INCONSISTENCIES IN THE REGULATION OF ANTI-CIRCUMVENTION IN THE EU

Petroula Vantsiouri*

Abstract

This paper identifies the differences in the regulation of anti-circumvention in the EU by three different legislative instruments, namely the Information Society Directive, the Software Directive and the Conditional Access Directive and demonstrates the practical implications of those differences. The paper concludes that the great inconsistencies within the regulation of anti-circumvention in the EU demand a reevaluation of the policies that led to the adoption and to the current form of anti-circumvention norms.

1. Introduction

Of all the issues of copyright policy in the last twenty years, probably the most controversial has been the issue of technological protection measures (TPMs). TPMs constitute self-help mechanisms, such as copy protection for DVDs, password protection for online services, and encryption of television broadcast signals, which are designed to prevent acts of infringement and exploitation of intellectual property rights by controlling copying or access to works.[1] As it was anticipated that ways would be found to circumvent these copy and access controls, the legal systems of many countries provide TPMs legal support by giving to the right holders concerned specific protection when trying to enforce and manage their rights by technical means. These so-called anti-circumvention norms do not create or enlarge exclusive rights as such, but they enhance the exploitation and enforcement of exclusive rights by making it illegal either to circumvent TPMs or to offer services that enable circumvention.[2]

* PhD Candidate Cantab, LL.M. Harvard. The author may be contacted at pv250@cam.ac.uk.

The establishment of legal regimes for the protection of TPMs was not an easy decision though. The adoption of anti-circumvention norms and the policies that they should serve have been very controversial issues. In the debate divergent opinions have been expressed regarding the form that anti-circumvention norms should take. The EU legislature resorted to three different formulas for EU anti-circumvention norms, according to the sector which TPMs protect. In particular, anti-circumvention provisions can be found not in one or two, but in three Directives, namely in the Information Society Directive[3], in the Software Directive[4] and in the Conditional Access Directive.[5] The Software Directive and the Information Society Directive protect copyright holders of computer programs and other works protected by copyright, including broadcasts, databases and performances respectively, whereas the Conditional Access Directive protects service providers from the unauthorized reception of their conditional access services, regardless of whether they contain works protected by copyright.[6]

During the legislative process of the three Directives the Commission did not identify any reasons that would justify the differentiation in the legal treatment of TPMs according to the sector to which they are applied, nor is there any technical evidence that TPMs work differently for different forms of subject matter.[7] Hence, one may assume that the existing differentiation among the anti-circumvention provision of the three Directives would be insignificant. On the contrary, the comparison among the anti-circumvention provisions found in the Information Society Directive, the Software Directive and the Conditional Access Directive indicates that there are important differences in the established legal regimes with regard to the prohibited acts, the *mens rea* of the infringer, the circumvention means, the protected technological measures, the relation of the anti-circumvention provisions to contract law and to the limitations of copyright law.

In that regard, this paper demonstrates the practical implications of the differences in the scope of application of the anti-circumvention norms according to the subject matter protected by TPMs. The paper concludes that there are great inconsistencies within the regulation of anti-circumvention, which demand a reevaluation of the policies that led to the adoption of the current form of EU anti-circumvention norms.

2. Differences in the regulation of anti-circumvention in the EU

2.1. The prohibited acts

With respect to the Software Directive and the Conditional Access Directive the legislature opted to address the problem of circumvention at its source and solely target the intermediaries that enable consumers to circumvent TPMs instead of going against the wider public, in light of the enforcement and marketing issues that would be raised, whereas that protection was not deemed to be adequate for the protection of copyright works. Thus, the Information Society Directive condemns both circumvention *per se* and trafficking in circumvention devices, whereas the Software Directive and the Conditional Access Directive do not prohibit the act of circumvention as such.[8] In other words, the EU anti-circumvention norms condemn viewers that circumvent copy controls embedded in DVDs featuring movies but they do not target either computer program users that circumvent TPMs to copy software, or viewers that circumvent TPMs embedded in their pay-TV decoders.

