IIC
https://doi.org/10.1007/s40319-021-01120-3

ARTICLE

Preserving the Public Domain: Limits on Overlapping Copyright and Trade Secret Protection of Software

Ulla-Maija Mylly

Accepted: 21 September 2021

Abstract The traditional understanding of intellectual property (IP) suggests that each IP category has a discrete subject matter of its own and exceptions thereto. Based on such an understanding of IP law, one would assume that there would not be overlapping IP protection for the same subject matter or product features. However, this understanding does not hold water. It has been argued that the development of overlapping IP rights has intensified as the subject matter that can be protected has expanded through the introduction of new rights and as the scope of protection for existing rights has increased. What may be particularly problematic is that, when policymakers focus on one IP regime at time, any issues arising from IP overlaps may remain undetected. For quite some time, there has been a policy tendency towards broadening the scope of intellectual property protection, which has led to a decrease in scope for the public domain. This tendency shows that the value of the public domain has not been appropriately identified or at the least not appreciated. One way to define the public domain is as the sphere that is not protected by any form of IP. This article will focus on the overlaps created by the Software Copyright and Trade Secrets Directives with regard to the protection of

This article was written within the framework of the following projects funded by the Academy of Finland: "Constitutional Hedges of Intellectual Property"; "Fairness, Morality and Equality in International and European Intellectual Property Law (FAME-IP)"; and "Dissecting the Trade Secret Chimera in the Era of Data-riven Economy DISTRASEC" (338849).

I would like to thank Sharon K. Sandeen, Professor of Law and Director of the IP Institute at Mitchell Hamline School of Law, for her valuable comments on an earlier draft of this paper. I would also like to thank the anonymous referees of the IIC Journal for their valuable comments.

U.-M. Mylly (✉)
Academy Research Fellow, Faculty of Law, University of Turku, Turku, Finland
e-mail: ulla-maija.mylly@utu.fi

Published online: 20 October 2021

software. The ultimate aim of the article is to query whether the combined effects of these two Directives could be interpreted in a way that limits the undesirable expansion of protection.

Keywords Trade secrets · Copyright · Public domain · Overlap · Software · Reverse engineering

1 Introduction

The traditional understanding of intellectual property (IP) suggests that each IP category has a discrete subject matter of its own and exceptions thereto. For example, patent rights protect technological inventions, while copyright protects artistic creations.[1] In line with such an understanding, each subcategory of IP has its own particular purpose. The rights created by the applicable laws serve the specific functions of the regime in question.[2] Based on such widely shared textbook understanding of IP law, one would assume that there would not be overlapping IP protection for the same subject matter. At the least, different IP subcategories would protect the same product features only exceptionally and to an insignificant degree.

However, this understanding does not hold water. The phenomena of overlapping intellectual property rights are part of complex reality. The question of IP overlaps has also been visible in the recent case law of the European Court of Justice (ECJ), for example in its *Brompton Bicycle* and *Cofemel* cases.[3] It has been argued that the development of overlapping IP rights has intensified as subject matter that can be protected has expanded through the introduction of new rights and as the scope of protection for existing rights has increased. The lowering of the threshold for protection is one example of an issue that has contributed to the expansion of existing protection. Consequently, situations where rights overlap are more frequent than before.[4] For quite some time, there has been a policy tendency towards broadening the scope of intellectual property protection, which has led to a decrease in scope for the public domain. This tendency shows that the value of the public domain has not been appropriately identified or at the least not appreciated.[5]

[1] Pila (2017).

[2] Tomkowicz (2012), p. 7.

[3] In the *Brompton Bicycle* case the patent protection had expired, and the question was whether the functional aspects of bicycles could be protected by copyright. C-833/18, ECLI:EU:C:2020:461. In the *Cofemel* case the question was about the threshold for copyright protection when there was also design protection available. C-683/17, ECLI:EU:C:2019:721. Interestingly, in the *Cofemel* case it was highlighted that the protection of designs and copyright protection pursue fundamentally different objectives and are subject to distinct rules (para. 50). Moreover, it was decided that granting protection, under copyright, to subject matter that is protected as a design must not have the consequence of undermining the respective objectives and effectiveness of those two forms of protection (para. 51). In essence, this meant that normal requirements for copyright eligibility should be applied in potential overlap situations and that Portugal was not allowed to set different requirements for copyright eligibility in such situations (paras. 48, 29, 56).

[4] Derclaye and Leistner (2011), pp. 1–2.

[5] Boyle (2008), p. 16.

One way to define the public domain is as the sphere that is not protected by any form of IP.[6] The role of the public domain, in line with the purpose of the IP system, is to enable creativity, culture and innovation. The public domain is the raw material for new creation and innovation. Therefore, it is detrimental if we do not limit the expansion of IP.[7] Recognizing the importance of the public domain informs us of the impact of various policy decisions that may be detrimental to the public domain, for example threats to lock down information.[8] We need information and ideas, at least, to flow. If IP protection limits that flow, we face problems. What may be particularly problematic is that, when policymakers focus on one IP regime at time, any issues arising from IP overlaps may remain undetected.

The recent introduction of the Trade Secrets Directive[9] is an example of expansion of protection at EU level. Even though an obligation to protect trade secrets is already enshrined in the TRIPS Agreement,[10] its provisions leave considerable discretion to the Member States to design the scope of protection for trade secrets. In addition, the TRIPS Agreement does not prevent overlapping rights. The Trade Secrets Directive expands protection in the EU by affording more detailed and stronger protection for secret information. Even though it is questionable whether trade secrets should be classified as IP,[11] the Trade Secrets Directive seems to provide an IP type of protection. Such expanded protection is also available for information residing in software products. However, software product features are to some extent protectable also through copyright.[12] In the EU, copyright protection for software was already harmonized in the 1990s by the adoption of the Software Copyright Directive.[13]

At present, these two Directives combined create a web of rights covering software products and the information residing in them. This article will focus on the overlaps created by these two Directives as regards the protection of software. One aspect highlighted in this article is that the exceptions and limitations put in

[6] Samuelson (2003), p. 149.

[7] Boyle (2008), pp. 38–41.

[8] Samuelson (2003), p. 150.

[9] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1.

[10] Agreement on Trade-Related Aspects of Intellectual Property Rights, the TRIPS Agreement, Annex 1C of the Marrakesh Agreement establishing the World Trade Organization, signed in Marrakesh, Morocco on 15 April 1994.

[11] *See* Bently (2013) and Udsen et al. (2020), pp. 22–23. Note also that the Trade Secrets Directive does not designate trade secrets as intellectual property. The EU's General Court treated trade secrets as equivalent to intellectual property rights in its competition law decision *Microsoft*, but still did not define trade secrets as intellectual property rights. In this case, trade secrets were granted neither less nor more protection than intellectual property rights. T-201/04 *Microsoft Corp. v. Commission* [2007] ECR II-3601, paras. 289–290.

[12] Patent protection is likewise available but will not be discussed in this article.

[13] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version), OJ L 111, 5.5.2009, pp. 16–22. Lately, the expansion of copyright protection has been recognized as a general trend in the EU. *See*, for example, Bently et al. (2018), p. 53.

place to protect the sphere of the public domain are not appropriately enabling access to information in the context of software. This is a particular problem under the software copyright rules, which seem to lead to a lack of accessibility to ideas in software products, even though the founding principle of the copyright regime is that ideas should be free. This is an example of how protection has been expanded by blurring the distinction between which information in software products can and cannot be protected. This article will address how to prevent an escalation of the problem created by copyright rules. The main argument is that protection should be available under these regimes only if the specific requirements of each particular regime are fulfilled. Protection should not be afforded to information otherwise. In particular, putative holders of trade secrets should not receive trade secret protection based on the copyright regime's inappropriate restrictions on accessing information. This is one way of addressing the problem related to IP overlaps and adhering to a balanced approach to the scope of IP protection and protection of the public domain. This article will focus on analyzing what should remain in the public domain.

