devaiah and Indranath Gupta (eds), *Complications and Quandaries in the ICT Sector: Standard Essential Patents and Competition Issues* (Springer 2018) 79.

415 Timothy McIver, Andrea Pomana and Judith Schmidt, 'Between Patent Protection and Abuse of Dominance: Highest EU Court Issues Landmark Decision on Standard-Essential Patents' (2015) 36 ECLR 533; Markus Gamp, 'Huawei v ZTE – CJEU Landmark Decision Provides New Ground Rules for Asserting Standard-Essential Patents in Europe.' (2015) 31 CLS Rev 810; Reto M Hilty and Peter R Slowinski, 'Standardessentielle Patente – Perspektiven außerhalb des Kartellrechts' (2015) 64 GRUR International 781.

416 Tuomas Mylly, 'The Constitutionalization of the European Legal Order: Impact of Human Rights on Intellectual Property in the EU' in Christophe Geiger (ed), *Research Handbook on Human Rights and Intellectual Property* (Edward Elgar 2015) 104. *Contra*, Peter Oliver and Christopher Stothers, 'Intellectual Property Under the Charter: Are the Court's Scales Properly Calibrated?' (2017) 54 Common Market Law Review 517, 564.

impacts the extent to which external limitations can be invoked to re-empower the IoT user affected by the death of ownership.

Amongst other SEPs, Huawei owns the patent ‘Method and apparatus of establishing a synchronisation signal in a communication system’⁴¹⁷ and notified it to ETSI as essential to ‘Long Term Evolution,’ a wireless broadband communication standard.⁴¹⁸ This notification included, as per ETSI’s IPR Policy, the commitment to license the patent on FRAND terms.⁴¹⁹ ZTE, the defendant, marketed products equipped with software linked to the aforementioned standard. Therefore, they engaged in negotiations with Huawei by indicating the royalty which they considered fair and reasonable to reach a cross-licensing agreement.⁴²⁰ Although the agreement was not finalised, ZTE kept marketing the products at issue. It followed that Huawei brought an action for infringement seeking a prohibitory injunction, account of profits, delivery-up, and damages.⁴²¹ The Landgericht Düsseldorf (Court of First Instance) decided to stay the proceedings and ask the CJEU whether Huawei’s conduct qualified as an abuse of dominant position under Article 102 TFEU. Such an abuse occurs when a dominant undertaking resorts to methods different from those governing normal competition, thus (i) hindering the maintenance of the degree of competition still existing in the market where competition is weakened because of the presence of the dominant undertaking, or (ii) hindering the growth of that competition.⁴²² A dominant position is:

[A] position of *economic strength* enjoyed by an undertaking which enables it to *prevent effective competition* being maintained on the relevant market by affording it the power to *behave to an appreciable extent independently* of its competitors, customers and ultimately of its consumers.⁴²³

On the abusive qualification of Huawei’s conduct, two views could be taken. On the one hand, in line with the European Commission’s position in *Samsung/UMTS*,⁴²⁴ to seek an injunction when the defendant shows willingness to negotiate a license would constitute an abuse of dominant position, regardless of whether the parties could not agree on the content of certain clauses in the licensing agreement,

417 European Patent EP 2090050 B 1/.

418 LTE is a standard for wireless broadband communication for mobile devices and data terminals. See ‘ETSI – 4G – Long Term Evolution’ (ETSI) <www.etsi.org/technologies/mobile/4g>.

419 *Huawei v ZTE* (n 380) [22]; ETSI Intellectual Property Rights Policy, Clause 6.1.

420 *Huawei v ZTE* (n 380) [23], [24].

421 EPC, art 64, on the rights of the European patent owner and the applicability of national law to infringement proceedings; Patentgesetz (PatG or Germany’s Patent Act), § 139 on the injunction (*Unterlassung*).

422 Case 85/76 *Hoffmann-La Roche v Commission* [1979] ECR 461 [91].

423 *ibid* [38].

424 Case AT.39939 *Samsung C(2014)2891* final [2014] OJ C 350/8. Samsung had sought injunctive relief in various member states’ courts against competing mobile device makers based on alleged infringements of certain of its patent rights which it has declared essential to implement European mobile telephony standards.

including the royalty.⁴²⁵ On the other hand, the Bundesgerichtshof (Germany's Federal Court of Justice)⁴²⁶ held that this conduct would be abusive only under certain circumstances. First, the defendant must have made an unconditional offer to conclude a licensing agreement not limited exclusively to cases of infringement. Second, the defendant must account for past acts of use and to pay the sums resulting therefrom.⁴²⁷ The first view relied on a pro-competitive approach to IP, the second view, a pro-proprietary one. The CJEU decided to espouse the latter approach on the following grounds.

