

DIGITAL ACCESS TO SCHOLARSHIP AT HARVARD
DASH.HARVARD.EDU

HARVARD LIBRARY


Legal Frameworks and Technological Protection of Digital Content: Moving Forward towards a Best Practice Model

Citation

Urs Gasser, Legal Frameworks and Technological Protection of Digital Content: Moving Forward towards a Best Practice Model, 17 Fordham Intell. Prop. Media & Ent. L.J. 39 (2006).

Published version

http://ir.lawnet.fordham.edu/iplj/vol17/iss1/2/

Link

http://nrs.harvard.edu/urn-3:HUL.InstRepos:13548615

Terms of use

This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material (LAA), as set forth at

https://harvardwiki.atlassian.net/wiki/external/NGY5NDE4ZjgzNTc5NDQzMGIzZWZhMGFlOWI2M2EwYTg

Accessibility

https://accessibility.huit.harvard.edu/digital-accessibility-policy

Share Your Story

The Harvard community has made this article openly available.
Please share how this access benefits you. Submit a story

Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 17, *Issue* 1 2006 *Article* 2

VOLUME XVII BOOK 1

Legal Frameworks and Technological Protection of Digital Content: Moving Forward towards a Best Practice Model

Urs Gasser*

*S.J.D. (St. Gallen), ugasser@cyber.law.harvard.edu

Copyright ©2006 by the authors. *Fordham Intellectual Property, Media and Entertainment Law Journal* is produced by The Berkeley Electronic Press (bepress). http://ir.lawnet.fordham.edu/iplj

Legal Frameworks and Technological Protection of Digital Content: Moving Forward Towards a Best Practice Model

Urs Gasser*

INTRODUCTION 40

I. OVERVIEW OF INTERNATIONAL AND SELECTED NATIONAL LEGAL FRAMEWORKS 43

A. INTERNATIONAL OBLIGATIONS 43
1. WIPO Internet Treaties 43
2. Bilateral Trade-Agreements 51
3. Conclusion 56

B. SELECTED REGIONAL AND NATIONAL LEGAL FRAMEWORKS .. 57
1. European Union 57
2. United States 62

II. DESIGNING ANTI-CIRCUMVENTION FRAMEWORKS: OPTIONS AND APPROACHES 65

A. INTRODUCTION 65

B. SELECTED APPROACHES 66
1. Subject Matter and Scope 66
a) Technological protection measure 66
b) Effectiveness 69
c) Acts prohibited: "circumvention" 72

* Associate Professor of Law, S.J.D. (St. Gallen), J.D. (St. Gallen), LL.M. (Harvard); Attorney at Law, Director, Research Center for Information Law, Univ. of St. Gallen; Faculty Fellow, Berkman Center for Internet & Society, Harvard Law School. I owe special thanks to the team at the Research Center for Information Law at the University of St. Gallen: Silke Ernst and James Thurman for research assistance and great support, and Daniel Haeusermann for his contribution to the Model Law section. In particular, I would like to thank Maja Bogataj, Ian Brown, Herbert Burkert, John Palfrey, and Derek Slater for their comments on initial drafts of this Article. Any errors, however, are entirely attributable to me. Contact information: ugasser@cyber.law.harvard.edu.

2. Limitations and Exceptions..... 75
a) Basic approaches..... 75
b) Scope of limitations and exceptions 80
3. Sanctions and Remedies 87
C. CONCLUSION 93

III. PRINCIPLES AND ELEMENTS OF A MODEL LEGISLATIVE FRAMEWORK 95

A. EXPERIENCES AND LESSONS LEARNED 95
B. DESIGN PRINCIPLES AND OUTLINE OF A MODEL LAW 102
1. Basic Principles..... 102
C. CONCLUSION 113

INTRODUCTION

Digitization in tandem with the emergence of electronic communication networks (the Internet) has changed the ways in which we create, distribute, access, and use information. In particular, digital content such as text, pictures, music, and movies can be duplicated without loss of quality and transmitted to a large number of recipients around the world at costs close to zero. As a consequence, the digitally networked environment provides manifold opportunities for users, businesses, and the public at large for rapid, inexpensive, and global dissemination of information, knowledge and entertainment. At the same time, however, the enabling technology also poses complex conceptual and practical challenges for intellectual property and related rights.

The increased ability to copy and distribute information triggered by the Internet has provoked a technological response. In order to gain back control, rightsholders have made use of so-called technological protection measures (TPM)—including, for instance, Digital Rights Management (DRM) schemes—that are aimed at regulating the copying, distribution, and use of and access to digital works through computer code ("code is law"). Activists, in turn, have immediately taken counter-measures and designed tools that enable the hacking of TPM such as copy and access controls. In response, lawmakers at both the international and national level have enacted legal provisions aimed at banning the

act of circumvention of TPM on the one hand and the production and dissemination of circumvention tools on the other hand.[1] Prominent examples of such legislation, among others, are the World Intellectual Property Organization (WIPO) Internet Treaties,[2] the Digital Millennium Copyright Act (DMCA) section 1201,[3] the European Copyright Directive (EUCD) articles 6 and 8,[4] and the respective implementations of the EUCD into the laws of EU Member States.[5]

Against this backdrop, this Article[6] takes it as its baseline that many countries have already enacted legislation or will soon legislate on TPM in order to comply either with international obligations under WIPO, or with international free trade agreements involving a party that has powerful content industries such as the U.S. Thus, the immediate question before us is no longer whether the second and third layer[7] of protection of digital works is appropriate or viable. Rather, at this stage, attention should be drawn to the alternative design choices that remain with countries that face the challenge of drafting or revisiting a legal regime aimed at protecting TPM. Consequently, the purpose of this Article is to identify different legislative and regulatory approaches and to discuss them in the light of previous experiences

---

1 *See, e.g.*, WIPO Copyright Treaty, Dec. 20, 1996, 36 I.L.M. 65, art. 11 (1997) [hereinafter WCT]; WIPO Performances and Phonograms Treaty, Dec. 20, 1996, 36 I.L.M. 76, art. 18 (1997) [hereinafter WPPT]; Digital Millenium Copyright Act, 17 U.S.C. § 1201 (2000) [hereinafter DMCA]; Council Directive 2001/29/EC, arts. 6 & 8, 2001 O.J. (L 167) 10 (EC) [hereinafter EUCD].

2 Consisting of the WCT and the WPPT.

3 17 U.S.C. § 1201.

4 EUCD, *supra* note 1, arts. 6, 8.

5 *See infra* Part 1.B.1.

6 This Article builds in part upon prior research by the author and a team of researchers at the Berkman Center for Internet & Society at Harvard Law School and the Research Center for Information Law at the University of St. Gallen (Switzerland). In this Article, however, the author shares his personal observations and expresses his personal opinion, which does not reflect the views of the institutions mentioned here.

7 *See*, *e.g.*, Jacques 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*, 189 REVUE INTERNATIONALE DU DROIT D'AUTEUR (2001) (manuscript on file with author, at 3) (discussing three layers of copyright protection that have emerged: the first is the *legal* framework of basic copyright law, the second is the *technical* means by which works may be protected, and the third is the *legal* protection against the circumvention of such technical measures.).

with TPM legislation in the U.S. and in Europe. Ultimately, the Article seeks to formulate basic design (or best practice) principles and to sketch the contours of a model law that aims to foster innovation in the digitally networked environment and minimize frequently observed spillover effects of TPM legislation.