Part 2 examines the discourses related to IP overlaps. It explains how IP overlaps may reveal problems in the respective IP regimes and offers some solutions to overcome such issues. Part 3 analyzes the copyright protection of software features, and evaluates the lack of protection for ideas and how access to these is unsatisfactorily ensured through reverse engineering rights. Part 4 analyzes the key elements in the Trade Secrets Directive that impact on the scope of protection and suggests how the provisions of the Trade Secrets Directive should be interpreted in order to prevent the expansion of protection. Particular attention is paid to the definition of "trade secret" and how this definition should be understood as a doctrine limiting the scope of protection. This would be one important way of preserving the public domain under the trade secret regime. Part 4 also discusses the interpretations related to reverse engineering rights as a means of accessing information and how this is the major limitation to the protection of trade secrets. Both Parts 3 and 4 analyze the possibility of a contractual waiver of reverse engineering rights. Part 5 concludes by explaining the problems found and elaborating on what is left for the public domain.

The ultimate aim of the article is to query whether the combined effects of these two regimes could be interpreted in a manner that limits the undesirable expansion of protection. Special attention is paid to defining the scope of protection and available exceptions and limitations with regard to accessing information. As the Trade Secrets Directive is a relatively new instrument, particular attention is paid to its provisions and how they are likely to be interpreted. However, the key perspective throughout the article is that of overlaps between copyright and trade secret protection. Although the article has limited itself to these two protection categories in a specific context, it is assumed that its findings may also have a more generic relevance for the overlap discourse.

2 Theory of Overlaps

On a general level, the problem related to overlaps in IP protection, in particular when stemming from the introduction of new rights and the expansion of the scope of protection, is that it tends to reduce the public domain.[14] The phenomenon of overlapping rights, when stemming from the expansion of rights without limiting doctrines, increases the scope of protection. This may occur through various intellectual property rights being invoked concurrently or subsequently.[15] However, there is no generally accepted rule of how to deal with IP overlap cases or whether the situation is reasonable in the first place. For instance: Should IP owners be required to choose between applicable regimes?

One possible answer relates to the underlying justifications for the respective IP regimes.[16] In line with this approach, it has been stressed that none of the justifications related to particular IP regimes require double rewards, even though the natural law justifications assume rewards based on many of these regimes individually.[17] Moreover, no intellectual property regime is limited to the interest of protection only, but has to take account of multiple competing considerations, seeking to find a justifiable compromise between the right to protection and the freedom to use and disseminate information. Consequently, overlap may create situations that can be problematic from the perspective of one regime's delicate balance between protection and dissemination or the public domain. In other words, the IP rights afforded in one regime may cancel the limitations on the scope of rights created by another regime. One solution to prevent such deviation from the established equilibrium is to consider whether protection in the overlap situation distorts the justifiable balance of the related regime.[18]

Each IP regime has its own balancing principles and related exceptions and limitations to safeguard the public domain. However, at international treaty level, one finds balancing principles applicable to all IP related rights in Arts. 7 and 8 of the TRIPS Agreement in particular. Article 7 explicitly states that intellectual property protection should contribute to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations. Article 8, in turn, allows WTO members to take into account the public interest when enacting and applying their IP laws, with Art. 8, for example, allowing member states to promote the public interest in sectors of vital importance to their socio-economic and technological development. The aspect of technological development is highly relevant in the area of IP protection related to the information residing in software technology. These general principles are considered to provide safeguards to maintain public interest considerations as part of any IP protection under the TRIPS Agreement. It is also noteworthy that these objectives and principles have lately gained a more important

[14] Derclaye and Leistner (2011), p. 3.

[15] Tomkowicz (2012), pp. 15–17.

[16] Wilkof and Basheer (2012), pp. lvi–lvii.

[17] Tomkowicz (2012), pp. 17–19.

[18] Tomkowicz (2012), p. 14.

role in interpretations of the TRIPS Agreement. This may mean that their role will be highlighted more in the future.[19]

In its preamble, the WIPO Copyright Treaty[20] also recognizes the balancing principle for the copyright regime, explicitly "the need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information."[21] Access to information, as a balancing principle to protection, is likewise part of the EU copyright and trade secret regimes. Access to information is of paramount relevance and importance for the analysis that will be conducted by this article, in particular of the right to reverse engineer under these regimes, largely because information is critical for the very invention and creativity that most IP laws seek to encourage.

A perspective limited to one type of IP subject matter may not provide sufficient answers to the potential problems created by the expansion of rights and the ensuing overlaps. One important perspective, highlighted in this article, on the problems related to overlaps is that overlap situations often reveal an imbalance in the applicable IP regimes. In line with this understanding, the problem might not always be the overlaps as such, but rather those situations in which a particular IP regime no longer honors its own limits and justifications, which are reflected in the ideal compromise between the interest in protection and that of securing freedom of use and access for third parties. The justifications and underlying principles of each intellectual property category, including exceptions and limiting doctrines, clarify the acceptable limits of protection. Consequently, the issue of overlapping rights might help us to more critically and analytically consider the exact objectives of each system and to pay more attention to the potentially problematic consequences of the expansion of intellectual property rights illuminated by IP overlaps. This awareness may help us to tailor each regime to better fulfill its objectives in a more balanced manner and limits the undesirable expansion of rights. Doing so would also be in line with preserving the public domain, which constitutes an essential background premise for the intellectual property system.[22]

As already explained, one element in reasonably limiting expansion of rights relates to how exceptions are interpreted. Exceptions to each IP regime balance protection with other important interests. It is important that how exceptions are interpreted adheres to the regime's intended balance. This article analyzes reverse engineering rules. One way to approach IP overlaps, in accordance with the IP overlap literature, is to resort to consistent application of similar looking rules, especially exceptions, under different IP regimes. The consistent and coherent application of exceptions would help to maintain the balance between the interest to protect the interests of the rightholder and the competing public interests protected under intellectual property law across various IP regimes.[23] These public interest

[19] Geiger and Desaunettes-Barbero (2020).

[20] WIPO Copyright Treaty adopted in Geneva on 20 December 1996.

[21] Derclaye and Leistner (2011), pp. 27–28 and at p. 297 referring to EU case law where Art. 7 has been explicitly mentioned as a limiting principle in addition to EU legislation.

[22] *See* Derclaye and Leistner (2011), pp. 284–285

[23] Derclaye (2017), p. 19.

considerations underlying the exceptions are often also connected to the underlying justifications of a system. Therefore, there might also be reasons to adopt a different interpretation for different regimes when a regime in question justifies and explicates such a deviation.

One of the aims of emerging IP overlap scholarship has been to provide some guidelines or solutions on how to deal with the potential problems created by overlaps. Often, the overlaps are studied by analyzing a pair of IP rights, for example trade secret and patent protection. However, the combination of trade secret protection and copyright protection has not gained much attention in existing research related to overlaps.[24] This is partly due to the fact that trade secrets have been understood as part of unfair competition law in many European countries, and overlaps between IP and unfair competition law have often been discussed only very briefly and in relation to all sorts of rights under unfair competition laws.[25] Another reason for the lack of research related to overlaps involving trade secrets might be that the overlap between unfair competition law and IP rights has not been considered to be so problematic, as unfair competition law does not protect specific subject matter but only regulates wrongful conduct.[26] However, the fact that trade secret protection is not confined to a specific subject matter (like technical inventions in patent law), but can protect multiple types of information, increases the likelihood of IP overlaps between trade secrets and other IP rights.