As *Volvo*,⁴²⁸ *Magill*,⁴²⁹ and *IMS Health*⁴³⁰ exemplify, it is settled case law that the exercise of an IP can qualify as an abuse of dominant position in 'exceptional circumstances.'⁴³¹ The essential facility doctrine⁴³² set forth in these cases means that a refusal to grant an IP licence may constitute an abuse when:

- (i) The undertaking requesting a licence intends to offer new products for which there is potential consumer demand;
- (ii) No objective considerations justify a refusal to license;
- (iii) Through the refusal, the IP holder reserves the market to itself, thus eliminating all competition.⁴³³

The difference between this jurisprudence and the current dispute does not escape the court. First, SEPs are, by definition, 'essential,' as opposed to normal patents, in which case excluded third parties can 'manufacture competing products

425 The Commission accepted legally binding commitments by Samsung whereby the company will not seek injunctions in Europe on the basis of its SEPs for smartphones and tablets against licensees who sign up to a specified licensing framework. Under this framework, any dispute over what are FRAND terms for the SEPs in question will be determined by a court, or, if both parties agree, by an arbitrator. Thus, 'Samsung will not be able to seek injunctions on the basis of its Mobile SEPs against any potential licensee willing to enter into a licence agreement on FRAND terms and conditions' (*Samsung* (n 425) [19]).

426 Urteil 6 May 2009 – KZR 39/06 (*Orange Book*).

427 *Huawei v ZTE* (n 380) [30]–[33].

428 Case 238/87 *Volvo AB v Erik Veng (UK) Ltd* [1988] ECR 6211 about the refusal by the proprietor of a registered design to grant to third parties a licence for the supply of parts.

429 Joined Cases C-241/91 P and C-242/91 P *Radio Telefis Eireann v Commission* [1995] ECR I-743 on the refusal to grant a copyright licence regarding TV guides in Ireland.

430 C-418/01 *IMS Health v NDC Health* [2004] ECR I-5039 about the refusal to grant a copyright licence regarding a database.

431 *Volvo* (n 429) [9]; *Magill* (n 430) [50]; *IMS Health* (n 431) [35].

432 This doctrine was developed with regards to the owners of physical facilities or infrastructure, although it can apply to intangible facilities, such as IP. Pursuant to this doctrine, the owner may, by virtue of this facility or infrastructure, have a dominant position on a market, and the refusal to give access to it to competitors on nondiscriminatory terms may constitute an abuse under Article 102 TFEU. See *Sealink/B&I* [1992] 5 CLMR 255.

433 See Thomas F Cotter, 'Intellectual Property and the Essential Facilities Doctrine' (1999) 44 *The Antitrust Bulletin* 211; Roberto Pardolesi and Massimiliano Granelli, 'Licenza Obbligatoria Ed Essential Facilities Nell'antitrust Comunitario' (2004) 2 *Riv dir ind* 323; Colangelo and Pardolesi (n 386).

without recourse to the patent concerned and without compromising the essential functions of the product in question.⁴³⁴ It follows that SEP holders can prevent competitors' Things from appearing or remaining on the market and reserve to themselves their manufacture. Second, FRAND commitments create a legitimate expectation that the SEP holder will grant a FRAND licence. Therefore, 'a refusal by the proprietor of the SEP to grant a licence on those terms may, in principle, constitute an abuse.'⁴³⁵ This defence can be raised in infringement proceedings if the claimant refuses to grant a FRAND licence. There is disagreement, however, as to what is required for a term to be FRAND.

To resolve the disagreement as to the meaning of 'FRAND,' *Huawei v ZTE* set forth a procedure that the parties must comply with to achieve a fair balance of interests. In elaborating on the balance, the CJEU referred to the EU Charter of Fundamental Rights and, in particular, to Article 17(2) on the protection of IP and Article 47 on the right to an effective remedy. Both rights can be invoked by the SEP holder against technology implementers. Surprisingly, the court ignores the competing fundamental rights that could play a role in rebalancing the protection of IP. In particular, the right to conduct a business,⁴³⁶ the right to consumer protection,⁴³⁷ and freedom of expression.⁴³⁸ Similarly, the ruling disregards that, whilst protecting property, the charter recognises that the law can limit it on public interest grounds.⁴³⁹ One may object that the public interest limitation is expressly stated with regard to property, and it is not repeated in paragraph 2 that cryptically provides, 'Intellectual property shall be protected.'⁴⁴⁰ However, the rules on property are increasingly applied to IP, at least by analogy.⁴⁴¹ *Luksan*⁴⁴² e.g. referred not only to Article 17(2) but also to the first paragraph of the provision, whereby one may be deprived of one's possessions, if this is in the public interest. If one rejects the qualification of IP as property, limitations would nonetheless stem from Articles 52 and 54 of the EU Charter. Under the former, limitations to the Charter rights may be made if they are proportionate, necessary, and 'genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.'⁴⁴³ In *ZZ (France)*,⁴⁴⁴ the CJEU confirmed that

434 *Huawei v ZTE* (n 380) [50].

435 *ibid* [53].

436 EU Charter, art 16. The AG himself had noted that a SEP injunction 'places a significant restriction on (the freedom to conduct business) and is therefore capable of distorting competition' (Opinion of AG Wathelet in *Huawei v ZTE* (n 380) [59]). The CJEU overlooked this point.