The Article is divided into three parts. In the first part, I provide a brief overview of international and national legal frameworks that protect technological measures by banning the circumvention of TPM. The second part of the Article discusses three particularly important yet generally controversial elements of anti-circumvention legislation—i.e., subject matter and scope; exemption interface; and sanctions and remedies—and analyzes in greater detail some of the differences among jurisdictions in order to identify alternative approaches or what we may call "design choices." The third part provides a brief summary of what commentators have identified as core areas of concern with this type of legislation. Based on the findings of Parts I and II, basic design principles will be suggested. The final section paints in broad strokes a model law with discussion issues and some guiding principles that might be helpful to policy-makers who face the challenge of crafting anti-circumvention legislation.

Three caveats are necessary. First, the Article is limited in scope and does not provide an analysis of all aspects of TPM legislation that must be considered. Rather, it seeks to highlight key issues and to point to basic design choices. Second, the Article does not seek to provide a comprehensive comparative analysis of all existing anti-circumvention laws. Instead, it discusses a representative selection of interesting models and approaches taken by legislators on different continents. Third, this Article is a work in progress and therefore subject to change.

I. OVERVIEW OF INTERNATIONAL AND SELECTED NATIONAL LEGAL FRAMEWORKS

A. International Obligations

1. WIPO Internet Treaties

The so-called *third layer of protection* of digital works, i.e., the legal protection against the circumvention of technological protection measures,[8] was introduced at the international level through the WCT and the WIPO Performances and Phonograms Treaty (WPPT) both adopted on December 20, 1996, and entered into force on May 6, 2002, and May 20, 2002, respectively.[9] Neither the WIPO conventions adopted before the Internet Treaties nor the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) contained any provisions dealing with TPM.[10] The drafters of the WIPO Internet Treaties, however, could build upon prior initiatives by the WIPO itself,[11] the EU,[12] and the U.S.[13] The respective provisions setting forth obligations

---

[8] *Id.*

[9] MIHÁLY FICSOR, THE LAW OF COPYRIGHT AND THE INTERNET, § 6.01 (Oxford University Press 2002).

[10] *Id.*

[11] *See*, *e.g.*, Jane C. Ginsburg, *Legal Protection of Technological Measures Protecting Works of Authorship: International Obligations and the US Experience*, 3 Columbia Law Scl. Columbia Pub. Law & Legal Theory Working Papers, paper 0593, (2005), *available at* http://lsr.nellco.org/columbia/pllt/papers/0593 (citing further references). The idea to protect technological measures goes back to the draft WIPO Model Provisions for Legislation in the Field of Copyright in preparation for the first session of the Committee in 1989. *See* FICSOR, *supra* note 9, §§ 6.02–6.07.

[12] *See* Council Directive 91/250, art. 7(1)(c), 1991 O.J. (L 122) (EEC) (discussing the legal protection of computer programs, obligating Member States to provide appropriate remedies against a person committing "any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program"); *see, also, e.g.*, Alain Strowel & Séverine Dusolier, Legal Protection of Technological Systems, *Workshop on Implementation Issues of the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)* (World Intellectual Property Organization 1999), http://www.wipo.int/documents/en/meetings/1999/wct_wppt/pdf/imp99_2.pdf.

[13] *See* U.S. Audio Home Recording Act, 17 U.S.C. § 1002 (2000) (requiring digital audio recording devices to be equipped with Serial Copying Management Systems that

concerning technological measures—article 11 of the WCT and article 18 of the WPPT—are among the key provisions of the treaties and have a long and eventful history as far as preparatory work, consultations and negotiations are concerned.[14]

Article 11 of the WCT reads as follows:

> *Article 11*
> *Obligations concerning Technological Measures*
>
> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.[15]

Similarly, article 18 of the WPPT provides:

> *Article 18*
> *Obligations concerning Technological Measures*
>
> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law.[16]

The general wording of the two provisions—in the following paragraphs we will refer to the text of article 11 of the WCT—

disabled unauthorized serial copying of musical recordings and prohibiting devices and services aimed at circumventing the system); *see*, *e.g.*, Christine C. Carlisle, *The Audio Home Recording Act of 1992*, 1 J. INTELL. PROP. L. 335 (1994).

[14] *See* FICSOR, *supra* note 9, §§ 6.01–6.76 (discussion of the emergence of the relevant provisions in lengthy informal consultations and negotiations); *see also* Ian Brown, *The Evolution of Anti-circumvention Law*, INT'L REV. L. COMPUTERS, & TECH. (forthcoming 2006).

[15] WCT, *supra* note 1, art. 11.

[16] WPPT, *supra* note 1, art. 18.

raises a set of complex interpretative questions. Four elements are of particular interest in the context of this Article: (1) The meaning of the term "effective technological measures;" (2) the phrase "used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention;" (3) the phrase "that restricts acts, in respect of their works, which are not authorized by the authors concerned or permitted by law;" and (4) the term "effective legal remedies."[17]

(1) The WIPO Internet Treaties do not define what *technological measures* are[18] because "rapid technological advancements and the need for new adaptations in response to the repeated attempts by 'hackers' and 'crackers' to break the protection and develop means to circumvent it" make it impractical to provide a substantive definition or description of the protective technologies.[19] Not only the term "technological measures" is undefined; indeed, it also remains unclear what exactly makes such measures "*effective*." Arguably, the criterion suggests two things that may be seen as the opposite ends of a spectrum. On the one end, the term indicates that not all TPM need to be protected.[20] On the other end, it seems clear that it cannot be interpreted such that only those measures are effective

[17] WCT, *supra* note 1, art. 11. Ginsburg has also noted that a problem arises in the implementation of article 11 of the WCT, since circumventing devices or services can always be used for non-infringing purposes such as decrypting works in the public domain. Therefore, a general prohibition of all circumvention devices or services will prevent legitimate activities as well as the development of legitimate and "useful" technologies. Ginsburg, *supra* note 11, at 9.

[18] For an overview of existing techniques, see, e.g., SÉVERINE DUSOLLIER, DROIT D'AUTEUR ET PROTECTION DES OEUVRES DANS L'UNIVERS NUMERIQUE 39 et seq. (Larcier 2005).

[19] *See* FICSOR, *supra* note 9, § C11.02.

[20] *Compare* Kamiel Koelman & Natali Helberger, *Protection of Technological Measures*, Inst. for Info. Law, Amsterdam, at 8 (November 1998) (Neth.), http://www.ivir.nl/publicaties/koelman/technical.pdf *with* FICSOR, *supra* note 9, § C11.06, (questioning whether the concept of "effectiveness" has really added anything to the meaning of the provision under article 11 of the WCT) *and* FICSOR, *supra* note 9, §§ 6.67, 6.73 (explaining that the "effectiveness" criterion, introduced by an African Group during the Diplomatic Conference, was intended to narrow the scope of protection).

that cannot be circumvented.[21] Commentators have suggested, among others, the following interpretations:

- TPM that can easily be circumvented should not be legally protected.[22]
- TPM that can accidentally be circumvented should not be legally protected.[23]
- Rightsholders must put some effort into protecting their works in order to deserve protection.[24]
- Malfunctioning TPM need not be protected against circumvention.[25]
- TPM are not effective, even if they function properly, if access can be gained by other means, i.e., where another "door" exists that is not technologically locked down.[26]

Given this range of possible interpretations,[27] legislators across the world have implemented the "effectiveness" criterion in several different ways as will be discussed in greater detail in one of the subsequent sections.