Recital 2 to the Trade Secrets Directive explains that confidentiality is used in relation to a diverse range of information that extends beyond technological knowledge to commercial data such as information on customers and suppliers, business plans, and market research and strategies. The lack of specific subject matter creates particular challenges for limiting the undesirable and unintended expansion of trade secret protection. The requirement of commercial value is the only qualitative criterion for clarifying what type of information may be subject to trade secret protection. Hence, it is highly important, *inter alia*, to understand the definition of trade secrets as a doctrine limiting the scope of trade secrets, as will be further explained in Part 4.

3 Scope of Copyright Protection and Access to Information in Software Products

An important balancing principle under copyright rules is that copyright does not protect ideas but only their original expression. This divide is generally defined as the idea-expression dichotomy. It means that others are free to use the ideas behind a copyrighted work without fear of infringement. It also ensures that copyright protection does not exclude the use of functional ideas and elements. The lack of

[24] For example, in the Wilkof and Basheer book there were at least 12 such pairs of IP protection rights, but none of these pairs covered trade secret versus copyright protection.

[25] This is the approach in Derclaye and Leistner (2011). Now the situation has changed also in Europe following the introduction of the Trade Secrets Directive.

[26] Derclaye and Leistner (2011), pp. 297–298.

protection of ideas and facts balances the interests of copyright holders with those of users and the general public.[27] The divide between ideas and expressions ensures that copyright gives protection only to something more than the mere recombination of elements of the common stock. It is therefore key for protection of the public domain.[28] However, as will be explained, ideas underlying software products may be protected to some extent by copyright rules related to reverse engineering exceptions, as well as by the fact that copyright and trade secrets overlap. This article will elaborate the possibilities for sustaining the initial balance by explaining ways to interpret the key provision that distorts the equilibrium.

The idea-expression principle is explicitly stipulated in international treaties.[29] The principle is also explicitly expressed in Art. 1(2) of the Software Copyright Directive: "Ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under this Directive."

In the *SAS v. WPL* case, Art. 1(2) of the Software Copyright Directive was interpreted by the ECJ to the effect that "[…] neither the functionality of a computer program nor the programming language and the format of data files used in a computer program in order to exploit certain of its functions constitute a form of expression of that program for the purposes of Art. 1(2) of Directive 91/250." It further emphasized that accepting that the functionality of a computer program can be protected by copyright would enable the monopolization of ideas, to the detriment of technological progress and industrial development. The ECJ even referred to the explanatory memorandum to the Proposal for Directive 91/250 [COM(88) 816], which states that the main advantage of protecting computer programs by copyright is that such protection covers only the individual expression of the work and thus leaves other authors the desired latitude to create similar or even identical programs provided that they refrain from copying.[30] This judgment and its reasoning illustrates well the intended balance within copyright not to give protection to ideas and specifically how this is interpreted in the software copyright context.[31] It also highlights the impact of freedom of ideas on technological and

[27] Bently et al. (2018), pp. 217–218. However, these authors explain that the idea-expression dichotomy is quite unhelpful in practical cases for drawing the line between what can and what cannot be protected. Ibid.

[28] Boyle (2008), pp. 32–33.

[29] The TRIPS Agreement, Art. 9.2., provides as follows: "Copyright protection shall extend to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such." The WIPO Copyright Treaty, Art. 2, defines the scope of copyright protection similarly.

[30] C-406/10 *SAS Institute Inc. v. World Programming Ltd*, ECLI:EU:C:2012:259 paras. 39–41.

[31] In the *BSA* case, which was about the protection of a program's graphic user interface, the ECJ held that components of the graphic user interface that were differentiated only by their technical function could not be protected as the author's own original expression. Where the expression of those components is dictated by their technical function, the criterion of originality is not met, since the different methods of implementing an idea are so limited that the idea and the expression become indissociable. C-393/09, *Bezpečnostní softwarová asociace – Svaz softwarové ochrany v. Ministerstvo kultury,* ECLI:EU:C:2010:81 paras. 48–50. In this case the idea-expression dichotomy was an important element in deciding what could be protected.

industrial development, which is likewise recognized as important under the balancing principles of the TRIPS Agreement.

However, the exclusive rights of a copyright holder under the Software Copyright Directive, namely the rights of reproduction, translation and adaptation of a software code, may to some extent prevent access to ideas underlying software code. Firstly, copyright legislation gives the copyright holder the exclusive right of reproduction, in other words copying. In the ECJ case law, the right of reproduction has been recognized as an essential right in the copyright legislation.[32] In many countries, the right of reproduction is the oldest exclusive right. However, at present, the exclusive right of reproduction has proved problematic,[33] especially for computer programs. Whenever a computer program is used, it needs to be copied. The starting point of copyright legislation is that, because of the reproduction right, such copying falls within the exclusive rights of a copyright holder; this is the case also under Art. 4(1)(a) of the Software Copyright Directive. Consequently, copyright legislation needs specific rules to enable end users to reproduce necessary copies in this specific technological context in order to access ideas that are not eligible for protection.

Under Art. 5 of the Software Copyright Directive a person having the right to use a copy of a computer program is entitled, without the authorization of the rightholder, to observe, study or test the functioning of the program in order to determine the *ideas and principles* that underlie any element of the program if he/she does so while performing any of the acts of loading, displaying, running, transmitting or storing the program that he/she is entitled to do. The exception is a mandatory exception, which cannot be excluded by contract. This authorization covers in principle just normal actions or operations of the user while using software. However, the purpose of these operations does not need to be the normal use of the software. The end user is allowed to run these operations for the purpose of analyzing ideas and principles in the software product. This exception resolves most of the issues related to the copyright holder's exclusive right of reproduction, thus ensuring access to ideas.

In the *SAS v. WPL* case the ECJ interpreted this exception and clarified that the purpose for which the license is given does not restrict the methods of analysis under Art. 5(3) of the Software Copyright Directive. The ECJ stated that the licensee is entitled to carry out acts covered by the license and the acts of loading and running necessary for use of the computer program. By recourse to all these acts, the licensee may observe, study or test the functioning of the program so as to determine the ideas and principles underlying any element thereof.[34] In this case, the ECJ did not give copyright holders further options to control access to ideas

[32] Joined Cases C-457/11 to C-460/11 *Verwertungsgesellschaft Wort (VG Wort) v. Kyocera Document Solutions Deutschland GmbH and Others, Canon Deutschland GmbH Fujitsu Technology Solutions GmbH and Hewlett-Packard GmbH v. Verwertungsgesellschaft Wort (VG Wort)*, ECLI:EU:C:2013:34 para. 33.

[33] For example, Pihlajarinne has suggested a new context-based approach to reproduction rights. For the digital context, she argues that, even though the right of reproduction is a fundamental principle of copyright law, it is most unfit for the digital environment. Pihlajarinne (2017).

[34] C-406/10 *SAS Institute Inc. v. World Programming Ltd*, ECLI:EU:C:2012:259.

through contractual clauses. The ECJ's argumentation strongly supports the basic principle that ideas cannot be protected. The outcome is also in line with Art. 8 of the Software Copyright Directive, as all contracts that contradict Art. 5(3) thereof are null and void.

However, in addition to reproduction, the unauthorized translation, adaptation or transformation of the form of the code for which a copy of a computer program has been made available constitutes an infringement of the exclusive rights of the author under Art. 4(1)(b) of the Software Copyright Directive. In the process of decompilation, which is one technique of reverse engineering, a computer program code is translated from object code back to source code. The source code version is the version of the software that humans can understand. Therefore, in order to fully understand how the software is put together, as well as all the ideas and principles underlying the code, one needs access to the source code version of the software. Not all the ideas and principles are detectable by observing the software while it is functioning. But code translations need authorization either through an exception in the Software Copyright Directive or from a copyright holder.