437 EU Charter, art 38.

438 EU Charter, art 11.

439 EU Charter, art 17(1).

440 See Christophe Geiger, 'Intellectual Property Shall Be Protected!?' Article 17 (2) of the Charter of Fundamental Rights of the European Union: A Mysterious Provision with an Unclear Scope' (2009) 31 EIPR 113.

441 Opinion of AG Wathelet in *Huawei v ZTE* (n 380) [66], fn 41; *R. (on the application of British American Tobacco UK Ltd) v Secretary of State for Health* [2016] EWCA Civ 1182.

442 Case C-277/10 *Martin Luksan v Petrus van der Let* [2013] ECDR 5 [68].

443 EU Charter, art 52(1).

444 Case C-300/11 *ZZ (France) v Secretary of State for the Home Department* [2013] QB 1136.

Article 52 permits limitations on the exercise of the right to an effective remedy.⁴⁴⁵ This right includes the right to an injunction.⁴⁴⁶ The advocate general in *Huawei* confirmed that this provision can be leveraged also to introduce limitations to IP, although this point was overlooked by the court.⁴⁴⁷ The right to conduct business, consumer protection, and freedom of expression can justify limitations either as 'general interest' or as 'rights and freedoms of others.' Under Article 54 of the Charter, the abuse of rights is prohibited. This doctrine is popular in civil law jurisdictions, and it prevents rightsholders from using their rights to impinge in third parties' rights to a greater extent than provided by the law.⁴⁴⁸ This means that SEP holders cannot weaponise their IP to engage in activities aimed at the limitation of the Charter rights and freedoms beyond what the Charter allows.⁴⁴⁹ None of these considerations figure in the court's reasoning, which – whilst declaring the importance of a fair balance – focused only on the proprietary interests of the SEP holder. Indeed, the CJEU used the Charter to argue that a high level of IP protection and effective enforcement must be ensured. Accordingly, it held the fact that any use of the patent must be preceded by a license and that FRAND commitments 'cannot negate the substance of the rights guaranteed to that proprietor.'⁴⁵⁰ This is not an isolated incident. A recent analysis of the EU case law has indeed showed that 'Article 17(2) (is) essential in order to strengthen the discipline of intellectual property protection.'⁴⁵¹ It could be said that the more user ownership dies, the more the right to property thrives. In an IoT world, where standards are vital and each comprises countless SEPs, this imbalanced stance is not socially just as it prevents smaller IoT business and newcomers from entering the market while reducing consumer freedoms.

In *Huawei v ZTE*, the CJEU does not regard Article 102 as a source of fundamental rights that the defendant could rely on. Instead, it regards it as the source

445 This was also noted by the AG, who, however, seemed to give more importance to the right of access to the courts rather than Article 52, despite the statement of principle whereby 'the Charter does not create a hierarchy among the fundamental rights which it recognises' (Opinion of AG Wathelet in *Huawei v ZTE* (n 380) [67]).

446 Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH* [2014] Bus LR 541 [63].

447 Opinion of AG Wathelet in *Huawei v ZTE* (n 380) [66], fn 41, that refers, by analogy, to Case 44/79 *Hauer v Land Rheinland-Pfalz* [1979] ECR 3727, where it was held that the interference in the right to property stemming from the EU rules that had prevented a German citizen from planting new vines on her land were justified in the public interest.

448 In Scots law, that is a mixed common-civil law system, the *aemulatio vicini* – a doctrine aimed at preventing neighbours from abusing their property rights (e.g. by depriving them of light in *Ross v Baird* (1829) 7 S 361) – can be regarded as a limited abuse of rights doctrine. See Elspeth Reid, 'Strange Gods in the Twenty-First Century: The Doctrine of Aemulatio Vicini' in Elspeth Reid and David Carey Miller (eds), *A Mixed Legal System in Transition: T. B. Smith and the Progress of Scots Law* (EUP 2005) 239.

449 EU Charter, art 54.

450 *Huawei v ZTE* (n 380) [59].

451 Alain Strowel, 'Copyright Strengthened by the Court of Justice Interpretation of Article 17(2) of the EU Charter of Fundamental Rights' in Oreste Pollicino, Giovanni M Riccio and Marco Bassini (eds), *Copyright and Fundamental Rights in the Digital Age* (Edward Elgar 2020) 28.

of a limited obligation for the SEP holder to ‘comply with specific requirements when bringing actions against alleged infringers.’⁴⁵² Therefore, it would constitute an abuse if the SEP holder brought an action for a prohibitory injunction or for the recall of products ‘without notice or prior consultation with the alleged infringer,’⁴⁵³ regardless of whether the latter has already used the SEP. Instead of the flexible and balanced approach of the European Commission in *Samsung*⁴⁵⁴ and its focus on the defendant’s willingness to negotiate, the court opts for a rather-rigid and imbalanced step-by-step procedure that the parties are expected to follow to escape liability (the ‘*Huawei* protocol’). The steps are as follows.