Equally significant are the differences in the scope of application of the anti-circumvention norms of the three Directives with regard to the wrongful acts that facilitate circumvention. The Information Society Directive requires Member States to censure the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of circumventing devices of both access and rights controls.[9] The Conditional Access Directive targets solely commercial acts that facilitate the circumvention of access controls[10] and the Software Directive condemns "any act of putting into circulation or the possession for commercial purposes" of circumventing devices.[11]

Hence, the "possession of circumventing devices of access controls for commercial purposes" is the only wrongful act targeted by all three Directives. Illustrating how limited the common scope of application of the three Directives is, an example of such unlawful acts presents the possession of devices that circumvent access controls protecting computer programs or copyright works or the possession of illicit pay-TV decoders by a provider of a website that offers unauthorised copies of songs, films, computer programs and TV broadcasts. Still, there is ambiguity regarding the meaning of

the term "commercial use", which may create confusion and differentiation among the interpretation of the term in the context of the three Directives. In particular, the notion of "commercial use", which is not defined in the Software or the Conditional Access Directive, could vary from profit making purposes to any economic advantage.[12]

However, the differences in the types of acts targeted by the three directives are far more significant. On the one hand, the Software and the Information Society Directives have a broader scope of application in comparison to the Conditional Access Directive, to the extent that the act of "putting into circulation", and the "manufacture, import, distribution, sale, rental, advertisement for sale or rental" do not need to be conducted for commercial purposes.[13] A computer expert who loans to her friends a circumventing device for TPMs embedded in music CDs or CDs with computer programs is infringing the norms of the Information Society Directive and the Software Directive, regardless of whether she receives any direct or indirect economic advantage; in contrast thereto, the computer expert is not liable according to the norms of the Conditional Access Directive, if she loans to her neighbors her illicit pay-TV decoder.

On the other hand, the Software Directive has a more limited scope of application in comparison to the other two Directives to the extent that it does not target acts such as the "advertisement for sale or rental" or the "use of commercial communications" to promote circumventing devices or services.[14] Hence a website that advertises devices circumventing TPMs that protect computer programs is not infringing according to the anti-circumvention norms of the Software Directive. Furthermore, in contrast to the Information Society Directive, the Software Directive does not target the manufacture and import of circumventing devices for non commercial purposes, when such devices are not subsequently put into circulation.[15] In other words, the owner of copyright in computer programs cannot make use of the anti-circumvention provisions, when an end user of a program manufactured or imported a circumventing device, unless the copyright owner can prove, for example, that the end user loaned the device to third parties.

Summing up, only the Information Society Directive condemns the act of circumvention *per se*, whereas all three Directives target the making and dealing in devices that facilitate circumvention. Still, the scope of the European anti-circumvention provisions as regards the prohibited acts differs to a considerable degree. The anti-

circumvention provisions of the Information Society Directive have the broader scope of application of the three, whereas the Software Directive has a broader scope of application in comparison to the Conditional Access Directive as regards the circulation of circumventing devices, but a narrower scope of application as regards the manufacture, import and advertisement of circumventing devices.

2.2. The *mens rea* of facilitators of circumvention

Another difference of great significance among the anti-circumvention provisions of the three Directives concerns the required mens rea of the infringer. A distinction should be made between the required intent of circumventors of TPMs and the intent of people facilitating circumvention, as the two prohibitions target different groups of people and thus the interests that need to be protected by the legal order in each case differ. In particular, the actual circumventors of TPMs are the users of copyright works, the majority of whom may not have the technological knowledge to circumvent a TPM. In contrast thereto, the facilitators of circumvention are usually professionals or computer experts who manufacture or distribute circumventing devices and assist users to circumvent TPMs. As circumventing devices and services may also have additional non-infringing uses, it is crucial to determine under which circumstances the manufacturer or distributor of such devices is deemed to be infringing the anti-circumvention norms of the three directives.