Article 6 of the Software Copyright Directive defines specific situations in which decompilation techniques are lawful. Firstly, decompilation needs to be *indispensable in order to achieve interoperability* between two computer programs. This requirement severely limits the purpose for which decompilation is allowed and represents the major constraint in identifying ideas from the software source code. Consequently, some ideas and principles underlying a computer program may remain inaccessible, even if not eligible for protection under Art. 1(2) of the Software Copyright Directive, simply because access to source code is allowed only for interoperability purposes. Moreover, the exception under Art. 6 has very narrow wording, with many further conditions, which I have already elaborated in an earlier article.[35]

The narrowness of the exception becomes clear from Art. 6(3), which requires that Art. 6 may not be interpreted in such a way as to allow its application in a manner that unreasonably prejudices the rightholder's legitimate interests or that conflicts with normal exploitation of the computer program. The Article here refers to the Berne Convention's three-step test for exceptions. In the *SAS v. WPL* case it was initially suspected that the competitor had used a more demanding reverse engineering technique, decompilation, in accessing the ideas not eligible for protection. In this case the Advocate General explained, in line with the three-step test, that decompilation may not be used in such a way as to prejudice the legitimate interests of the rightholder or to conflict with normal exploitation of the program. The Advocate General further considered that "decompilation may be contemplated in very specific circumstances only." Moreover, he explained that the licensee should demonstrate the absolute necessity for decompilation, which should be understood as an exceptional act.[36] These interpretations indicate that the Art. 6 reverse engineering rule in the Software Copyright Directive as an exception to the rightholders' exclusive rights has to be construed narrowly.

[35] For further discussion of these requirements and comparison with the US *see* Mylly U-M. 2010.

[36] C-406/10 *SAS Institute Inc. v. World Programming Ltd* ECLI:EU:C:2011:787, paras. 85–87.

Similarly to the *SAS v. WPL* case and to some other earlier ECJ case law, the ECJ continued to hold, in two quite recent copyright cases – *Spiegel Online* and *Funke Medien* – that, as a general rule, derogations from the main rule of exclusive rights being held by rightholders are to be interpreted narrowly. The national courts must apply an interpretation consistent with the wording used in the specific exception and the three-step test.[37] However, in the *Spiegel Online* and *Funke Medien* cases the ECJ acknowledged that, even though Art. 5 of the Information Society Directive provides "exceptions and limitations," these give rights to users, and that the aim of this Article is to ensure a fair balance between the rights and interests of rightholders and those of users of subject matter that is eligible for protection. Therefore, a national court must interpret these exceptions in a manner that ensures their effectiveness. The ECJ also highlighted that, even though intellectual property is protected under the Charter of Fundamental Rights of the European Union, there is nothing to suggest that it is an absolute right.[38]

The EJC has also previously highlighted a balanced approach and observance of the effectiveness of an exception, for example in its *FAPL* case. In this case, when interpreting the mandatory exception under Art. 5(1) of the Information Society Directive, the ECJ took into account the purpose of the exception, which was to ensure the development of new technologies. This objective was derived from *travaux préparatoires* and the preamble to the Information Society Directive.[39] Likewise, in the *VOB* case the ECJ held that exceptions had to be interpreted strictly, but that the interpretation must also enable the effectiveness of the exception to be safeguarded and its purpose to be observed. The ECJ reasoned that copyright must adapt to new economic developments such as new forms of exploitation. The ECJ further reasoned that digital lending of books indisputably constituted one of those new forms of exploitation and, accordingly, necessitated the adaptation of copyright to new economic developments. The ECJ considered that lending electronic books was essentially similar to lending printed books and therefore the exception applicable for printed books was also applicable to electronic books.[40] Here the ECJ adopted a teleological interpretation for the exception in question.[41] In both of these cases copyright exceptions were also linked to economic and technological developments. Similarly, technological development can be seen to be of paramount importance when interpreting the Software Copyright Directive's rules and exceptions.

Consequently, when interpreting the decompilation exception under the Software Copyright Directive, this provision, too, needs to be interpreted in a manner that ensures its effectiveness. Moreover, this exception provides important rights to users and also contributes to the balance of rights. ECJ case law on copyright, discussed

[37] C-516/17 *Spiegel Online GmbH* paras. 37, 53, 59; C-469/17 *Funke Medien NRW GmbH* at paras. 48, 52, 69, 76.

[38] C-516/17 *Spiegel Online GmbH* at paras. 46, 51–56, 59; C-469/17 *Funke Medien NRW GmbH* at paras. 52, 67–72, 76.

[39] C-403/08 *Football Association Premier League Ltd and Others* at paras. 163–164 and 175–180.

[40] C-174/15 *Vereniging Openbare Bibliotheken v. Stichting Leenrecht*, paras. 45 and 50–54.

[41] Sganga (2018), para. 52.

here, may provide some guidance on how to interpret the Software Copyright Directive in a more flexible manner in the future, taking into account also the objective of the exception and its role in ensuring technological development.

One aspect especially to be taken into consideration in future interpretations is the fact that the fundamental premise of copyright – the absence of protection for ideas – is partly ensured through these reverse engineering provisions. It is noteworthy that the exclusivity does not extend to ideas in software products. One could argue here that the main rule is the absence of protection for ideas. Allowing the use of decompilation techniques is in line with the fundamental purpose of the copyright regime, namely the absence of protection for ideas through enabling access to this information.[42] It also provides an important balance between protection and the public domain. If some ideas in software products remain unidentifiable due to restrictions in accessing them, the end result runs counter to the copyright regime's own basic principles and purposes. In addition, the end result is not the same as for other copyright protected materials where information is more easily identifiable. This creates a discriminatory situation between software products and other copyrighted materials, an end result that is neither technology-neutral nor coherent within the copyright regime.[43] The requirements for decompilation should be interpreted also with these factors in mind. Taking into account also the ECJ's guidance to respect the three-step test when interpreting copyright exceptions, it is noteworthy that, if reverse engineering was done in order to gain access to ideas and principles, there is nothing to suggest that this would prejudice the legitimate interests of the rightholder. This is because the copyright protection does not extend to ideas.

It is noteworthy that the importance of these reverse engineering exceptions is highlighted also in the Software Copyright Directive. The Software Copyright Directive makes the role of contracts very clear. Any contractual provisions contrary to Art. 6 (decompilation for interoperability) or Art. 5(3) (exceptions provided for observing ideas and principles) are null and void. This mandatory nature of the exceptions underscores the importance of these provisions. Moreover, this absence of protection for interoperability information goes beyond even the contracting parties: Information derived through utilization of a decompilation technique can be given to others when necessary for the interoperability of the independently created computer program.[44]

The mandatory rules of the Software Copyright Directive also apply in the context of the Trade Secrets Directive's context when the product is software. This is clear from Art. 3(1)(b) of the Trade Secrets Directive, which states that reverse engineering is lawful if a person is free from any *legally valid duty* to limit the acquisition of the trade secret. As anti-reverse engineering obligations are, in the specific situations explained, null and void under the copyright rules when a product

[42] Others have also argued that the idea-expression dichotomy needs to be strengthened, as its role has been diminished in the copyright regime; thin copyright protection would serve society better. Vaidhyanathan (2001), p. 15.

[43] The end result is not technology-neutral in its effects. On various interpretations of technology neutrality, *see* Graig (2016).

[44] Art. 6(2)(b) Software Copyright Directive.

is software, Art. 3(1)(b) of the Trade Secrets Directive confirms the invalidity of anti-reverse engineering obligations in the software context across copyright and trade secret rules. This provision demonstrates explicit consistency between these two directives. In this regard, the balance is achieved in a similar manner, and trade secret protection in this regard does not disturb the copyright balance.