- (i) The SEP holder has to alert the technology implementer of the alleged infringement by identifying the SEP and specifying the way in which it has been infringed.⁴⁵⁵
- (ii) It is for the alleged infringer to express its willingness to conclude a licensing agreement on FRAND terms.⁴⁵⁶
- (iii) The SEP holder has to present a specific written offer for a FRAND licence, in accordance with the undertaking given to the standardisation body. This has to include the amount of the royalty and how it has been calculated.⁴⁵⁷ The court justifies this by noting that the SEP holder has access to previous agreements and is better placed to check whether the offer is nondiscriminatory.⁴⁵⁸ *De lege ferenda*, it would be important that transparency is ensured: if these agreements were to be made public, the implementer would be in a better position to judge which terms are nondiscriminatory.
- (iv) The implementer has to respond to the offer diligently, in accordance with recognised commercial practices in the field, and in good faith. Delaying tactics would be expression of bad faith.⁴⁵⁹ In case of nonacceptance, the counteroffer must be prompt, specific, in writing, and FRAND.⁴⁶⁰
- (v) If the rightsholder rejects it, the alleged infringer has to provide appropriate security to cover for the past acts of use of the SEP, and an account must be rendered of those acts.
- (vi) Optionally, an independent third party will be appointed to determine the amount of the royalties.⁴⁶¹

It is for national courts to refer to the criteria of the so-called *Huawei* protocol ‘insofar as they are relevant, in the circumstances, for the purpose of resolving

452 *ibid* [59].

453 *ibid* [60].

454 (n 425).

455 *Huawei v ZTE* (n 380) [61, [62].

456 *ibid* [63].

457 *ibid*.

458 *ibid* [64].

459 *ibid* [65].

460 *ibid* [66].

461 *ibid* [68].

the dispute.⁴⁶² The decision of the CJEU is affected by the drawbacks of the positions of both the European Commission and the Bundesgerichtshof. On the one hand, it is affected by the same lack of certainty of the former, as the criteria set forth appear to be of merely advisory nature.⁴⁶³ This was confirmed in *Unwired Planet v Huawei*,⁴⁶⁴ where the UK Supreme Court was asked whether courts should refuse to grant a SEP injunction on grounds of noncompliance with the *Huawei* protocol. The Supreme Court rejected ‘the argument that the CJEU’s scheme was mandatory.’⁴⁶⁵ On the other hand, the ruling of the CJEU is affected by the lack of flexibility of the German approach, as it focuses on a step-by-step procedure rather than the open formula of the willingness to negotiate. On a positive note, *Huawei v ZTE* shows that the ‘exceptional circumstances’ required by the essential facility doctrine⁴⁶⁶ do not apply to SEP licensing, which means that, compared to the IP-competition conflict resolved under *Volvo*,⁴⁶⁷ *Magill*,⁴⁶⁸ and *IMS Health*,⁴⁶⁹ the defendant is more likely to escape liability. This is important because the essential facility doctrine requires the identification of a new product that could be produced by accessing the facility, but in IoT markets that rely on large quantities of industrial data, it is extremely difficult for the potential licensor to even imagine what the new product would look like. Indeed, to imagine it, they would need access to the IoT data that constitute the essential facility.⁴⁷⁰

As the case law stands, *Huawei* has ‘blunted the sword of antitrust law,’⁴⁷¹ and it is not by chance that, after *Huawei*, the European Commission has not intervened to temper patent abuses. This is in line with the Competition Commissioner’s statement whereby ‘the best way to solve those issues is sometimes to change the regulations, not to apply the competition rules.’⁴⁷² This stance further strengthens the case for the need of an EU harmonisation of patent law to set forth a single and balanced framework for SEP licensing without the need for competition law interventions that do not appear to be fit for the IoT. Such a harmonised framework would centre on the adoption of the ‘willingness to negotiate’ doctrine, the clear

462 *ibid* [70].

463 *Huawei* has also been interpreted as setting forth ‘strict obligations’ (Enrico Bonadio and Luke McDonagh, ‘2020 Is Set to Be a Crucial Year for Standard-Essential Patent Litigation in Europe’ (*Kluwer Patent Blog*, 17 January 2020) <<http://patentblog.kluweriplaw.com/2020/01/17/2020-is-set-to-be-a-crucial-year-for-standard-essential-patent-litigation-in-europe/>>).

464 (n 381).

465 *ibid* [158].

466 These are the conditions to be met: (1) the potential licensor intends to offer a new product on a secondary market, (2) lack of objective justification for the refusal to license, (3) the refusal reserves a secondary market by eliminating all competition on that market, and (4) the product or service is indispensable for enabling the undertakings to carry on business in a particular market.

467 (n 429).

468 (n 430).

469 (n 431).

470 *Drex1* (n 47).

471 *Podszun* (n 385) 729.

472 Margrethe Vestager cited *ibid*.

definition of FRAND terms, and the streamlining of exceptions, ideally modelled on fair use.