The three Directives have taken completely different approaches with regard to the required intent of the persons facilitating circumvention of TPMs.[16] According to the Information Society Directive, if the means that facilitate circumvention have no other or only a limited commercially significant use other than to circumvent, then the *mens rea* of the person facilitating circumvention is irrelevant.[17] Thus, if a device is primarily used for unauthorised circumvention of TPMs, but can be used for other legitimate purposes, a person commits an offence by manufacturing and selling such a device, even if the device was genuinely manufactured or sold for legitimate purposes. If the means facilitating circumvention have a commercially significant use other than to circumvent, the anti-circumvention provisions implementing the Information Society Directive are infringed

when someone promotes, advertises or markets those means with the intent that they are used for the purpose of circumvention, or she designs, produces, adapts or performs them with the intent that they are used primarily for the purpose of enabling or facilitating circumvention of any effective TPMs.[18]

As regards the Software Directive, it has been argued that the distribution or possession of TPMs as an instance of vicarious liability does not presuppose intention or negligence, as long as the articles concerned are specifically intended to facilitate the removal or circumvention of any technical means that have been applied to protect a computer program.[19] However, this statement appears to contradict itself. The required *mens rea* of the infringer is predicated on whether the "sole intended purpose" should be found according to the understanding of a third party, for example, a neutral observer or the average distributor of anti-circumvention devices or according to the intent of the actual distributor of anti-circumvention devices. The wording of the provision which refers to "sole intended" and not to "sole commercially significant" purpose, for example, supports the second interpretation. Thus, liability according to the Software Directive is always predicated on *scienter (dolus malus)*, and in particular, the distributor of the device must intend it to be used by a third party to circumvent a TPM.

Finally, the Conditional Access Directive does not require Member States to outlaw only the intentional facilitation of illicit devices, but it provides Member States with the discretion to condemn the commercial manufacture, distribution and promotion of infringing equipment or software, only if those activities are carried out in the knowledge or with reasonable grounds to know that the devices in question were illicit.[20]

The legislative choice to outlaw the unintentional facilitation of circumvention has significant practical consequences on technological innovation. An electronics retailer who offers for sale components necessary to assemble a device that circumvents TPMs embedded in music CDs is liable for facilitation of circumvention, if those components are primarily used by the public to circumvent TPMs, regardless of whether the retailer is unaware of the destination of the components or whether she promoted them for other lawful uses. In contrast thereto, if the electronic components are used to assemble a device that circumvents TPMs which protect computer programs and those components have any other lawful use other than to circumvent effective TPMs, the

retailer is liable only if she is distributing the components with the intention to facilitate the circumvention of TPMs. Thus, the choice to outlaw the unintentional facilitation of circumvention under the Information Society Directive and also potentially under the Conditional Access Directive, causes uncertainty within the markets for electronics and inhibits the development and circulation of technologies with additional beneficial uses. In contrast thereto, owners of copyright in computer programs bear the additional burden to prove that distributors and possessors of circumventing devices intended that the devices were used to circumvent TPMs, which, however, may fuel innovation.

2.3. The means of circumvention

2.3.1. The purpose served by circumventing means

The analysis above of the required *mens rea* for the infringement of the anti-circumvention provisions targeting preparatory acts has already highlighted a significant difference between the Information Society, the Software and the Conditional Access Directives as regards the types of circumvention devices or services that fall under their scope. According to Article 6(2)(c) of the Information Society Directive a device or service is considered infringing the anti-circumvention norms if its "primary purpose" is to enable or facilitate circumvention of TPMs, whereas pursuant to Article 7(1)(c) of the Software Directive if its "sole intended purpose" should be to facilitate circumvention. A device or service that has an intended purpose other than the unauthorised removal or circumvention of TPMs applied to computer programs, for example to allow software programmed to operate with Windows also to operate with Linux, does not violate the anti-circumvention norms. However, the same device may be considered infringing, if it circumvents TPMs applied to works other than computer programs, as in that case the copyright holder needs to prove the lower "primary purpose" standard, namely that the device is primarily designed to enable or facilitate circumvention, regardless of whether it may also have intended secondary legal uses.[21] Finally, an "illicit device" does not need to satisfy even the lower "primary purpose" standard in order to invoke the application of the Conditional Access Directive, since "any equipment or software designed or adapted to give access to a protected service" falls within the scope of the provision.[22] Thus,

potential legal uses of an "illicit device" are of no importance for the application of anti-circumvention provisions protecting conditional access services.[23]

2.3.1. The nature of circumventing means: devices or services

Another important difference regarding the scope of application of the EU Directives regards the nature of circumventing means as encompassing services. This distinction is of great significance as the Software Directive and the Conditional Access Directive do not target the act of circumvention *per se*. Still, a professional who circumvents TPMs that protect computer programs or conditional access services for the benefit of third parties could be held liable if the offer of circumvention services for commercial purposes was condemned. This is not the case though for the Conditional Access Directive, whereas there is disagreement as to whether the scope of application of the anti-circumvention provisions of the Software Directive extends to services.