However, the underlying challenge is that the Software Copyright Directive prevents access to ideas to some degree, and it is unlikely that this problem will fade away merely through flexible interpretation of the Software Copyright Directive's provisions, although it might be mitigated to some extent. However, a critical evaluation and analysis of trade secret protection, which will be carried out next, will illuminate possibilities to prevent an escalation of the problem through protection overlap. With careful interpretations of the provisions of the Trade Secrets Directive, it will be possible to limit the unnecessary expansion of trade secret protection.

4 Availability of Information Under the Trade Secrets Regime

4.1 Defining Trade Secret Requirements for Protection

When trade secret protection is analyzed from the perspective of the IP overlap discussion, particular attention needs to be paid to the scope of protection. In this analysis the justifications and underlying premises of trade secret protection also play a particular role. The scope of protection should not expand beyond the system's intended objectives.

An important feature of trade secret protection is that it does not create exclusive rights to information, even if that information is confidential. This is explicit in recital 16 to the Trade Secrets Directive, which provides that "[i]n the interest of innovation and to foster competition, the provisions of this Directive should not create any exclusive right to know-how or information protected as trade secrets." This aspect is further reinforced by the provisions of Art. 3(a) and (b), which allow the independent development and reverse engineering of information. The impact of these provisions is that the same information may belong to several entities, which limits the scope of protection considerably. Yet, another feature of trade secret protection is the lack of specific subject matter. The protection may cover information as such and many types of information, as already explained. Therefore, the definition of trade secret has to be understood in a way that clearly delineates one's trade secrets, clarifying the boundary between information that is an entity's trade secret and information that belongs to the public domain. But the definition also delineates when many entities may rely on trade secret protection for the same or very similar information provided that none of them has relied on wrongful activities when discovering the information in question.

The central feature of unfair competition law – the regulation of wrongful conduct – is an important premise of trade secret protection. For example, TRIPS refers to unfair competition law when ensuring protection for trade secrets.[45] TRIPS Art. 39(2) requires Members to protect trade secret information from being disclosed to, acquired by, or used by others without their consent *in a manner contrary to honest commercial practice*.[46] From recital 1 to the Trade Secrets Directive we learn that trade secrets are not considered to belong to the realm of IP rights. The recital states that use of intellectual property is one means for businesses to appropriate innovation-based results. Trade secrets are considered to be another means. This provision can be understood in the sense that trade secrets are still considered to belong to the area of unfair competition law, which has been the situation in many countries before the introduction of the Trade Secrets Directive.[47]

The unfair competition aspects of trade secret law are closely connected to the non-exclusivity of trade secret protection.[48] This approach can be seen also in Art. 3 of the Trade Secrets Directive, which explains which activities are considered lawful, and Art. 4, which elaborates on unlawful activities when accessing, disclosing or using information. The focus under the Trade Secrets Directive is on censuring wrongful conduct only, without creating exclusive rights to information. These aspects are important when analyzing and interpreting the scope of trade secret protection and in particular when looking at the possible interpretations of the definition of "trade secret" under the Trade Secrets Directive.

In order to determine which information in the source code of a software product may remain secret and qualify for trade secret protection, it is essential to discuss the definition of a trade secret. This designation proves problematic in many respects in the case of software products and their source code. The TRIPS Agreement defines trade secrets in Art. 39, but otherwise allows Members considerable discretion to design their trade secret laws and scope of protection.[49] The definition of trade secrets in Art. 2 of the Trade Secrets Directive closely follows the definition in the TRIPS Agreement, which states that "trade secret" means information that meets all of the following cumulative requirements: "(a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, *generally known* among *or readily accessible* to

[45] TRIPS Art. 39(1) "In the course of ensuring effective protection against unfair competition as provided in Art. 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2."

[46] However, the fact that TRIPS is an intellectual property treaty and the Art. 39 reference to unfair competition law has led some to define trade secrets as a form of hybrid protection. Bently (2013).

[47] For example for Nordic countries *see* Bruun and Schovsbo (2020), p. 87.

[48] *See also* Knaak et al. (2014), p. 955.

[49] TRIPS Art. 39(2) provides "[…] so long as such information:
(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."

persons within the circles that normally deal with the kind of information in question; (b) it has *commercial value because it is secret*; and (c) it has been subject to *reasonable steps* under the circumstances, by the person lawfully in control of the information, *to keep it secret.*" (emphasis added)[50]

When considering these requirements in the context of software products, it is noteworthy that the criteria are cumulative. Even though one may think that the criterion of commercial value is typically easily fulfilled, as software products normally do have commercial value, in this context the commercial value needs to stem from the parts of the software product that satisfy the other two requirements as well.[51] Therefore, potentially only small parts of the software code qualify for trade secret protection.[52]

The two other components deserve a more detailed analysis. The most critical part in the definition is that the information must be secret in the sense that it is not *generally known or readily accessible* by persons within the circles that normally deal with the kind of information in question. In practice, the requirement that information is not *generally known* does not refer to the situation in which information is known to the general public: it is sufficient that it is generally known in the relevant industry circles. Then it does not qualify for trade secret protection. The secrecy may be lost when products are placed on the open market.[53] When a product is released to the market, the information appearing on the outside of the product in question ceases to be secret.

Some uncertainty prevails over what "*readily accessible*" means in practice. Such uncertainty becomes apparent in the case of products with integrated technical features that are not apparent on simple observation. Information that can be observed through simple inspection and requires only limited or no reverse engineering, cannot qualify as a trade secret. Moreover, it was argued before the introduction of the Trade Secrets Directive that information can be discerned *with reasonable cost and time* from products placed on the market is not secret or confidential by nature.[54] Information that is readily ascertainable is not a trade

[50] The Trade Secrets Directive has been drafted to closely resemble the Defend Trade Secrets Act (DTSA) 2016 of the United States, which is US Federal law based on the Uniform Trade Secrets Act (UTSA), the earlier model law for state trade secret laws. *See* Sandeen (2020). Therefore, in this article, also US trade secret scholarship is utilized when substantively relevant.

[51] In the United States it is particularly stipulated in the UTSA that the information must "[derive] *independent* economic value, actual or potential, from not being generally known or readily ascertainable by other persons who can obtain economic value from its disclosure or use" (emphasis added) UTSA Sec. 1(4)(i). This has been interpreted to mean that this value should bring competitive advantage. *See* Sandeen (2010), p. 524.

[52] For more on the commercial value requirement, *see* Aplin (2014), pp. 261–262, where she explains the potential application of this requirement in the EU. For a more international discussion *see*, for example, Sandeen 2011, pp. 550–551, where she explains the drafting history of TRIPS Art. 39 and in more depth the commercial value requirement and the delicate differences of the TRIPS Members on this issue.

[53] *See*, for example, Sandeen (2020), p. 47. *See also*, for US law, the Uniform Trade Secrets Act Sec. 1, comment No. 5. The UTSA applies terminology "readily ascertainable" whereas TRIPS and the Trade Secrets Directive apply terminology "readily accessible" when defining trade secrets. The applied terminology in these legal texts serves the same function.

[54] Aplin (2013), p. 349.

secret, whereas information that is heavily reverse engineered may qualify for trade secret protection but is potentially not misappropriated.

Where we draw the line between information that is readily accessible or must be heavily reverse engineered affects the scope of trade secret protection greatly, as it determines whether some information can qualify as a trade secret in the first place. This cannot be determined purely on the basis of a contractual stipulation made by the potential trade secret holder.[55] If information is readily accessible, then it is part of the public domain in light of the definition of trade secrets. This cannot be agreed otherwise. For example, the Supreme Court of Finland ruled, under the previous legislation, that since it was possible to learn the information claimed to be a trade secret from the products that were publicly on sale, the instructions on how to build such products were not trade secrets.[56] The information was thus considered to be readily accessible. In this regard the requirement was the same under the previous legislation in Finland as it will be under the Trade Secrets Directive.