(2) As mentioned above, the effective TPM must be "used by authors in connection with the exercise of their rights under

---

[21] FICSOR, *supra* note 9, § C11.03. *Cf. Universal City Studio Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000).

[22] *See* de Werra, *supra* note 7, at 10 (citing ANDRE LUCAS, DROIT D'AUTEUR ET NUMERIQUE 274 (1998)).

[23] Koelman & Helberger, *supra* note 20, at 8.

[24] *Id.* at n.26 (citing ANDRE LUCAS, DROIT D'AUTEUR ET NUMERIQUE 274 (1998)).

[25] *See* Ginsburg, *supra* note 11, at n.15 (citing JÖRG REINBOTHE & SILKE VON LEWINSKI, THE WIPO TREATIES 1996, at 145 (Butterworths 2002) for the proposition that neither malfunctioning TPM nor TPM which "interfere with the normal functioning of the equipment or services" should be protected).

[26] *See* Ginsburg, *supra* note 11, at n.15.

[27] Commentators have argued that the effectiveness criterion has been introduced to enable some contracting parties—especially the U.S.—to challenge foreign national legislations in case those national laws, in their view, would not offer a sufficient level of protection. *See* Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA. J. INT'L L. 369, 404–07 (1997); de Werra, *supra* note 7, at 10.

this Treaty or the Berne Convention."[28] This phrase clarifies that the Treaties leave it to the authors—and other rightsholders[29]—to decide whether or not to apply TPM. Furthermore, it makes it clear that the obligations under article 11 of the WCT include TPM in connection with the exercise of any right—moral or economic—that is protected under the Treaties, irrespective of the form in which the right is exercised.[30] The "rights under this Treaty . . ." element, however, leads to yet another area of uncertainty since the wording makes it questionable whether an important subset of TPM that regulates access to a work of authorship falls within the scope of the anti-circumvention provisions. Some commentators have argued that mere access-preventing technologies are excluded from the respective provisions, because neither the WIPO Internet Treaties nor the Berne Convention provide for an exclusive right to control individual access to a work.[31] The only exception applies to cases where the TPM would restrict making a protected work available to the public.[32] Others argue that access control technologies fall within the scope of the WIPO Internet Treaties, because accessing a work in digital form implicates the reproduction right under the Berne Convention given the fact that every apprehension of a digital work involves the making of a temporary copy in the user's random-access memory (RAM).[33] In addition, it is argued that access controls underpin the communication and distribution right, and that therefore Member States are obliged to protect both copy and access controls against circumvention.[34]

---

[28] WCT art. 11**.**

[29] *See, e.g.*, FICSOR, *supra* note 9, § C11.07; Ginsburg, *supra* note 11, at 5; de Werra, *supra* note 7, at 10.

[30] FICSOR, *supra* note 9, § C11.08.

[31] *See, e.g.*, Koelman & Helberger, *supra* note 20, at 9.

[32] *Id.*

[33] Ginsburg, *supra* note 11, at 7.

[34] *Id*. *See also* FICSOR, *supra* note 9, § C11.09 ("Technological measures may restrict acts . . . in various ways. There are, however . . . two basic forms of restricting . . . acts: first, restricting access to works; and, second, restricting the carrying out of certain acts in respect of works. The obligations under article 11 cover both of these basic forms. . . . ").

The implementing national legislations, too, suggest that both copy and access control technologies fall under the WIPO Internet Treaties' provisions on TPM.[35]

(3) The third important element in the context of this Article is the requirement that the technological measure "restricts acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."[36] According to this phrase, not all acts of circumvention[37] are to be prohibited under article 11 of the WCT. First, it is obvious that Member States do not have an obligation to prohibit circumventions where users are authorized by the authors or other rightsholders to engage in such an act.[38] Second, and less obvious, the wording indicates that no obligation exists under the Internet Treaties to provide adequate legal protection and effective remedies against acts of circumvention which concern acts permitted by law. The

---

[35] *See infra* Part II.B.

[36] WCT, *supra* note 1, at art. 11.

[37] The term "circumvention" is not further specified in the WIPO Internet Treaties. Thus, it is not clear from the text what acts accomplished in connection with a circumvention of TPM should be prohibited. *See, e.g.*, de Werra, *supra* note 7, at 13 (indicating that article 11 of the WCT leaves unanswered the question whether (a) the act of circumvention itself; (b) the business/trafficking in circumvention technologies ("preparatory acts"); or (c) both the act of circumvention and the business/trafficking should be declared unlawful); *see also* Brown, *supra* note 14; Strowel & Dusollier, *supra* note 12, at 6–7 (claiming that the failure to define "circumvention" will permit the signatory states to determine which acts should be proscribed and will inevitably result in regulatory variation from jurisdiction to jurisdiction). It is, however, likely that the proper interpretation entails the prohibition of both the act of circumvention itself as well as preparatory acts; for if preparatory acts are not also declared illegal, the force of the provision is essentially rendered ineffective. Firstly, actual acts of circumvention will, in most contexts, occur in the user's home and therefore the discovery of such circumvention would require a violation of privacy. Secondly, the enforcement of the provision would be far more inefficient since legal action would have to be pursued against the multitude of individual violators as opposed to the far smaller number of circumvention technology providers. *See* FICSOR, *supra* note 9, § C11.12; Ginsburg, *supra* note 11, at 8.

[38] iTunes users, for instance, are authorized to unlock Apple's DRM with the use of specific tools in order to copy playlists a restricted number of times. *See* Urs Gasser et al., iTunes: How Copyright, Contract, and Technology Shape the Business of Digital Media—A Case Study, at 41, 83 (June 2004), http://cyber.law.harvard.edu/media/uploads/81/iTunesWhitePaper0604.pdf.

> most important applications of this sentence are exceptions and limitations granted by national laws, which of course must remain within the framework set forth by the relevant provisions of the Berne Convention and incorporating treaty law.[39] Consequently, member states have no obligation to outlaw circumventions of TPM that enable users to gain access to works in the public domain or to prohibit acts of circumvention that allow users to engage in non-infringing activities according to the national legislation's limitations of or exceptions to the rights granted under the applicable laws.[40] Commentators have pointed out that the difficulty in implementing article 11 of the WCT arises with respect to the prohibition of circumvention devices and services, because such devices and services, on the one hand, are needed to legally circumvent TPM (e.g. in order to gain access to a public domain work that has been protected by TPM), but may also be used for illegal purposes on the other hand. The WIPO Internet Treaties provide no guidance as to how member states shall resolve this tension,[41] and indeed it remains the "challenge for national laws . . . to determine how to regulate the creation and dissemination of circumvention devices without effectively cutting off the fair uses that at least some devices . . . would permit."[42]

---

[39] *See* FICSOR, *supra* note 9, § C11.10.

[40] *See, e.g.*, Ginsburg, *supra* note 11, at 8; de Werra, *supra* note 7, at 11. As de Werra points out, Judge Kaplan identified one potential problem in *Universal City Studios*. Where TPM is utilized to protect new creations that are combined with works in the public domain, any circumvention to gain access to the public domain work would also provide access to the copyrighted work. The absolute prohibition against circumvention could create a new form of legal protection for works which were previously not entitled to such protection, such as works unprotected by copyright as well as works which fall under the category of "thin copyright," where there may be a greater scope of fair use. *See* de Werra, *supra* note 7, n.52.