Future research should critically assess if the Competition Commissioner's caution is to be applauded, considering how national courts are interpreting *Huawei*. At a cursory look, it would seem that domestic approaches are converging in assuring a pro-proprietary application of *Huawei*. The UK Supreme Court in *Unwired Planet* declared English courts' jurisdiction to determine a FRAND global licence for a multinational SEP portfolio. An approach sensitive to the necessity to strike a balance between IP and competing interests would have led to the clarification that the market value should not be the be-all and end-all of royalty determination when SEPs are involved. Instead, the Supreme Court imposed 'fair market price'⁴⁷³ to technology implementers.⁴⁷⁴ The pro-monopolist favour is also confirmed by the fact that the court regarded damages inadequate, opting for an injunction – a discretionary remedy that constitutes an indirect form of specific performance.⁴⁷⁵ They did so on the untested assumption that compensation would give implementers an incentive to hold out country by country until compelled to pay damages in each country.⁴⁷⁶ This preference for 'property rules' (injunction) over 'liability rules' (damages) well illustrates the imbalance of the SEP framework.⁴⁷⁷ Similarly, Germany's Supreme Court⁴⁷⁸ held that (i) a willing licensee is one who is willing to accept a license on FRAND terms, however FRAND may be construed, and (ii) *nondiscriminatory* does not mean that the rate should be the same as previous comparable agreements. Finally, in the Netherlands, the Court of Appeal of The Hague granted injunctions allowing Philips to stop alleged infringements by Asus and Wiko and reiterated that the *Huawei* protocol is not binding.⁴⁷⁹

473 *Unwired Planet* (n 381) [114].

474 A similar evolution can be seen with regard to the compensation offered to landowners subject to expropriation in the public interest. The compensation was originally much lower than the market value, but also through the rhetoric reference to the human right to property, the compensation now has to match the market value of the expropriated land. See, critically, Luca Nivarra, 'La Funzione Sociale Della Proprietà: Dalla Strategia Alla Tattica' (2014) 31 Riv crit dir priv 503.

475 Like specific performance, an injunction is an equitable remedy that is awarded if damages do not adequately compensate the claimant, as the latter needs to restrain the defendant from starting or continuing a breach of a negative contractual undertaking (prohibitory injunction) or needs to compel performance of a positive contractual obligation (mandatory injunction). See *Lumley v Wagner* [1852] 1 DM & G604. On injunction as indirect specific performance, see James T Brennan, 'Injunction against Professional Athletes Breaching Their Contracts' (1967) 34 Brooklyn Law Review 61.

476 *Unwired Planet* (n 381) [169].

477 For this distinction, see the germinal Guido Calabresi and A Douglas Melamed, 'Property Rules, Liability Rules and Inalienability: One View of the Cathedral' (1972) 85 Harvard Law Review 1089.

478 Urteil des Kartellsenats 5 May 2020 – KZR 36/17 (*Sisvel v Haier*).

479 Gerechtshof Den Haag, 9 January 2020–200.219.487/01 (*Koninklijke Philips N.V. v Wiko SAS*); Gerechtshof Den Haag, 14 May 2019–200.221.250/01 (*Koninklijke Philips N.V. v Asustek Computers Inc. and others*).

Despite these shortcomings, the *Huawei* approach was endorsed by the European Commission in its Communication ‘Setting out the Approach to Standard Essential Patents’,⁴⁸⁰ and it has been welcomed by those scholars who see it as satisfying ‘in an effective manner the interests of all stakeholders.’⁴⁸¹ In general, the Commission follows *Huawei* in refusing a one-size-fits-all approach, which leaves an important role for national courts. In practice, this is leading to SEP overprotection.

The first pillar of the Commission’s framework is transparency. Technology implementers – including companies wishing to enter the IoT market – can hardly predict their exposure if they cannot easily access information about the existence and scope of SEPs. Ironically, SEP databases held by standard-developing organisations are not standardised and lack transparency. The main standards are covered by hundreds of thousands of SEPs held by dozens of parties.⁴⁸² Uncertainty stems also on the fact that ETSI members can submit their declarations of essentiality before the actual grant of the patent, which may ultimately not be granted. As a consequence of this overdeclaration issue, the ‘current declaration practices do not convey reliable information on the essentiality of declared patents.’⁴⁸³ Essentiality is self-assessed, without external scrutiny. Nor is clarity provided at the licensing stage. The Commission notes that this is especially problematic in the context of IoT, where new players with little experience of SEPs licensing are ‘continually entering the market for connectivity.’⁴⁸⁴ Therefore, the Commission:

- (i) Called on standard-developing organisations to improve the quality of their databases by making them user-friendly, searchable on the basis of the standardisation project, synchronised with patent offices’ databases.⁴⁸⁵
- (ii) Called on these organisations to transform the current declaration system into a tool that provides up-to-date and precise information in a way that helps technology implementers assess patent infringement exposure;
- (iii) Committed to the launch of a pilot project for SEPs in selected technologies with a view of facilitating the introduction of an appropriate mechanism to scrutinise their essentiality to a standard.⁴⁸⁶

The second pillar is a framework for FRAND licensing. The Commission’s starting point is that the parties are best placed to achieve a common understanding of what is a fair rate. This consensus is hindered by conflicting interpretations

480 European Commission, ‘Communication “Setting out the EU Approach to Standard Essential Patents”’ (n 384).

481 McDonagh and Bonadio (n 385) 6.

482 Bartlett and Contreras (n 385).

483 Pohlmann and Blind (n 387) 3.

484 European Commission, ‘Communication “Setting out the EU Approach to Standard Essential Patents”’ (n 384) [1].

485 *ibid* [1.1].