The Information Society Directive explicitly targets "devices, products or components or the provision of services".[24] An equally elaborate definition of "illicit devices" is included in the Conditional Access Directive, which instructs Member States to prohibit commercial acts regarding "any equipment or software designed or adapted to give access to a protected service".[25] Thus the scope of application of the Information Society Directive is broader to the extent that it also targets services enabling circumvention, whereas the Conditional Access Directive targets solely devices and code. In contrast thereto, the Software Directive targets "any means facilitating the unauthorised removal or circumvention of TPMs" without providing any further explanation regarding the meaning of the term. The broad term "any means" logically encompasses "devices, products, or components" within the meaning of Article 6 of the Information Society Directive.[26] However, there is disagreement as to whether the expression "any means" as used in the text of the Software Directive, extends to services.

Hence, although all three Directives target the provision of devices facilitating circumvention, only the Information Society Directive elaborately condemns the provision of circumvention services. The Conditional Access Directive does not target facilitators of circumvention who offer their services to third parties, whereas there is

legal uncertainty as to whether services are fall within the scope of application of the Software Directive.

2.4. Exceptions and Limitations to Copyright

The most common criticism against TPMs is that they frequently block non-infringing uses of copyright works. A number of scholars have examined the consequences of anti-circumvention regulation on the privileges enjoyed by end users according to "traditional" copyright law and they struggled with the question of whether and how anti-circumvention law could better accommodate copyright exceptions.[27] On such an important issue, the EU legislature has taken different stands as to the extent and the method that exceptions and limitations of copyright are accommodated under each Directive.

The Information Society Directive requires the protection of all TPMs that prevent or restrict uses or access not authorised by the right holders, regardless of whether the users attempting access or use can take advantage of some of the exceptions established in Article 5 of the Directive. Article 6(3) of the Information Society Directive defines TPMs as technologies designed to prevent or restrict acts "which are not authorized" by the concerned rightholders and thus it makes no reference to the technological measures that impede violation of copyright.

As a response to concerns regarding the expansion of the right of copyright holders to the detriment of the public, the Information Society Directive encourages right holders to provide a voluntary mechanism in order to make available to beneficiaries of certain exceptions permitted under the Directive the means of benefiting from them and it requires Member States to ensure that right holders do in fact make available such means.[28]

However, the Information Society Directive provides an exclusion from this requirement for "works or other subject matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them".[29] This provision effectively annuls the established voluntary method of addressing copyright exceptions in the online

environment, as the norm is that online applications allow members of the public to access works from a place and time individually chosen by them, after they have agreed to standard form contractual provisions (take-it-or-leave) set out by the provider of the work.[30] In short, the Information Society Directive privileges a rule of prevalence of contract over exceptions in the online environment.

For example, an academic who wants to copy parts of a movie for her class cannot raise the defence of "illustration for teaching" against the owner of the copyright in the movie and circumvent the TPMs that protect it. In such a case, the copyright holder is encouraged to take voluntary measures to accommodate the needs of the teacher, or else the Member State where this incident occurs shall take appropriate measures to ensure that right holders make available to the teacher the means of benefiting from that exception. However, if the protected movie is streamed online through a conditional access service, the copyright holder bears no obligation to take voluntary measures to accommodate the needs of the teacher.

As regards the Software Directive, it has been argued that Article 7(1)(c) applies also in cases where the means of circumvention are used only in order to carry out acts that do not require authorisation on the ground of an exception of a restrictive act.[31] The reasoning, which was also adopted by the High Court of England & Wales in *Sony v Ball*, is that in cases where circumvention takes place to enable the exercise of an exemption, the "sole intended purpose" of the device remains circumvention and circumvention is "unauthorised". Thus, Article 7(1)(c) is not limited to situations where the person knows or has reasons to believe that the means will be used to make infringing copies.[32] However, this reasoning does not explain what the word "unauthorized" adds to the meaning of the provision. If the legislator wished to exclude from the scope of Article 7(1)(c) only circumvention devices which have more functions, other than to circumvent, such as a personal computer, the provision would target devices the sole intended purpose of which would be to facilitate circumvention. The inclusion of the term "unauthorised" establishes a requirement that the copyright holder must have the power to prohibit circumvention on a basis other than the anti-circumvention provisions, such as copyright or contract law. The wording of the provision suggests that there should be a link between copyright infringement and infringement of the anti-circumvention provisions