The definition of trade secrets in Art. 2 of the Trade Secrets Directive also requires that in order to receive trade secret protection, the information needs to have been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. It is important that this requirement is fulfilled as it enables third parties to understand the specific nature of certain information. These reasonable steps have the function of informing third parties that certain information requires special treatment and is subject to legal protection. In the absence of such visible steps, third parties could not consider appropriate actions with respect to such information, as they would not be able to understand its nature as a trade secret. Thus the reasonable steps, together with the other prerequisites of trade secret protection, set the boundaries of legal protection with respect to such information. This has been aptly called *the notice function of trade secret protection*.[57] It has been suggested that the interpretation of the notion of reasonable steps in the Trade Secrets Directive would cover both factual circumstances in the form of clear safekeeping measures and explicit agreements. In any case, the nature of the information has to be conveyed in such a way that there is no ambiguity about its secret nature.[58] Hence, under the Trade Secrets Directive, there can be no legal presumption that such measures have been resorted to. In other words, if a party has neglected to take the reasonable steps required, trade secret protection cannot be effectively claimed later in court proceedings.[59]

[55] This has been the interpretation at least under US law. *See*, for example, Sandeen (2005), p. 124.

[56] Supreme Court of Finland case KKO 1991:11. However, a particular feature of the Finnish Trade Secret Act is that even information that would not qualify as a trade secret can be protected as a technical instruction and the same remedies will be available. This was the case also under the previous Finnish legislation. However, it is questionable whether this protection without qualification as a trade secret is allowed under the Trade Secrets Directive. At the least, it is clearly against the harmonization objective. *See* Bruun and Schovsbo (2020), p. 94.

[57] Bone (201)1, p. 59.

[58] Knaak et al. (2014), p. 957.

[59] Vapaavuori (2019), p. 85. Note that, according to Ohly, in Germany these actions were merely assumed before the implementation of the Trade Secrets Directive. Ohly (2020), p. 109.

In practice, this criterion of trade secret protection is often not problematic to meet, as long as the person seeking protection has paid attention to this requirement. One way to fulfill this requirement is through contracts. In order to keep certain information secret and later be able to refer to trade secret protection, one needs to limit access to the information through contractual clauses or otherwise. The role of a contractual clause is to give notice to a party of the intended nature of the information as a trade secret.[60] Giving such notice is important, as trade secret protection under the Trade Secrets Directive is against unlawful acquisition, use or disclosure.[61] In principle, it should not be possible to commit a bona fide infringement of trade secrets. The infringing party needs to be aware of the nature of the information in question.[62] This principle is also visible in Art. 4 of the Trade Secrets Directive where the directive explains what type of activities are considered unlawful.[63] This element of trade secret protection refers to the unfair competition type of protection, as it condemns wrongful or improper conduct.

However, as the analysis is highly contextual, it is uncertain what means other than contractual notifications qualify as reasonable steps. Fulfilling the reasonable steps criterion requires some activity from the person claiming trade secret protection. This activity should also somehow be apparent to third parties. Udsen, Schovsbo and van der Donk have indicated that, for example, encryption and embedding can fulfill the criterion of reasonable steps.[64] However, here it is argued that these measures qualify as reasonable steps only if this type of activity creates sufficient difficulty with regard to reverse engineering that it is unambiguous to third parties that information should be treated confidential. The mere difficulty of reverse engineering, alone, is not sufficient. Relying on this type of activity as reasonable steps is therefore uncertain means for the trade secret holder.

Importantly, copyright rules also restrict access to software source code. This is because copyright law allows more demanding reverse engineering activities – decompilation of the software object code version back to the source code version – *only* for specific interoperability purposes. Otherwise, decompilation is not allowed as it involves – at the least – reproducing and translating the software, which both fall under the exclusive rights of the copyright holder. Software proprietors may consider that, because of these legal restrictions, there is no need to take further

[60] *See*, for example, Varajadaran (2018), p. 1547.

[61] Art. 4 of the Trade Secrets Directive refers to *unlawful* acquisition, use and disclosure of trade secrets. In the United States the definition of *misappropriation* is utilized. The Defend Trade Secrets Act and the the Uniform Trade Secrets Act are in conformity with each other in this definition. *See* 114th Congress House of Representatives Report 114-529, p. 14. "First, 'misappropriation' is defined identically in all relevant respects to the definition of misappropriation in Sec. 1(2) of the UTSA. The Committee intentionally used this established definition to make clear that this Act is not intended to alter the balance of current trade secret law or alter specific court decisions."

[62] *See* Ohly (2020), p, 109. He also argues that it is important for third parties to know the nature of the information.

[63] Also a third party liability under Art. 4 of the Trade Secrets Directive requires that a "*person knew or ought*, under the circumstances, *to have known* that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully within the meaning of [the previous] paragraph" (emphasis added).

[64] Udsen et al. (2020), p. 35.

steps to protect secrets in software source code, as it is already unlawful to access the information residing in the source code, except for specific interoperability purposes. In other words, copyright legislation could be argued to be among the circumstances to be taken into consideration when addressing the required reasonable steps under the Trade Secrets Directive. Udsen et al. have considered that copyright rules would potentially be *lex specialis* for regulating reverse engineering practices in the case of software products.[65] However, it is noteworthy that Art. 3(1)(b) of the Trade Secrets Directive explicitly mentions reverse engineering as a lawful means of accessing trade secrets. This explicitly indicates a different approach when compared with the copyright context. And under the Trade Secrets Directive protection is not automatic: to qualify for trade secret protection the reasonable steps should have been taken.

Even though accessing information in source code through decompilation, a sophisticated reverse engineering technique, outside the interoperability exception of the Software Copyright Directive constitutes a copyright infringement, it should not automatically lead to an infringement of trade secret protection. If copyright norms also created trade secret protection for the software source code, they would provide an additional protection layer, leading to double rewards through copyright. But copyright legislation does not constitute an action of a person invoking trade secret protection. Hence, it should not fall under the reasonable steps required from a person invoking trade secret protection. The person invoking trade secret protection should take some action in order to gain protection: passivity and copyright norms alone should not be sufficient for establishing trade secret protection for the information residing in the software source code. This interpretation is in line with the idea that trade secret protection should only operate where clear enough boundaries with respect to the information have been communicated to third parties in the form of concrete steps to protect the secrecy of the information in question. In addition, the reasonable steps requirement has normally been understood as referring to the reasonableness of the protection measures required from the putative trade secret holder.[66] Asking a putative trade secret holder, for example, to include a contractual clause in the software licensing agreement to indicate the existence of trade secrets in the source code can be considered a reasonable requirement and, in many cases, does not create an overly burdensome requirement to fulfill.

However, under the Trade Secrets Directive, the role of contracts in protecting confidential information is somewhat complex. As already mentioned above, one cannot change the nature of public information to that of trade secret information by a simple contractual stipulation. This refers to the situations where information is generally known or readily accessible and therefore cannot qualify for protection. However, in some circumstances, when they qualify as reasonable steps, contracts do provide the required protection for confidential information, as explained in this chapter. And in some cases, contracts are necessary if one wishes to prevent otherwise lawful reverse engineering activities, as will be further elaborated next.

[65] Udsen et al. (2020), p. 35.

[66] *See*, for example, Sandeen (2020), pp. 50–52.