486 *ibid* [1.2.2].

of 'FRAND,' especially in the IoT sectors, where '[d]ivergent views and litigation over FRAND licensing risk delaying the uptake of new technologies.'⁴⁸⁷ To overcome this, the Commission invites negotiating parties to consider efficiency considerations, mutual expectations, and importance of the uptake by implementers to promote the diffusion of the standard. Worryingly, the Commission takes a pro-monopolist stance that seems even more extreme than the CJEU's. Indeed, the value to consider is not the market value: it is the nebulous concept of 'value added of the patented technology (which is) irrespective of the market success of the product.'⁴⁸⁸ Nonetheless, the Commission seemed aware that this liberal approach of leaving the FRAND determinations to party autonomy does not work in the IoT, due to its complex supply chain and imbalanced relationships. Accordingly, it called on standard-developing organisations and SEP holders to develop effective, transparent, and predictable solutions 'to facilitate the licensing of a large number of implementers in the IoT environment,'⁴⁸⁹ via patent pools or other licensing platforms.⁴⁹⁰ Meanwhile, it committed to monitor licensing practices, in particular in the IoT sector.

The third pillar is a predictable enforcement environment. SEP patents are more litigated than regular patents, and this can result in barriers to entry.⁴⁹¹ This is particularly true for IoT stakeholders that report that 'uncertainties and imbalances in the enforcement system have serious implications for market entry.'⁴⁹² Once again, the Commission prefers to leave the solution to party autonomy on the premise that good faith will be a guiding principle and that injunctions can be granted against implementers in bad faith. Leaving aside the limited role of good faith in common law jurisdictions,⁴⁹³ this approach has four shortcomings. First, it ignores that the corrective virtues of good faith are of limited relevance in the context of imbalanced business-to-business relationships that are commonplace in the IoT, especially if the implementer cannot enter a market without using a SEP.⁴⁹⁴

487 *ibid* [2].

488 *ibid* [2.4].

489 *ibid*.

490 E.g. Ericsson launched Avanci, an IoT licensing platform that promises to be 'the first marketplace for licensing patented cellular technology to the Internet of Things' ('Licensing on FRAND Terms' (*Ericsson*, 25 January 2017) <www.ericsson.com/en/patents/frand>). This platform allows technology implementers to access SEPs under one agreement and for one fair, flat per-unit rate.

491 Pohlmann and Blind (n 387).

492 European Commission, 'Communication "Setting out the EU Approach to Standard Essential Patents"' (n 384) [3].

493 Although in some cases in recent years UK courts have not found the idea of good faith as repugnant as they once did, there is considerable divergence between common law and civil law countries in this matter. See David Campbell, 'Good Faith and the Ubiquity of the "Relational" Contract: Good Faith and the Ubiquity of the "Relational" Contract' (2014) 77 *The Modern Law Review* 475.

494 In business-to-business relationships, the stronger company can (i) impose contracts that are unfair, relying on the fact that the economic dependence and reputational factors will deter the weaker company from suing them, and (ii) set aside the contract and impose a relationship that is factually unfair. More on this in Noto La Diega (n 97). The laws controlling the fairness of the

Second, the *Unwired Planet* ‘saga has shown that different views on the way the parties should negotiate are always just around the corner.’⁴⁹⁵ Therefore, it is hard to understand why the Commission, the CJEU, and national courts share the view that parties to a SEP licensing agreement are in the best position to determine the terms that are most appropriate for their specific situation. Third, it disregards that implementers may be in good faith and yet infringe e.g. because the SEP holder is unilaterally imposing unfair ‘FRAND’ terms or because they cannot afford to pay the market value or the added value for each of the thousands of patents that are declared essential to a standard. Fourth, it lacks detail with regard to the ‘precise terms of FRAND licensing and the exact meaning of good faith.’⁴⁹⁶ This means that FRAND terms will be determined in a fragmented way, patent holder by patent holder, patent by patent, usually in separate proceedings: this can harm the IoT ‘as *technology convergence* continues to impact standardisation in key areas such as next-generation wireless communication and the Internet of Things.’⁴⁹⁷ The Commission declared that it would improve the enforcement environment by working ‘with stakeholders to develop and use methodologies, such as sampling, which allow for efficient and effective SEP litigation.’⁴⁹⁸ This confirms the coregulatory preference of the EU, the dangers of which have been underlined in Chapter 1. The statement also corroborates the idea that the Commission wants to achieve an ‘efficient and effective’ outcome as opposed to a balanced outcome.⁴⁹⁹ Imbalanced efficiencies are likely to come from implementers passively accepting FRAND terms and injunctions being given the antitrust green light. This can also be seen in the Commission’s ambiguous treatment of the concept of open