[41] *See* FICSOR, *supra* note 9, § 6.65 (indicating that during the Diplomatic Conference hosted by WIPO in 1996, the draft provisions for the WIPO Internet Treaties were more specific: article 13 and article 22 of the Basic Proposals addressed devices or products, the "primary purpose or primary effect" of which is to circumvent and that some conference participants even suggested that the application of these provisions should be confined to devices which had the "sole purpose" of circumvention).

[42] Ginsburg, *supra* note 11, at 10.

(4) The WIPO Internet Treaties' provisions on TPM require contracting parties to provide effective legal remedies against acts of circumvention, but do not specify in detail what types of remedies must be implemented. According to one commentator, "it seems obvious that, in general, civil remedies are indispensable. . . ."[43] He also suggests that criminal sanctions are needed for preparatory activities (e.g., trafficking in circumvention devices and services) due to their "piratical" nature.[44] It has also been suggested that the TRIPS provisions on the enforcement of IPR can provide guidance as to the range of remedies that constitute effective relief.[45] However, it is important to note that the relevant provisions of the WCT and WPPT themselves are silent on this issue and, therefore, leave significant discretion to the contracting parties. The differences in implementation among national laws, as we will discuss in Part II.B.3. in greater detail, confirm this finding.

In sum, article 11 of the WCT and article 18 of the WPPT, due to their open wording, allow implementing Member States suitable liberties in transposing them into their national laws as long as the legal protection is "adequate" and the legal remedies are "effective."[46] The lack of definitions of key terms leaves not only leeway, but also causes much strife during the implementation process since different interest groups each seek to have the balance shift their way. As a result, different implementation regimes are evolving across the globe, mostly influenced by the approaches of the U.S. with the Digital Millennium Copyright Act (DMCA) and the European Union with its EU Copyright Directive (EUCD).[47]

---

43 FICSOR, *supra* note 9, § C11.13 (emphasis added).

44 *Id.*

45 Ginsburg, *supra* note 11, at 10; s*ee also* FICSOR, *supra* note 9, § C11.13.

46 *See* Communication of the WIPO Standing Committee on Copyright and Related Rights, *Current Developments in the Field of Digital Rights Management*, SCCR/10/1, at 38 (Aug. 1, 2003).

47 *See infra* parts I.B.1, I.B.2.

2. Bilateral Trade-Agreements

International obligations to adopt anti-circumvention legislation may not only derive from multinational treaty law as discussed in the previous section, but can also result from bilateral agreements. In fact, free trade agreements (FTA) between the U.S. and its trade partners have recently played an important role in diffusing the concept of third layer protection of copyrighted works through the legal protection of technological measures.[48] A recent and illustrative example is the Free Trade Agreement between Australia and the United States (AUSFTA), which aims—among other things—to strengthen the protection of intellectual property rights.[49]

---

[48] See also in this context the Kuwait-U.S. Trade and Investment Framework Agreement (TIFA), which may lead to negotiations toward a Free Trade Agreement. According to the latest submission from the International Intellectual Property Alliance with regard to the USTR Section 301 Report on Kuwait, "[t]he IPR chapter of an FTA with Kuwait would need to: (a) be TRIPS-plus; (b) include in specific terms obligations which would meet the requirements of implementing the WCT and WPPT; (c) include modern and effective enforcement provisions, including those to respond to the threats of digital and Internet piracy; and (d) contain specific commitments with regard to combating optical disc piracy through regulations on production and strict enforcement." *See* International Intellectual Property Alliance, 2006 Special 301 Report Kuwait, Feb. 13, 2006, at 282, n.7, *available at* http://www.iipa.com/rbc/2006/2006SPEC301KUWAIT.pdf.

[49] *See also* the anti-circumvention provisions in the FTA with Bahrain (Agreement between the Government of the United States of America and the Government of the Kingdom of Bahrain on the Establishment of a Free Trade Area, U.S.-Bahr., Sept. 14, 2004, art. 14.4.7, http://www.ustr.gov/assets/Trade_Agreements/Bilateral/Bahrain_FTA/final_texts/asset_upload_file211_6293.pdf); Chile (United States-Chile Free Trade Agreement, U.S.-Chile, June 6, 2003, art. 17.7.5, http://www.ustr.gov/assets/Trade_Agreements/Bilateral/Chile_FTA/Final_Texts/asset_upload_file912_4011.pdf); Jordan (Agreement between the United States of America and the Hashemite Kingdom of Jordan on the Establishment of a Free Trade Area, U.S.-Jordan, October 24, 2000, art. 4(13), http://www.ustr.gov/assets/Trade_Agreements/Bilateral/Jordan/asset_upload_file250_5112.pdf); Morocco (United States-Morocco Free Trade Agreement, U.S.-Morocco, June 15, 2004, art. 15.5.8, http://www.ustr.gov/assets/Trade_Agreements/Bilateral/Morocco_FTA/FInal_Text/asset_upload_file797_3849.pdf); Oman (Agreement between the Government of the United States of America and the Government of the Sultanate of Oman on the Establishment of a Free Trade Area, U.S.-Oman, Jan. 19, 2006, art. 15.4.7, http://www.ustr.gov/assets/Trade_Agreements/Bilateral/Oman_FTA/Final_Text/asset_upload_file715_8809.pdf); and Singapore (United States-Singapore Free Trade Agreement, U.S.-Sing., May 6, 2003, art. 16.4.7, http://www.ustr.gov/assets/Trade_Agreements/Bilateral/Singapore_FTA/Final_Texts/asset_upload_file708_4036.pdf). Similar provisions are set out in The Dominican Republic-Central America–United States Free

The relevant chapter 17 of the AUSFTA on intellectual property rights includes 29 articles and three exchanges of side letters. It endorses, *inter alia*, multilateral treaties such as TRIPS, addresses parallel importation, covers the protection of materials in digital form and distributed over electronic networks, stipulates the principle of national treatment, and extends the duration of protection for copyrighted works to 70 years after the death of the author.[50] More important for the context of this Article, the AUSFTA obliges the parties in article 17.4 paragraph 7 to provide *adequate legal protection and effective legal remedies* against the circumvention of effective technological measures.[51] This provision, in contrast, for instance, to the WIPO Internet Treaties, sets forth a detailed set of definitions. Article 17.4 paragraph 7(a), for instance, requires that each party—in order to provide adequate legal protection and effective legal remedies against the circumvention of technological measures—shall provide that any person who

> (i) knowingly, or having reasonable grounds to know, circumvents without authority any effective technological measure that controls access to a protected work, performance, or phonogram, or other subject matter; or
>
> (ii) manufactures, imports, distributes, offers to the public, provides, or otherwise traffics in devices, products, or components, or offers to the public, or provides services that:

Trade Agreement (CAFTA), art. 15.5.7, Aug. 5, 2004, http://www.ustr.gov/assets/Trade_Agreements/Bilateral/CAFTA/CAFTA-DR_Final_Texts/asset_upload_file934_3935.pdf. *See also* the draft agreement on the Free Trade Area of the Americas (FTAA), http://www.eff.org/IP/FTAA; Brown, *supra* note 14.