and, thus, exceptions to copyright should be regarded as prevailing over the anti-circumvention norms established by the Software Directive. It is likely that the interpretation followed by the High Court was prompted by policy considerations. If the provision had been limited to situations where the person knows or has reasons to believe that the means will be used to make infringing copies, there would have been pragmatic difficulties in applying it to computer programs.

Furthermore, the Software Directive establishes a rule that certain exceptions will prevail over contractual terms, so that contractual provisions contrary to the exceptions referred to in Articles 5(2) and (3) and 6 are deemed null and void.[33] Thus, the making of a back-up copy, the observation, study or testing of the functioning of a computer program and decompilation to achieve interoperability are raised to the level of guaranteed rights of access and use, which cannot be by-passed by contractual provisions offering more protection to copyright holders.

Finally, the Conditional Access Directive does not contain within its text any limitations, or any provision regarding its relationship to copyright exceptions. The lack of explicit mention of copyright limitations led commentators to interpret Recital 21 of the Directive, which states that the Directive is without prejudice to the application of intellectual property rights, as signifying that the Directive is also without prejudice to any exceptions to intellectual property rights. Hence the relationship between the Conditional Access Directive and copyright exceptions would be unclear.[34] However such an interpretation disregards the scope of application of the Conditional Access Directive and the nature and scope of application of copyright exceptions. The copyright exceptions and limitations are defences that a defendant may rely upon when sued for copyright infringement. Hence they may be raised *vis-a-vis* copyright holders, and not towards third parties. They do not constitute an absolute right for users of copyright works. On the contrary, they allow certain uses of copyright works, which would otherwise infringe the copyright of protected works. Thus, users could raise the defence against broadcasters that they benefit from copyright exceptions, only to the extent that broadcasters raise claims based on infringement of their copyright on the broadcasts or as licensees of the copyright holders. However, the object of protection of the Conditional Access Directive is the remunerated service and not copyright. Since broadcasters enjoy a

distinct right to remuneration based on a different legal basis than copyright law, the exception to copyright cannot extend its application beyond the scope of copyright law. Furthermore, as the services in question are protected also when their content is not protected by copyright at all, logic dictates that those services will be protected also when their content is a copyright work, but users can benefit from an exception.

4. Conclusion

While the need for protection of TPMs is unequivocal according to European anti-circumvention norms, in practice, the degree of protection for TPMs varies according to the protected subject matter and is often uncertain, as the wording of the anti-circumvention provisions in the EU is complex, difficult to interpret and in some cases contradictory. Only the Information Society Directive targets the act of circumvention *per se* and the targeted preparatory acts to circumvention also differ under the three Directives. The rules clarifying the required *mens rea* of the facilitator of anti-circumvention as well as the characteristics of the circumventing means differ under the norms of the three Directives. Finally, the European legislature took different approaches to the question of whether exceptions to copyright should prevail over the anti-circumvention norms and any contractual arrangements or vice versa.

The differences in the scope of application of anti-circumvention norms according to the protected subject matter reflect different underlying policies that dictated the adoption of the one or the other approach. The choice to pursue the goals of anti-circumvention by targeting organized intermediaries who facilitate circumvention or the public who use the means made available to them entails the question of whether we should promote a "sheriff prosecution system"; on the one hand, it is more effective in shaping the conscience of the public that circumventing TPMs is illegal and thus will lessen the demand for devices and services that enable circumvention. On the other hand, it raises enforcement and proportionality issues as only an insignificant part of the infringers can be prosecuted, and thus those people will be treated as scapegoats to "scare" the rest of the public and make it conform to the "demands" of the law. Secondly, the approach taken under the Software Directive not to target the use of commercial communications aims to ensure the freedom of speech that media should enjoy and tries