terms of business-to-business contracts are still underdeveloped. See Simon Whittaker, ‘Unfair Terms in Commercial Contracts and the Two Laws of Competition: French Law and English Law Contrasted’ (2019) 39 *Oxford Journal of Legal Studies* 404. Good faith in business-to-consumer transactions plays a crucial role, as epitomised by the Unfair Terms Directive, which considers a contractual term to be unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties’ rights and obligations.’ This gives corrective powers to courts that can weigh up the fairness of a term in a consumer contract. See Simon Whittaker and Reinhard Zimmermann, ‘Good Faith in European Contract Law: Surveying the Legal Landscape’ in Reinhard Zimmermann and Simon Whittaker (eds), *Good Faith in European Contract Law* (CUP 2000) 7, esp 53. The corrective function of good faith is disputed. Cf Carmelo Restivo, *Contributo Ad Una Teoria Dell’abuso Del Diritto* (Giuffrè 2007); Claudio Scognamiglio, ‘Abuso Del Diritto, Buona Fede, Ragionevolezza (Verso Una Riscoperta Della Pretesa Funzione Correttiva Dell’interpretazione Del Contratto?)’ (2010) 2 *NGCC* 139.

495 Giuseppe Colangelo and Gianluca Scaramuzzino, ‘Unwired Planet Act 2: The Return of the FRAND Range’ (2019) 40 *ECLR* 306.

496 McDonagh and Bonadio (n 385) 7.

497 Bartlett and Contreras (n 385) 285. Italics added. The authors recommend a mechanism of statutory interpleader be used to join the holders of all patents covering a particular technology standard into a single proceeding in which an aggregate FRAND royalty may be determined.

498 European Commission, ‘Communication “Setting out the EU Approach to Standard Essential Patents”’ (n 384) [3.6].

499 This is in spite of emphatic declarations whereby ‘a balanced IPR framework is needed that supports a sustainable and efficient standardisation ecosystem and SEP licensing environment’ (ibid [5]). For a more optimistic appraisal, see McDonagh and Bonadio (n 385).

source. On the one hand, it recognises that open source is important to improve standard development, standard take-up, and interoperability. On the other hand, it concludes with the concerning notation whereby we need to ‘pay attention to the interaction between open source community projects and (standardisation)’⁵⁰⁰ due to the divergences between the former and the latter in terms of IPR policies and balance. It is this book’s conviction that, as opposed to looking at free and open-source Things with scepticism or even hostility, open-source community projects should be convincingly supported – in them lies the hope to take back control of the IoT.

This area of law will have to be kept under observation as changes are in sight. At the end of 2020, the European Commission published its *IP Action Plan*,⁵⁰¹ where it declared that new technologies such as the IoT provide an opportunity to modernise the IP framework by intervening in five areas. These include the proposal for action to ‘facilitate access to and sharing of intangible assets while guaranteeing a fair return on investment.’⁵⁰² The Commission implicitly admits that the Communication ‘Setting out the Approach to Standard Essential Patents’⁵⁰³ was not a success as ‘[d]espite the guidance provided in the SEPs Communication . . . some businesses continue to find it difficult to agree on SEP licensing,’ as agreeing on what is fair remains controversial. However, instead of learning from its own mistakes (the focus on self- and coregulation as well as on party autonomy), the Commission reiterates that, at least in the short term, the solution will be provided by industry-led initiatives. Positively, reforms will be considered, including third-party checks on whether the SEP declarations actually regard ‘essential’ patents.⁵⁰⁴ Hopefully, the reform will include a harmonisation of patent laws, including SEPs licensing and streamlining of IP exceptions, so as to rebalance the IP framework, currently tilted in favour of monopolists and deaf to the arguments of fairness.

Overall, competition law appears to be an ineffective tool in the regulation of the IoT and in curbing the underlying power imbalance. This was confirmed in June 2021, when the Commission published the initial findings of its inquiry into the consumer IoT sector.⁵⁰⁵ The respondents reported difficulties in competing with vertically integrated companies, such as Amazon, Google, and Apple, which have built their own ecosystems within and beyond the consumer IoT sector. In particular, they complained about (i) exclusivity and tying practices; (ii) big tech role as bottlenecks controlling user relationships; (iii) use of data by

500 European Commission, ‘Communication “Setting out the EU Approach to Standard Essential Patents”’ (n 384) [4]. Emphasis attention.

501 European Commission, ‘Making the Most of the EU’s Innovative Potential. An Intellectual Property Action Plan to Support the EU’s Recovery and Resilience’ (2020) COM(2020)760 final.

502 *ibid* 3.

503 European Commission, ‘Communication “Setting out the EU Approach to Standard Essential Patents”’ (n 384).

504 The plan is based on Rudi Bekkers and others, ‘Pilot Study for Essentiality Assessment of Standard Essential Patents’ (2020) JRC119894.