[50] *See, e.g.*, Urs Gasser, *Copyright and Digital Media in a Post-Napster World: International Supplement*, The Berkman Center for Internet and Society and GartnerG2, Jan. 2005, *available at* http://cyber.law.harvard.edu/media/wpsupplement2005.

[51] Australia-United States Free Trade Agreement, U.S.-Austl., May 18, 2004, 118 Stat. 919, art. 17.4.7(e)(i), *available at* http://www.dfat.gov.au/trade/negotiations/us_fta/final-text/index.html [hereinafter AUSTFA].

> (A) are promoted, advertised, or marketed for the purpose of circumvention of any effective technological measure;
>
> (B) have only a limited commercially significant purpose or use other than to circumvent any effective technological measure; or
>
> (C) are primarily designed, produced, or performed for the purpose of enabling or facilitating the circumvention of any effective technological measure,
>
> shall be liable and subject to the remedies specified in Article 17.11.13. Each Party shall provide for criminal procedures and penalties to be applied where any person is found to have engaged willfully and for the purposes of commercial advantage or financial gain in any of the above activities. Each Party may provide that such criminal procedures and penalties do not apply to a non-profit library, archive, educational institution, or public non-commercial broadcasting entity.[52]

It has been argued that the anti-circumvention framework established by the AUSFTA establishes a very protective regime that goes beyond the obligations under the relevant provisions of the WIPO Internet Treaties. Consequently, the AUSFTA necessitates further amendments to the Australian Copyright Act, which has already implemented the WIPO Internet treaties—including the provisions on technological measures—through the Australian Copyright Amendment (Digital Agenda) Act of 2000.[53]

---

[52] AUSFTA art. 17.4.7(a).

[53] These amendments have been the subject of controversy. For instance, the Copyright Agency Limited (CAL) complained that the legislation provided "less security to rightsholders than that contained in comparable overseas jurisdictions." Recommendation of Copyright Agency Limited to the Australian House of Representatives Standing Committee on Legal and Constitutional Affairs, Inquiry into Technological Protection Measures (TPM) Exceptions (October 2005), para. 14, http://www.aph.gov.au/house/committee/laca/protection/subs/sub016.pdf. Others supported a balanced approach that takes into consideration the rights of the general public. *See, e.g.*, *Review of Tecnological Protection Measures Exceptions: Hearing Before the H.R. Standing Comm. on Legal and Constitutional Affairs of the*

A recent report[54] by the Standing Committee on Legal and Constitutional Affairs of the House of Representatives, after careful review, has identified three core differences between article 17.4.7 and the current Copyright Act[55]:

> *Differences between the definition of TPM in the Act and the AUSFTA*. The Copyright Act defines a TPM in a narrower sense than article 17.4.7 by limiting the definition to devices that "prevent or inhibit the infringement of copyright."[56] Article 17.4.7, by contrast, protects a broader category of access devices that control access to copyrighted materials. In response to this broadness and its inherent problems, the above-mentioned Committee recently recommended that the provision aimed at implementing article 17.4.7 AUSFTA should clearly require a direct link between access control and copyright protection in order to avoid overprotection.[57]
>
> *Different scope of exceptions*. The current Copyright Act sets forth certain exceptions to liability for both civil actions and criminal proceedings where the circumvention device is supplied to a beneficiary of an exception for a permitted use (e.g., reproduction of computer programs for the purpose of interoperability; lawful copying by libraries, educational organizations, etc., but not "private copying"), if the person provided the supplier with a signed

Commonwealth of Australia, (Nov. 15, 2005) (statement of Jamie Wodetzki), at 2, http://www.aph.gov.au/hansard/reps/commttee/R8876.pdf.

54 Review of technological protection measures exceptions, by the Standing Committee on Legal and Constitutional Affairs, House of Representatives, The Parliament of the Commonwealth of Australia, Feb. 2006, Canberra, *available at* http://www.aph.gov.au/house/committee/laca/protection/report/fullreport.pdf. [hereinafter Report].

55 *See Report*, *supra* note 54, § 2.53.

56 In *Stevens v. Sony*, the High Court of Australia concluded that region coding devices in computer games were not technological protection measures since they do not "inhibit" copyright infringement: "The console's inability to load the software from an infringing copy does not make it impossible or more physically difficult to make an infringing copy." Stevens v Kabushiki Kaisha Sony Computer Entertainment (2005), HCA 58, para. 143 (Austl.), *available at* http://www.austlii.edu.au/au/cases/cth/high_ct/2005/58.html.

57 *Report*, *supra* note 54, § 2.61.

declaration.[58] The scope of the particular exceptions specified in the AUSFTA,[59] by contrast, is narrower.[60] The Committee's Report, however, recommends that the legislation implementing the relevant article 17.4.7 AUSFTA should maintain the existing permitted purposes and exceptions to the extent possible,[61] and should not narrow in any way the scope of the exceptions specified in the free trade agreement.[62]

Different liability rules. The current Copyright Act provides for civil actions and criminal sanctions in the case of trafficking in circumvention devices.[63] The use of such devices however—i.e., the act of circumvention itself—is not illegal, regardless of whether the TPM controls access to or protects a copyrighted work. Under article 17.4.7, in contrast, both the provision of circumvention devices as well as the act of circumvention is prohibited.[64] In addition, commentators have argued that the AUSFTA extends the scope of criminal offences related to the trafficking in circumvention devices.[65]

In sum, the previous paragraphs have demonstrated that Free Trade Agreements may contain relatively detailed provisions regarding the protection of technological measures, which may arguably go beyond the obligations under the WIPO Internet Treaties, as the example of the Australian-United States Free Trade Agreement illustrates. However, this brief discussion also suggests

---

[58] *See* WIPO Standing Committee on Copyright and Related Rights, *Current Dev. in the Field of Digital Rights Mgmt.*, (Tenth Session Nov. 3–5, 2003) (prepared by Jeffrey P. Cunard et al.) [hereinafter Cunard et al.], *available at* http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf.

[59] AUSFTA art. 17.4.7(e)(i)–(vii).

[60] *See, e.g.*, *Report*, *supra* note 54, §§ 2.66 and 3.4. *See also* David Richardson, *Intellectual Property Rights and the Australia-US Free Trade Agreement*, Research Paper No. 14 2003-04 (May 31, 2004), *available at* http://www.aph.gov.au/Library/pubs/RP/2003-04/04rp14.htm.

[61] *Report*, *supra* note 54, § 4.4; *see also* AUSFTA art. 17.4.7(f).

[62] *Report*, *supra* note 54, § 3.34.

[63] *See also id.* § 2.34.

[64] *See also id.* §§ 2.62–2.65.

[65] *See* Richardson, *supra* note 60.

that national governments, even vis-à-vis a rather detailed Free Trade Agreement, enjoy some leeway with regard to implementing legislation and regulation.

3. Conclusion

In the field of legal protection of TPM, the WIPO Internet Treaties on the one hand and bilateral trade agreements on the other hand can be seen as the main drivers of a larger trend towards harmonization—or convergence—of copyright laws in the broader sense. The rough overview provided in the first section of this Article illustrates that the WIPO Internet Treaties create a level playing field, but leave significant leeway to the parties as to the exact manner in which they implement the anti-circumvention provisions. International obligations with finer granularity with regard to TPM, however, can result from bilateral free trade agreements. The United States and other exporters of information goods and entertainment products lobby other contracting nations for such free trade agreements as a means of securing the implementation of TRIPS and WIPO standards. In some instances, the provisions on TPM set forth by such agreements may even go beyond the obligations under WIPO, as the example of the recent AUSFTA illustrates. However, experience shows that a certain degree of flexibility remains with national legislators even in the case of bilateral free trade agreements.