to relief them from the burden of checking if what they publicise infringes anti-circumvention norms or not. A third issue of major importance is whether the anti-circumvention norms should make their enforcement easier for right holders at the cost of impeding technological innovation or vice versa. In particular, the lack of a required *mens rea* for the facilitators of circumvention and the adoption of "primary purpose" instead of "sole intended purpose", as the criterion that a device should serve in order to fall under the definition of circumventing device according to the Information Society Directive, reflect a policy choice to broaden the scope of application of the anti-circumvention provisions to entail devices and services with beneficial uses that can contribute to technological innovation; In contrast thereto, the legislature opted to allow the production and use of such devices under the Software Directive, at the cost of making the enforcement of its anti-circumvention norms less effective. Potential infringers may claim that their devices have other uses and right holders bear the additional burden to prove that the infringers were aware of the circumventing function of their devices or services. Finally, the prevalence of anti-circumvention provisions over user exceptions and limitations and contract law or vice versa is a hotly debated issue that is dealt with differently under each Directive and which allegedly affects the balance that copyright law should serve. Those concerns can be answered only after a re-evaluation of the policies that led to the adoption and to the current form of anti-circumvention norms. There is a need to explore whether different policy reasons dictate the different scope of anti-circumvention norms according to the protected subject matter, or whether the indicated differences are a result of inconsistent and inefficient protection of TPMs.

---

[1] For a detailed definition and description of TPMs see K.J. Koelman & N. Helberger, 'Protection of Technological Measures' in P. B. Hugenholtz (ed.) *Copyright and Electronic Commerce* (1998), p. 168,172; A. Strowel & S. Dusollier, 'La protection legale des systemes techniques' in WIPO Workshop on Implementation Issues of the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), WIPO doc WCT-WPPT/IMP/2, p. 2; J. De Werra, 'The Legal System of Technological Protection Measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union Directives and other national laws (Japan, Australia)', Contribution to the ALAI 2001 Conference on Adjuncts and Alternatives to Copyright.

[2] M. Ficsor, *The Law of Copyright and the Internet, The 1996 WIPO Treaties, their Interpretation and Implementation*, (2002), p. 544; S. Ricketson & J. Ginsburg, *International Copyright and Neighbouring Rights, The Berne Convention and Beyond*, (2006), p. 965.

[3] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, O.J. L167, 22/06/2001 (henceforth Information Society Directive).

[4] Directive 2009/24/EC of the European Parliament and the Council of 23 April 2009 on the Legal

Protection of Computer Programs, O.J. L111, 16, 05/05/2009 (henceforth Software Directive).

[5] Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, OJ L320, 28/11/1998 (henceforth Conditional Access Directive).

[6] A conditional access service is defined as television broadcasting, radio broadcasting or information society services, where provided on the basis of technical measures against remuneration and upon prior individual authorisation. See Article 2(a) and (b) Conditional Access Directive.

[7] On the legislative history of the three directives see: 1) Conditional Access Directive: Commission Green Paper 'on the Legal Protection of Encrypted Services in the Internal Market`, Brussels, 06/03/1996, European Parliament: tabled legislative report, 1st reading, 15/04/1998, Official Journal C 152 18.05.1998, p. 0005. A4-0136/1998, COD/1997/0198 : 30/04/1998 - EP: debates in plenary; 2) Software Directive: Green Paper on Copyright and the Challenge of Technology - Copyright Issues Requiring Immediate Action. COM (88) 172 final, 7 June 1988; Proposal for a Council Directive on the legal protection of computer programs, COM (88) 816 final, SYN 183, Submitted by the Commission on 5 January 1989, 89/C 91/05; Explanatory Memorandum; Amended Proposal of the Commission, COM (90) 509 final published OH No. C. 320. 20. 12. 90; Communication from the Commission to the Parliament SEC (91) 87 final. SYN 183 of 18.1.91; The Council's Reasons, Common Position Adopted by the Council on 13 December 1990 with a view to the adoption of a directive on the legal protection of Computer Programs, 10652/1/90. 3) Information Society Directive: *Europe and the Global Information Society-Recommendations of the High-level Group on Information Society to the Corfu European Council*, Brussels, 26 May 1994, p. 79; Commission Green Paper on Copyright and Related Rights in the Information Society, COM(95) 358 final, Brussels 19.07.1995; Commission Opinion pursuant to Article 251(2)(c) of the EC Treaty on the European Parliament's amendments to the Council's common position regarding the proposal for a Directive of the European Parliament and of the Council on the harmonization of certain aspects of copyright and related rights in the information society, COM (2001) 170 final, Brussels 29.03.2001; Proposal for a European Parliament and Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society, Explanatory Memorandum, (henceforth Explanatory Memorandum) COM(97) 628 final, Brussels, 10.12.1997 and its Explanatory Memorandum; Common Position (EC) No 48/2000 of 28 September 2000 adopted by the Council, acting in accordance with the procedure referred to in Article 251 TEC with a view to adopting a European Parliament and Council Directive of the European Parliament and of the Council on the harmonization of certain aspects of copyright and related rights in the information society, OJ C 344, 01/12/2000; Legislative resolution embodying Parliament's opinion on the proposal for a European Parliament and Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society, OJ C 150, 28/05/1999, p. 0170 Amended Proposal , OJ C 180, 25.6.1999.