505 ‘Antitrust: Initial Findings of Consumer IoT Sector Inquiry’ (n 296).

voice assistant providers not only to improve the market position of their general-purpose voice assistants but also to allow them to leverage more easily into adjacent markets; and (iv) ‘the prevalence of *proprietary technology*, leading at times to the creation of “*de facto standards*”, together with technology fragmentation and lack of common standards, raise concerns as to the *lack of interoperability*.’⁵⁰⁶ Unlike ownership, property is alive and well, and it prevails on those ‘official’ standards that – overburdened with SEPs and not helped by the lack of decisive antitrust interventions – struggle to play a meaningful role in the realisation of an interoperable and open IoT.

6.7 Interim Conclusion

‘Smart’ capitalism equates rentier capitalism. Increasingly, IoT companies leverage their intangible assets – and their integration in proprietary hardware – to impose monopolistic prices, inaccessible barriers to access, and behavioural constraints, thus harming newcomers, consumers, and society as a whole. The death of ownership is the chief manifestation of the underlying imbalance of power. In a way that, on the face of it, would resemble medieval times, we exercise our rights on ‘our’ property subject to the control of the digital lords. However, as the collective interest and reciprocal duties played an important role in limiting property in the feudal system, the real precursor of the current state of things ought to be found in the individualist outlook of bourgeois society. Under IoT capitalism, the death of ownership does not amount to a death of the right to property, which has never been stronger, at least in its IP species. Hypertrophic IP portfolios held by few multinational IoT corporations are a threat both to individual ownership and to the commons. This is well illustrated by the phenomenon of IP overlaps and by the prevalence of patents on competition in the context of FRAND licensing.

In the IoT, IP overprotection and the death of ownership are the result of a combination of overlapping IPRs and corporate control over the Thing exercised by factual, technological, and legal means. IP overlaps hamper any attempt to rely on IP’s internal limitations to protect the IoT user. For instance, an act that falls under a copyright exception (e.g. reverse engineering) may qualify as infringement under patent law. My recommendation to courts is to leverage European fundamental rights – mainly freedom of expression and prohibition of abuse of rights – to (i) interpret existing exceptions as user rights that are of equal standing as the IP holder’s rights; (ii) recognise an autonomous, open-ended defence along the lines of fair use in the US. As IPRs become ubiquitous and sterilise IP exceptions, the case for a fair use approach has never been more convincing. Such an approach would allow the public interest to play more of a role in IP governance, and it would make sure that the IoT unleashes its sustainability potential. A more generous approach to exceptions would be robustly grounded in the ECHR jurisprudence that regards IP as an exception to human

506 *ibid.*

rights, and the CJEU freedom-of-expression-driven jurisprudence. Should a flexible approach be rejected, a second-best solution would see EU lawmakers streamlining existing defences across the different IP subsystems to make sure that they are framed explicitly as user rights, as well as being mandatory, binding, and covering commercial and mixed purposes.

Private power, including the power of IoT platforms and consortia, is the traditional domain of competition law interventions. In the IoT, the IP-competition conflict is mainly resolved through the qualification of SEP holders' actions as an abuse of dominant position. Regrettably, the CJEU took an imbalanced, pro-SEP holder stance that has been worsened by national courts. Rather than the flexible pro-competitive approach taken by the Commission in *Samsung*, a rigid and pro-proprietary, step-by-step protocol has prevailed in *Huawei v ZTE* and its aftermath. The Commission has unquestioningly accepted this new turn and, in keeping with its coregulatory preference, is leaving to public and private stakeholders to codify a licensing and enforcement framework that revolves around party autonomy and good faith. These are unlikely to work in the IoT, with its complex supply chain, the abundance of players that are new to the technicalities of SEP licensing, and its ubiquitous power imbalance. One can only hope that the Commission takes a braver approach and adopts a binding instrument that would harmonise patent law in the EU, thereby embracing the willingness to negotiate as a more flexible method and clearly defining FRAND terms as opposed to leaving the definition of fairness to market dynamics. As things stand, similarly to Ricardo's and Marx's rentiers that would exploit their monopoly power over the land to impose a rent that was a monopoly price, SEP owners aggressively patrol the gates to IoT innovation and seek monopolistic rents in the form of licensing fees that are only nominally fair.

IP law and competition provide an unsatisfactory solution to the death of ownership. This is partly due to the increasing influence of private superpowers. Thanks to them – and to the lawmakers that accommodated their demands – IP has become pervasive and imbalanced, whilst market forces no longer erode their monopolies.⁵⁰⁷ Antitrust itself has not yet developed adequate ways to address data power, with the end result that both internal and external limitations are unlikely to play an effective role in rebalancing IoT relationships, at least if relied upon in isolation. Legal arguments based on exceptions and competition have failed, but where the law fails, collective action may succeed. Free and open source, open hardware, open data, and open standards – in a word, the commons – may provide the opportunity to organise new forms of resistance and address the IoT struggle.⁵⁰⁸ This will be the ambitious task of the next chapter, which will attempt to draw some conclusions.

507 Ricolfi (n 11) 26.

508 Evgeny Morozov and Francesca Bria, 'Rethinking the Smart City. Democratizing Urban Technology' (2018) Rosa Luxemburg Stiftung New York Office <www.rosalux-nyc.org/rethinking-the-smart-city/>.