Against this background, the overview provided in the preceding sections draws our attention to three particularly important and controversial aspects of legislation aimed at implementing international obligations regarding TPM: first, the question of the definition of terms such as, for instance, "technological protection measures," "effectiveness" of technological measures, "acts of circumvention," and the like; second, the interface between TPM and exceptions and limitations; and third, the question of sanctions and remedies in the event of a violation of anti-circumvention provisions. These three areas, one can argue, should be of particular interest to national policy-makers for at least two reasons: On the one hand, the particular design of each element and the organization of the interplay among them greatly influence the actual scope of legal protection of TPM.

On the other hand, legislators have significant discretion with regards to the implementation of these elements in the respective national (copyright) laws and regulations,[66] as will be discussed in greater detail in Part II of this Article.

B. Selected Regional and National Legal Frameworks[67]

1. European Union

Copyright issues and related rights in Europe are governed not by a single body of law but by legislation both at the EU level and the national level. EU Member States, however, have significantly harmonized their national copyright laws since 1991 as a result of several EU Directives aimed at vertical standardization, including the Software Directive, Rental Right Directive, Satellite and Cable Directive, Term Directive, Database Directive and the Artists' Resale Rights Directive. In the specific context of this Article, the most important piece of EU legislation is Directive 2001/29/EC, better known as the European Copyright Directive (EUCD),[68] entered into force on June 22, 2001. Its purpose is twofold: (1) to harmonize the divergent European copyright regimes that were increasingly seen as an obstacle to the EU single market and as not yet ready for the information age; and (2) to transpose the WIPO Internet Treaties.[69] Still pending implementation in some Member States,[70] the EUCD sets the European Community legal framework

---

[66] The WCT does not require that protections for technological measures are enacted as part of national copyright laws. It is possible to protect them under more general laws or unfair competition law. *See* Ginsburg, *supra* note 11, at 10. For example, the Japanese provisions concerning the protection against the circumvention of *access control* measures can be found in the Unfair Competition Law. *See* FICSOR, *supra* note 9, § C11.22.

[67] A list of links to selected national legislations is provided in the Appendix.

[68] EUCD, *supra* note 1.

[69] *See, e.g.*, Michael Hart, The Copyright in the Information Society Directive: An Overview, 24 E.I.P.R. 2, at 58 (2002).

[70] France, Poland, Spain and the Czech Republic have not (fully) implemented the Directive yet. *See* Digital Media Project, EUCD—Collection of Materials, http://cyber.law.harvard.edu/media/eucd_materials. France, however, passed legislation on June 30, 2006 aimed at implementing the Directive. The text of the French legislation is available in French at http://www.assemblee-nationale.fr/12/ta/ta0596.asp. It is possible, however, that this legislation will be challenged by parlamentarians before the Constitutional Council. *See* "DADVSI Adopté: Prochaine Étape Conseil

for copyright by standardizing three fundamental exclusive rights, introducing an exhaustive list of copyright exceptions, and stipulating obligations on safeguarding TPM.[71]

With regard to the legal protection of TPM, two provisions of the EUCD are particularly important: Article 6 of the EUCD obliges EU Member States to provide for anti-circumvention provisions and deals with definitions and exceptions,[72] and article 8 of the EUCD embodies sanctions and remedies for the directive as a whole as well as with respect to article 6 of the EUCD on TPM.[73] Article 6.1 of the EUCD obliges Member States to provide "adequate legal protection against the circumvention of any effective technological measures."[74] Thus, article 6.1 clarifies at the outset that the act of circumvention itself is illegal.[75] The provision requires that persons engaged in circumvention are doing it with knowledge or reasonable grounds to know that they are pursuing circumvention of a protection measure, and that they do not have the authority to do so.[76] Article 6.3 defines "technological measures" as follows:

> For the purposes of this Directive, the expression 'technological measures' means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholders of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC.[77]

Constitutionnel," http://eucd.info/index.php?2006/06/30/334-l-ump-vote-la-pire-loi-sur-le-droit-d-auteur-en-europe (last visited July 10, 2006).

71 *See*, *e.g.*, Urs Gasser & Michael Girsberger, *Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States, A Genie Stuck in a Bottle?*, http://cyber.law.harvard.edu/media/files/eucd.pdf; Hart, *supra* note 69.

72 EUCD, *supra* note 1, art. 6.

73 *Id.*, art. 8.

74 *Id.*, art. 6.1.

75 *Id*.

76 *See*, *e.g.*, Markus Fallenböck, On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions, 7 I.J.C.L.P. 36 (2002), *available at* http://www.ijclp.org/7_2003/pdf/fallenboeck-artikel-ijclp-15-01-03.pdf.

77 EUCD, *supra* note 1, art. 6.3.

Evidently, the definition does not explicitly separate between "access control" and "copy control."[78] The ambiguity of the provision as to the protection of particular types of technological measures has led to a variety of regimes at Member State level in the process of transposing the directive, [79] as will be illustrated in Part II of the Article. The second important definition set forth in article 6.3 of the EUCD concerns the term "effective." According to this provision,

> [t]echnological measures shall be deemed 'effective' where the use of a protected work or other subject-matter is controlled by the rightholders through the application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.[80]

Again, the Member States have interpreted this rather vague concept[81] of "effectiveness" in different ways—with consequences, of course, for the concrete levels of protection of TPM across EU countries.

Contrary to article 11 of the WCT, article 6 of the EUCD clarifies that both acts of circumvention and "preparatory acts" shall be outlawed by the Member States.[82] Article 6.2 obliges Member States to provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which

> (a) are promoted, advertised or marketed for the purpose of circumvention of, or
>
> (b) have only a limited commercially significant purpose or use other than to circumvent, or

---

78 *Id.*

79 *See* Gasser & Girsberger, *supra* note 71, at 9.

80 EUCD, *supra* note 1, art. 6.3.

81 However, the EU definition frames the "the universe of protected measures," and the wording suggests that technological measures that control neither access nor copying are not considered to be "effective." Ginsburg, *supra* note 11, at 5.

82 EUCD, *supra* note 1, art. 6.

> (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of,
>
> any effective technological measures.[83]

One of the major controversies with regard to article 6 of the EUCD was the fear that TPM could create a technically executed monopoly over all uses of copyrighted works, since they can be used by rightsholders to block genuinely lawful acts such as copying permitted by exception or copying of works where the term of copyright has expired.[84] Article 6.4 of the EUCD addresses the problem where beneficiaries of certain copyright exceptions provided for in article 5 of the EUCD[85] are precluded from making use of those exceptions due to the technological lock-down of the work.[86] The exceptions set out in article 6.4 of the EUCD can be divided into two categories: the "public policy exceptions" on the one hand and the "private copying exception" on the other.[87] Article 6.4.1 of the EUCD states with regard to public policy exceptions—including exceptions in relation to photocopying, the copy and archival purposes of educational facilities, broadcaster's own ephemeral recordings, non-commercial broadcasts, teaching and research, use by disabled individuals, and public safety—that Member States "shall take appropriate measures to ensure that rightsholders make available to the beneficiary of an exception or limitation . . . the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work . . . concerned."[88] While the public policy exceptions are mandatory,

---

83 *Id.*, art. 6.2.