4.2 Reverse Engineering as a Lawful Means of Accessing Trade Secrets

Article 3 of the Trade Secrets Directive lists reverse engineering as a legal means of accessing a trade secret: "The acquisition of a trade secret shall be considered lawful when the trade secret is obtained by […] observation, study, disassembly or testing of a product or object that *has been made available to the public or* that is lawfully in the possession of the acquirer of the information who is *free from any legally valid duty to limit the acquisition of the trade secret.*" (emphasis added)

The interpretation of this Article can be divided in two parts. The first part of Art. 3 (before "or that is lawfully …") refers to situations where a product has been made available to the public. This part of the Article does not refer to the possibility of limiting access to the trade secret. The latter part of Art. 3 refers to the situation where a product has not been made available to the public, but only to restricted circles. The latter part of the Article refers to the possibility of restricting access to trade secrets, as it stipulates that a product is lawfully in the possession of the acquirer who is free from a legally valid duty to limit acquisition of the trade secret. As software products are normally licensed to the users this type of restriction can be included in those licenses.

It has been argued that, if products are put on the mass market, one cannot restrict reverse engineering through contracts. This interpretation is based on the "made available to the public" situation in Art. 3.[67] The impact of this provision would be that products delivered to the mass market could under the Trade Secrets Directive even be heavily tested in order to gain access to trade secrets. More generally, the right to reverse engineer has been understood as an important principle of information laws. It has been suggested that because reverse engineering is such a vital part of the information laws, contractual freedom should be construed narrowly. With respect to mass market products, reverse engineering thus could not be waived.[68] The basic premise of the Trade Secrets Directive that reverse engineering is lawful also supports the argument that restrictions on reverse engineering under copyright law should not as such be sufficient to establish trade secrecy for software source code.

When information contained in software qualifies for trade secret protection, it is still lawful under the Trade Secrets Directive to access this information through sophisticated and demanding reverse engineering techniques such as decompilation. This is because Art. 3 of the Trade Secrets Directive defines that it is lawful to access *trade secrets* through reverse engineering. Typically, accessing information through decompilation does not, in principle, change the nature of the information thus accessed unless the information can be deemed readily accessible. Therefore, the information accessed will still be defined as a trade secret of the first holder of the information, as long as it does not become generally known through a third party accessing the information and, for example, disclosing it further. In these specific situations, the information accessed may also become a trade secret of the second

[67] Udsen et al. (2020), pp. 35–36. In a somewhat similar vein, Ohly (2020), p. 115, but he refers to the situation where products have been sold.

[68] Udsen et al. (2020), pp. 34 and 36.

party after the second party reverse engineers it, if the second party keeps it secret and the other requirements are still met,[69] most importantly the requirement that the information has not become generally known.

On the other hand, the trade secrets that are incorporated in software will be destroyed when a large enough number of people have conducted reverse engineering of a product so that the information has become generally known.[70] Thus, if mass marketed products cannot be subject to anti-reverse engineering obligations under the Trade Secrets Directive, one may assume that, once products are delivered to a large enough number of end users, the information has lost its secret nature as it is available to the masses. Furthermore, even if such anti-reverse engineering obligations are enforceable, if those obligations are breached by enough people the trade secrets may become generally known in any case.

In contrast to the situation of mass marketed software, the utilization of reverse engineering techniques can be restricted between *contracting parties* under the Trade Secrets Directive if the product has been delivered only to restricted circles. For example, Nordberg has argued that, even though mass marketed products cannot be subject to anti-reverse engineering obligations, a trade secret holder can issue such an obligation in the supply chain to its direct contracting parties.[71] Recital 16 provides, however, that freedom to enter into such agreements may be limited by law. This enables Member States to decide their own approach to the validity of anti-reverse engineering contracts: for instance, Member States are free to decide that they do not enforce such contracts.

When analyzing German implementation of the Trade Secrets Directive, Ohly has questioned whether standard contract terms could validly be used to restrict reverse engineering.[72] The validity of standard contract terms in limiting reverse engineering depends on the national law in question. However, the Software Copyright Directive mandates that certain contractual restrictions on reverse engineering – those limiting access to interoperability information – be rendered invalid throughout the EU. The Software Copyright Directive also mandates permitting less demanding reverse engineering techniques, if the purpose is to get access to ideas and principles underlying the software.

If the trade secret regime were to be understood as forming part of information law, as some have suggested, the most consistent approach would be not to enforce such contractual clauses at all. However, at EU level, the Trade Secrets Directive does not take that clear approach to the nature of trade secret protection. Nevertheless, it is possible to interpret the various provisions of the Trade Secrets Directive in a way that sets clear requirements and boundaries for the information that qualifies for trade secret protection. It has to be borne in mind that the objective of the trade secret regime is not to create exclusive rights to information. Moreover,

[69] Vapaavuori (2019), p. 114.

[70] *See* Aplin (2013), p. 355. Nordberg has even argued that if the information can be accessed with lawful means, in particular through reverse engineering, it will not be subject to trade secret protection at all. Nordberg (2020), p. 206.

[71] Nordberg (2020), p. 215.

[72] Ohly (2020), p. 116.

the provisions defining reverse engineering as lawful means for accessing information enable information flows that are important for the public domain.

5 Scope for the Public Domain with Concluding Remarks

If one considers copyright and trade secret regimes separately and without a specific context in mind, one may think that neither regime offers strong protection. Copyright does not protect ideas or principles: these are free for others to use. Trade secret law allows independent development and does not provide exclusive rights to information. Both copyright protection and trade secret protection have rules and doctrines in place that enable access to information and consequently allow competition and scope for the public domain to flourish. However, when one analyses the specific case of software and the cumulative and overlapping protection provided by these regimes, the dangers of the expansion of rights and the related problems of the regimes become visible. This has been explicitly highlighted in intellectual property overlap scholarship. The overlap situation helps us to recognize situations where the protection regime may expand beyond its inherent objectives.

This article has made some suggestions on how to interpret the cumulative effects of the EU Software Copyright Directive and the Trade Secrets Directive so as to maintain the intended balance of both regimes. Most importantly, in this article, the two regimes and their scope of protection have been interpreted from the perspective of their justifications and underlying principles. For the copyright regime, access to ideas and principles should be secured as far as possible, because the absence of protection for ideas and principles is one of the basic premises and justifications of the system. Furthermore, it sets the boundary between protection and the public domain. Consequently, exceptions enabling access to ideas should be interpreted so as to ensure the efficiency of the rule in question, as also emphasized in ECJ case law on copyright.

For the trade secret regime, the core limitation, based on the underlying principles and justifications of the system, is that the trade secret regime should only censure actions that are improper or wrongful by nature. Therefore, particular attention should be paid to application of the reasonable steps requirement, as this particularly sets the threshold for information that can be protected under trade secret law. This rule is of paramount importance, as trade secret protection does not have any specific subject matter capable of limiting the scope of application. Therefore, the reasonable steps requirement ensures the proper balance between what can be protected and the public domain, and ensures that the scope of what can be protected has been communicated. To reduce the possibility of unintended overlap, putative trade secret holders are required to make active efforts to keep information secret, as indicated in the Directive. This ensures that trade secret protection censures wrongful conduct not only in theory but also in practice. Moreover, the basic premise of the trade secret regime is that reverse engineering is a lawful means of accessing information. This rule is a fundamental and intentional part of the trade secret regime in enabling the free flow of information. Therefore, limitations to such flow should be construed narrowly.

These ways of interpreting the rules would ensure that both systems remained truer to their basic objectives and core principles and would prevent the unintended and undesirable escalation of protection. In the end, adopting such premises for interpretation would contribute to maintaining the public domain, which forms one of the most fundamental background requisites for all creation and innovation. Even though it is possible in specific cases to rely on competition law measures in order to secure access to information protected by copyright or as a trade secret,[73] this does not remove the requirement that copyright and trade secret regimes honor their fundamental premises, and that these systems be interpreted in compliance with such objectives.