[8] Compare Article 6(1) Information Society Directive to Article 7(1)(c) Software Directive and Article 4 Conditional Access Directive. Also see Report from the Commission on the implementation and effects of Directive 91/250/EEC on the legal protection of computer programs, COM (2000) 199 final, p.18l, Commission Staff Working Paper, p. 9.

[9] "Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes..."Article 6(2) Information Society Directive.

[10] Article 4 of the Conditional Access Directive targets the "manufacture, import, distribution, sale, rental or possession", the "installation, maintenance or replacement" and the "use of commercial communications to promote illicit devices" for commercial purposes.

[11] Article 7(1)(c) of the Software Directive.

[12] The term "commercial use" appears in the Rental and Lending Rights Directive, the Information Society Directive and the Enforcement Directive. Article 1(3) Rental and Lending Right Directive defines non-commercial purposes in circumscribing the public rental right as the making available for use, for a limited period of time and "for direct or indirect economic or commercial advantage".It has been suggested construing the requirement of commercial use according to the Enforcement Directive. See M. Walter, 'Enforcement Directive' in Walter & Von Lewinsky (eds.) *European Copyright Law, A Commentary*, (2010), p. 1459.

[13] Article 4(a),(b) and(c) of the Conditional Access Directive. However, many Member States, such as Belgium, France, Italy, Poland and Spain chose to additionally sanction private use of illicit devices. See

Recital 21 Conditional Access Directive and KEA & Cerna, Study of the impact on the Conditional Access Directive, study prepared on behalf of the European Commission, December 2007, available at: http://ec.europa.eu/internal_market/media/docs/elecpay/study_en.pdf.

[14] Compare Article 7(1)(c) of the Software Directive with Article 6(2) of the Information Society Directive and Article 4(c) of the Conditional Access Directive.

[15] Compare Article 7(1)(c) of the Software Directive with Article 6(2) of the Information Society Directive and Article 4(a) of the Conditional Access Directive.

[16] As regards the required intent for the act of circumventing *per se*, which is targeted only by the Information Society Directive, only the intentional act of circumvention is condemned, as the infringer circumvents the TPM "in the knowledge, or with reasonable reasons to know, that he or she is pursuing that objective". See Article 6(2)(b) Information Society Directive.

[17] "Member States shall provide adequate legal protection against the manufacture […] of devices […] which […] o*r have only a limited commercially significant purpose or use other than to circumvent* […] any effective technological measures. Article 6(2)(b) of the Information Society Directive. (emphasis added)

[18]"Member States shall provide adequate legal protection against the manufacture […] of devices […] which *(a) are promoted, advertised or marketed for the purpose of circumvention of, or*[…] *or (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of,* any effective technological measures." Article 6(2)(a) and (c) and Recital 48 of the Information Society Directive. (emphasis added).

[19] *Kabushiki Kaisha Sony Computer Entertainment Inc v Ball* [2004] EWHC 1738 (Ch); [2004] ECDR 33, 323; [2005] FSR 9; [2005] ECC 24; W. Blocher & M. Walter, 'Computer Program Directive' in Walter & Von Lewinski (eds.) *European Copyright Law, A Commentary*, (2010) p. 196, 205.