84 *See*, *e.g.*, Hart, *supra* note 69, at 62.

85 Article 5 of the EUCD provides a list of 21 exceptions, whereof only the exception concerning ephemeral copying is mandatory. *See*, *e.g.*, Hart, *supra* note 69, at 59.

86 Nora Braun, *The Interface between the Protection of Technological Protection Measures and the Exercise of Exceptions To Copyright and Related Rights: Comparing the Situation in the United States and the European Community* 25 E.I.P.R. 11, 496, 499 (2006).

87 *See*, *e.g.*, *id.* at 500.

88 EUCD, *supra* note 1, art. 6.4.1.

recital 51 of the EUCD clarifies that Member States should take appropriate measures only in absence of "voluntary measures taken by rightholders, including the conclusion and implementation of agreements between rightholders and other parties."[89]

As far as the "private copying exception" is concerned, Member States may—but are not obliged to—take measures "unless reproduction for private use has already been made possible by rightsholders to the extent necessary to benefit from the exception or limitation concerned . . . without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions."[90]

Finally, it is important to note that both categories of exceptions—public policy and private copying—do not apply to "on-demand" services, i.e. works "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."[91]

As mentioned above, sanctions and remedies are set out in article 8 of the EUCD. Article 8 of the EUCD covers liability for the entire directive, but specifically in article 8.1 obliges Member States with regard to the anti-circumvention provisions to "provide appropriate sanctions and remedies" and to "take all the measures necessary to ensure that those sanctions and remedies are applied."[92] Furthermore, sanctions have to be "effective, proportionate and dissuasive."[93] The provision also obliges Member States to create mechanisms for rightholders to seek damages, injunctions and the seizure of infringing material and components referred to in article 6.2 of the EUCD.[94]

---

89 *Id.*, rec. 51.

90 *Id.*, art. 6.4.2.

91 *Id.*, art. 6.4.4; *See*, *e.g.*, Alvise Maria Casellati, *The Evolution of Article 6.4 of the European Information Society Directive*, 24 COLUM.-VLA J.L. & ARTS 369, 386–90 (2001); de Werra, *supra* note 7, at 30.

92 EUCD, *supra* note 1, art. 8.1.

93 *Id.*

94 *Id.*

2. United States

In the United States, the WIPO Internet Treaties have been implemented through Title I of the Digital Millennium Copyright Act (DMCA).[95] The background of this controversial piece of legislation as well as the provisions set out by the DMCA have been discussed in a great number of reports and papers.[96] Consequently, the following paragraphs only provide a high-level overview of the Act. Specific features of the DMCA will be further discussed where particularly relevant for this Article, i.e., in the context of Part II on design options and alternative approaches taken by legislators.

In essence, the DMCA prohibits three circumvention-related activities:[97]

- Section 1201(a)(1) of the DMCA prohibits the *acts of circumvention* of "a technological measure that effectively controls *access* to a work protected under this title."[98] Notably, the scope of the provision is very broad, because acts of access control circumvention are even outlawed if undertaken for purposes that are entirely lawful (e.g. fair use) and authorized by the Copyright Act.[99] In this respect (and others), the DMCA significantly exceeds the minimal protection level as set forth by the WIPO Internet Treaties. However, as discussed below, certain exceptions may apply. Note that the DMCA, in contrast to the EUCD, does not prohibit the act of circumvention of copy control technologies.

- Section 1201(a)(2) of the DMCA prohibits a person from manufacturing, importing, offering to the public, providing or otherwise trafficking "in any technology,

95 17 U.S.C. § 1201 (2000).

96 *See*, *e.g.*, David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673 (2000); Jane C. Ginsburg, *Copyright Legislation for the Digital Millennium*, 23 COLUM.-VLA J.L. & ARTS 137 (1999).

97 *See*, *e.g.*, Ginsburg, *supra* note 96.

98 17 U.S.C. § 1201(a)(1) (emphasis added).

99 *See*, *e.g.*, Cunard et al., *supra* note 58, at 47.

> product, service, device, component, or part thereof, that . . . is primarily designed or produced for the purpose of circumventing a technological measure that effectively *controls access* to a work . . . ; has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work . . . ; or is marketed by that person . . . for use in circumventing a technological protection measure that effectively controls access. . . ."[100] Thus, the DMCA prohibits tools that can be used for circumvention purposes based on their primary design or production, regardless of whether they can or will be used for non-infringing uses. However, uncertainty remains as to the exact meaning of the criterion "primarily designed or produced."

- Section 1201(b)(1) of the DMCA, finally, prohibits the trafficking in tools that circumvent technologies that effectively protect *a right of a copyright owner* in a work or portion thereof.[101] Similar to circumvention devices intended for cracking access controls, the threshold for violation of the Act is that the device is primarily designed for circumvention purposes, or has only a limited commercially significant purpose apart from circumvention, or is marketed for use in circumventing a relevant technology.

The term "technological measure" is not defined by the DMCA. However, section 1201(a)(3)(B) of the DMCA essentially defines a technological measure that controls access to a work as effective "if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[102] Similarly, section 1201(b)(2)(B) states that a technology measure "'effectively protects a right of a copyright owner under

[100] 17 U.S.C. § 1201(a)(2) (emphasis added).
[101] *Id.* § 1201(b)(1).
[102] *Id.* § 1201(a)(3)(B).

this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title."[103] Since its enactment, a series of cases have illustrated what qualifies as technological measures, and how the effectiveness criterion and the other terms must be interpreted.[104]

The definition of the term "circumvention" is broad both in the case of sections 1201(a) and 1201(b) of the DMCA. In the context of access circumvention, for instance, the term means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[105]

The prohibition on acts of circumvention of access controls and the bans on trafficking in circumvention of access and copy control technologies have limitations and exceptions, which will be discussed in greater detail in Part III.B.2 of this Article. Concerning specific exceptions, the DMCA sets forth a number of exceptions that apply both to acts of circumvention and preparatory acts, and two exceptions that only apply to acts of circumvention. The statutory exceptions include exceptions for nonprofit libraries, archives and educational institutions, law enforcement and government activities, reverse engineering, encryption research, protection of minors, circumventions relating to personally identifying information, and security testing. Additional exceptions have been established under the so-called rule-making process under sections 1201(a)(1)(B)–(E) of the DMCA by the Librarian of Congress.[106]

The obligation under the WIPO Treaties to grant effective legal remedies against the circumvention of TPM is implemented through section 1203 of the DMCA, regarding civil remedies, and

---

[103] *Id.* § 1201(b)(2)(B).

[104] *See, e.g.*, June M. Besek, *Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media, and the Arts*, 27 COLUM. J.L. & ARTS 385, 407–12 (2004) (giving a brief overview of the relevant case law).

[105] 17 U.S.C. § 1201(a)(3)(A).