Funding Open access funding provided by University of Turku (UTU) including Turku University Central Hospital.

References

Aplin T (2013) Reverse engineering and commercial secrets. CLP 66:341–377

Aplin T (2014) A critical evaluation of the proposed EU Trade Secrets Directive. IPQ 4:257–279

Bently L (2013) Trade secrets: intellectual property but not property? In: Howe R, Griffiths J (eds) Concepts of property in intellectual property law. Cambridge Intellectual Property and Information Law (21). Cambridge University Press, pp. 60–93. https://doi.org/10.1017/CBO9781107300880

Bently L, Sherman B, Gangjee D, Johnson P (2018) Intellectual property law, 5th edn. Oxford University Press, Oxford

Bone RG (2011) Trade secrecy, innovation and the requirement of reasonable secrecy precautions. In: Dreyfuss RC, Strandburg KJ (eds) The law and theory of trade secrets. Edward Elgar, Cheltenham, pp 46–76

Boyle J (2008) The public domain, enclosing the commons of the mind. Yale University Press, New Haven & London

Bruun N, Schovsbo J (2020) Implementation of the Trade Secrets Directive in the Nordic countries. In: Schovsbo J, Minssen T, Riis T, (eds) The harmonization and protection of trade secrets in the EU: an appraisal of the EU Directive. Edward Elgar, Cheltenham, pp 85–102

Derclaye E, Leistner M (2011) Intellectual property overlaps, a European perspective. Hart Publishing, Oxford

Derclaye E (2017) Overlapping rights. In: Dreyfuss R, Pila J (eds), The Oxford handbook of intellectual property law. https://doi.org/10.1093/oxfordhb/9780198758457.013.27

Geiger C, Desaunettes-Barbero L (2020) The revitalisation of the object and purpose of the TRIPS Agreement: the plain packaging reports and the awakening of the TRIPS flexibility clauses. In: Griffiths J, Mylly T (eds), Global intellectual property protection and new constitutionalism. Oxford, Oxford University Press, Forthcoming. Centre for International Intellectual Property Studies (CEIPI) Research Paper No. 2020-01

[73] *See* T-201/04 *Microsoft Corp. v. Commission* [2007] ECR II-3601.

Graig CJ (2016) Technological neutrality: recalibrating copyright in the information age, theoretical inquiries in law. 17: 601–632. https://doi.org/10.1515/til-2016-0022
Knaak R, Kur A, Hilty RM (2014) Comments of the Max Planck Institute for Innovation and Competition of 3 June 2014 on the Proposal of the European Commission for the Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure of 28 November 2013, COM (2013) 813 Final. IIC 45:953–967. https://doi.org/10.1007/s40319-014-0270-3
Mylly U-M (2010) An evolutionary economics perspective on computer program interoperability and copyright. IIC 41:284–315
Nordberg A (2020) Trade secrets, big data and artificial intelligence innovation: a legal oxymoron? In: Schovsbo J, Minssen T, Riis T (eds) The harmonization and protection of trade secrets in the EU: an appraisal of the EU Directive. Edward Elgar, Cheltenham, pp 192–218
Ohly A (2020) Germany: the Trade Secrets Protection Act 2019. In: Schovsbo J, Minssen T, Riis T (eds) The harmonization and protection of trade secrets in the EU: an appraisal of the EU Directive. Edward Elgar, Cheltenham, pp 103–123
Pihlajarinne T (2017) Should we bury the concept of reproduction – towards principle-based assessment in copyright law? IIC 48:953–976
Pila J (2017) The subject matter of intellectual property. Oxford University Press, Oxford
Samuelson P (2003) Mapping the digital public domain: threats and opportunities. Law&ContempProbs 66:147–172
Sandeen SK (2005) A contract by any other name is still a contract: examining the effectiveness of trade secret clauses to protect data bases. IDEA the Journal of Law and Technology 45:119–164
Sandeen SK (2010) The evolution of trade secret law and why courts commit error when they do not follow the uniform trade secrets act. Mitchell Hamline Law Review 33:493–543
Sandeen SK (2011) The limits of trade secret law: article 39 of the TRIPS Agreement and the Uniform Trade Secret Act on which it is based. In: Dreyfuss RC, Strandburg KJ (eds) The law and theory of trade secrets. Edward Elgar, Cheltenham
Sandeen SK (2020) Through the looking glass: trade secret harmonization as a reflection of US law. In: Schovsbo J, Minssen T, Riis T (eds) The harmonization and protection of trade secrets in the EU: an appraisal of the EU Directive. Edward Elgar, Cheltenham, pp 38–63
Sganga C (2018) A plea for digital exhaustion in EU copyright law, JIPITEC 9(3)
Tomkowicz R (2012) Intellectual property overlaps, theory, strategies and solutions. Routledge
Udsen H, Schovsbo J, van der Donk B (2020) Trade secrets as part of information law. In: Schovsbo J, Minssen T, Riis T (eds) The harmonization and protection of trade secrets in the EU: an appraisal of the EU Directive. Edward Elgar, Cheltenham, pp 22–37
Vaidhyanathan S (2001) Copyright and copywrongs: the rise of intellectual property and how it threatens creativity. NYU Press
Vapaavuori T (2019) Liikesalaisuudet ja salassapitosopimukset. 3rd edn, Alma Talent, Helsinki
Varajadaran D (2018) The trade secret-contract interface. Iowa Law Review pp. 1543–1591
Wilkof N, Basheer S (eds) (2012) Overlapping intellectual property rights. Oxford University Press, Oxford, pp. lvi–lvii

Official Materials

Agreement on Trade-Related Aspects of Intellectual Property Rights, The TRIPS Agreement, Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15 April 1994
114th Congress House of Representatives Report 114-529
Defend Trade Secrets Act (DTSA) 2016 of the United States
Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version), OJ L 111, 5.5.2009, pp. 16–22
Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1
Uniform Trade Secrets Act 1985 (UTSA)
WIPO Copyright Treaty adopted in Geneva on 20 December 1996

Case Law

Supreme Court of Finland KKO 1991:11
Bezpečnostní softwarová asociace – Svaz softwarové ochrany v. Ministerstvo kultury, C-393/09ECLI:EU:C:2010:81
Cofemel – Sociedade de Vestuário SA v. G-Star Raw CV, C-683/17, ECLI:EU:C:2019:721
Football Association Premier League Ltd and Others v. QC Leisure and Others (C-403/08) and *Karen Murphy v. Media Protection Services Ltd*, C-429/08, ECLI:EU:C:2011:631
Funke Medien NRW GmbH v. Bundesrepublik Deutschland, C-469/17, ECLI:EU:C:2019:623
Microsoft Corp. v. Commission, T-201/04 [2007] ECR II-3601
SAS Institute Inc. v. World Programming Ltd, C-406/10, ECLI:EU:C:2012:259
SI and Brompton Bicycle Ltd v. Chedech / Get2Get, C-833/18, ECLI:EU:C:2020:461
Spiegel Online GmbH v. Volker Beck, C-516/17, ECLI:EU:C:2019:625
Verwertungsgesellschaft Wort (VG Wort) v. Kyocera Document Solutions Deutschland GmbH and Others Canon Deutschland GmbH Fujitsu Technology Solutions GmbH and Hewlett-Packard GmbH v. Verwertungsgesellschaft Wort (*VG Wort*), Joined Cases C-457/11 to C-460/11 ECLI:EU:C:2013:34
Vereniging Openbare Bibliotheken v. Stichting Leenrecht, C-174/15 ECLI:EU:C:2016:856