[20] See Recital 22 Conditional Access Directive. See also Decision No. 2002/13661 of the Paris Court of Appeals of 21 May 2003, which convicted a couple sued by the French pay-TV operator Canal+ for offering for sale the components necessary to assemble a pirate decoder, despite the couple's assertion that they completely ignored the destination of the components that they were promoting and selling.

[21] See also *Sony Computer Equipment v Owen* [2002] E.C.D.R. 286.

[22] Article 2(e) Conditional Access Directive.

[23] See OLG Frankfurt, judgment of 05.06.2003, 6U 7/03 – Magic Modul, which held that a device sold for lawful purposes, and which did not advertise for its potential unlawful aptitudes could be considered an illicit device. The Hamburg Court of Appeals went even further with its subsequent decision OLG Hamburg, judgment of 08.02.2006 and held that developers of software that enables users to infringe pay-TV services should do everything necessary and reasonable to avoid infringement by users, such as implementing an appropriate DRM. In contrast thereto, in Sweden and Denmark illicit devices need to be sold for the purpose of illegally decoding Conditional Access Services. However, recent case-law in Sweden reversed the burden of proof and held that when there is a massive sale of blank cards, even when they can be used for legitimate purposes, it can be presumed that their purpose of sale is for illegally decoding conditional access services.(State v. Keycard, Case 2004:17, Dnr C 4/03, June 30 2004). See Kea & Cerna, Study on the Impact of the Conditional Access Directive, Study prepared on behalf of the European Commission, p. 93-97 (December 2007), available at: http://ec.europa.eu/internal_market/media/elecpay/index_en.htm#study.

[24] Article 6(2) Information Society Directive.

[25] Article 2(e) Conditional Access Directive.

[26] L. Bently, 'Directive 91/250/EEC – Directive on the legal protection of computer programs' in Dreier & Hugenholtz, *Concise European Copyright Law* (2006); Blocher & Walter, supra note 19, p.204. *Cf* Supreme Court of Finland of 3 October 2003 *Adobe Systems v A Software Distributor* [2004] ECDR 30, 303, which held that instructions in writing enabling installation of program updates did not fall within the scope of the corresponding provision of the Finnish Copyright Act.

[27] Indicatively see P. Akester, 'Technological Accommodation of Conflicts between Freedom of expression and DRM: the first empirical assessment', (CIPIL 2009) available at http://www.law.cam.ac.uk/faculty-resources/download/technological-accommodation-of-conflicts-between-freedom-of-expression-and-drm-the-first-empirical-assessment/6286/pdf; N. Braun, 'The Interface between the protection of the Technological Measures and the Exercise of Exceptions to Copyright and Related Rights: Comparing the Situation in the United States and the European Community', 25 *European Intellectual Property Review*

496 (2003); D. Burk & J. Cohen, 'Fair Use Infrastructure for Rights Management Systems', 15 *Harvard Journal of Law & Technology* 41 (2001); S. Dusollier, 'Tipping the Scale in Favour of the Right Holders: The European Anti-Circumvention Provisions', in E. Becker, W. Buhse, D. Günnewig, N. Rump (eds.) *Digital Rights Management. Technological, Economic, Legal and Political Aspects* (2003), p.462; K. J. Koelman, 'A Hard Nut to Crack: the Protection of Technological Measures' 22(6) *EIPR* 272 (2000); J. Litman, *Digital Copyright* (2006), Chapter 9; T. C. Vinje, 'A Brave New World of Technical Protection Systems: Will There Still be room for copyright', 18 *EIPR* 431 (1996).

[28] Article 6(4)(1) Information Society Directive. In addition, Article 12(1) instructs the Commission to examine and report on a triennial basis "whether the acts which are permitted by law are being adversely affected by the use of effective technological measures".

[29] Article 6(4)(4) Information Society Directive.

[30] See also Recital 53 Information Society Directive.

[31] Bently, supra note 26, p. 235; Blocher & Walter, supra note 19, p.205.

[32] *Ibid*; See also *Kabushiki Kaisha Sony Computer Entertainment Inc v Ball*, supra note 19.

[33] Article 8(2) with Articles 5(2), 5(3) and 6 Software Directive.

[34] T. Heide, "Access Control and Innovation under the Emerging EU Electronic Commerce Framework", *15 Berk.Tech.L.J*. 993 (2000), 1018, 1043.