[106] *Id.* § 1201(a)(1)(B)–(E).

section 1204 of the DMCA, which provides criminal penalties. The latter provision reads as follows:

> (a) In General.—Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain—
>
> (1) shall be fined not more than $500,000 or imprisoned for not more than 5 years, or both, for the first offense; and
>
> (2) shall be fined not more than $1,000,000 or imprisoned for not more than 10 years, or both, for any subsequent offense.
>
> (b) Limitation for Nonprofit Library, Archives, Educational Institution, or Public Broadcasting Entity.—Subsection (a) shall not apply to a nonprofit library, archives, educational institution, or public broadcasting entity (as defined under section 118 (g).
>
> (c) Statute of Limitations.—No criminal proceeding shall be brought under this section unless such proceeding is commenced within 5 years after the cause of action arose.[107]

II. DESIGNING ANTI-CIRCUMVENTION FRAMEWORKS: OPTIONS AND APPROACHES

A. Introduction

Governments around the world are faced with the challenge of enacting legislation aimed at protecting TPM. In most cases, the question before legislators is no longer whether a third layer of protection of copyrighted works is economically, culturally, or socially desirable. Rather, policy-makers, while designing intellectual property rights regimes, have been and will increasingly be confronted with international obligations as outlined in Part I of this Article, thereby following a larger trend

[107] *Id.* § 1204.

towards convergence of copyright laws across the globe.[108] With regard to anti-circumvention legislation, this Article has argued that three core elements of any legal framework aimed at protecting TPM should be of particular interest to national policy-makers: definitions, exemptions, and sanctions. The contours of any given anti-circumvention regime, including its degree of openness or restrictiveness, will depend to a large extent on the particular design of each component, and the mastering of the interplay among these elements.

The following section discusses in greater detail what approaches to the three core components—to be precise, certain aspects of the three components—legislators have taken when implementing anti-circumvention provisions in accordance with international obligations. The analysis is based on prior studies by the author of the Article and focuses, by and large, on the design choices made by legislators of EU Member States, because European jurisdictions—at least at the legislative level—provide probably the richest subject of analysis from a comparative law perspective.[109] References to section 1201 of the DMCA and occasional references to anti-circumvention provisions of non-EU-countries will complement the study.

B. Selected Approaches

1. Subject Matter and Scope

a) Technological protection measure

Often at the core of anti-circumvention legislation is the term "technological protection measures" or simply "technological

[108] *See*, *e.g.*, Graeme B. Dinwoodie, *The Development and Incorporation of International Norms in the Formation of Copyright Law*, 62 OHIO ST. L.J. 733 (2001).

[109] The EU, in a sense, represents a microcosm of the international harmonization of intellectual property law, and ongoing juristic observation and study of EU developments render a certain transparency to this process. *See*, *e.g.*, http://www.euro-copyrights.org; Gasser & Girsberger, *supra* note 71; http://www.edri.org/search/node/eucd; and http://cyber.law.harvard.edu/media/eucd_materials as helpful resources for policy makers dealing with anti-circumvention laws.

measures." Obviously, the definition[110] of this term determines the scope of the relevant provisions to a great extent.[111] A significant feature with regard to the definition of TPM is whether (and, if yes, in what manner) a distinction is drawn between *access controls* and *copy controls*. As discussed in the previous sections, the distinction has not been made in the WIPO Internet Treaties, but might appear in the context of free trade agreements or at the level of regional or national legislation. Looking at norms implementing article 11 of the WCT, one might roughly distinguish between three approaches.

- First, the drafters of a given legal framework can decide not to differentiate substantively between different types of technological measures. Prominently, for instance, the EUCD has not included the distinction in the definition provided in the first sentence of the above-mentioned article 6.3 of the EUCD. However, the directive touches upon these concepts later in the same subparagraph ("through application of an access control or protection process, such as encryption, scrambling. . . ."[112]), which leads to the presumption that the EUCD does analytically distinguish between access and copy-controls but—unlike the DMCA—grants equal treatment to both types of technology. The same approach has been taken by several implementing Member States, including the U.K. and Germany.[113]

- Second, definitions in the relevant copyright acts may clearly[114] differentiate between access and copy control

[110] Note that it would be impractical and inadequate to define the term in reference to particular technologies since rapid technological change would quickly render the legislation obsolete. FICSOR, *supra* note 9, section C11.02. *Cf.* DUSOLLIER, *supra* note 18 and accompanying text.

[111] In the U.S., for instance, the issue has arisen as to whether the "rolling code" of a garage door opener constitutes a technical access protection measure. *See Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004).

[112] EUCD, *supra* note 1, art. 6.3.

[113] *See* Gasser & Girsberger, *supra* note 71, at 13.

[114] The distinction between "access controls" and "copy controls" in practice may become increasingly difficult—and ultimately in some cases impossible—to make. *See generally* Anthony Reese, *Symposium: The Law and Technology of Digital Rights*

technologies in the sense that both concepts fall within the scope of the anti-circumvention provisions, but are treated differently under the respective legal regime. The DMCA serves as a good example of this approach. As mentioned above, it prohibits the circumvention of a technological measure that "effectively controls access to a [copyrighted] work," but does not outlaw the circumvention of a copy control or other technological measure that protects a right of a rightholder.[115] As to the trafficking in circumvention devices and services, finally, the DMCA specifies that both access and copy control technologies are protected.[116]

- Third, legal frameworks may discriminate between the two basic types of TPM in a more radical form by excluding one technology from the definition. For instance in Denmark, there is some evidence that the legislature has taken the approach of excluding access controls from the definition. Although the recent amendments to the Danish Copyright Act do not explicitly refer to "access" or "copy controls," the particular wording of the Danish legislation, which emphasizes the "protection" of works and does not refer to specific types of control, may not be accidental, but reflect the earlier position of Nordic countries that article 6.3 of the EUCD excludes "access control" technology because such technology does not necessarily prevent an act that would constitute an infringement.[117] This interpretation, moreover, finds support in the explanatory text of the new Danish Copyright law, which suggests that only technological measures aimed to prevent copying are protected.[118]

Management: Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?, 18 BERKELEY TECH. L.J. 619 (2003).

[115] 17 U.S.C. § 1201(a)(1)(A)(3)(B).

[116] *Id.* §§ 1201(a)(2), (b)(1).

[117] Braun, *supra* note 86, at 498.

[118] *See* Per Helge Sorensen, *Foundation for Information Policy Research Report, Implementing the EU Copyright Directive* 34–39, http://www.fipr.org/copyright/guide/eucd-guide.pdf. Terese Foged has also expressed the view that "access control devices

> Accordingly, the Copyright Act does not protect systems that are designed to control the user's own use of the work.[119] Ultimately, of course, it remains with the Danish courts and, finally, the European Court of Justice to determine whether a particular technological measure qualifies for protection.[120]

The question of definition, of course, is not just an interesting dogmatic one, but has very practical consequences.[121]

b) Effectiveness

A second important aspect of the definition of TPM is the concept of "effectiveness." As discussed in Part I.A.1 of this Article, this criterion is not further specified in the WIPO Internet Treaties. As to implementing legislation, one can distinguish three basic approaches: First, there are anti-circumvention laws that use the effectiveness criterion as well, but leave its interpretation entirely to the courts. Second, there is the possibility of not

---

are not protected under the Danish Copyright Act." Copyright Laws in Digital Europe, Country Report Denmark (2004), http://www.euro-copyrights.org/index/4/11.

[119] A similar position is expressed in the Finnish bill 14.10.2005/821 aimed at implementing the EUCD. *See* Viveca Still, Copyright Laws in Digital Europe, Country Report Finland (2006), http://www.euro-copyrights.org/index/3/4.

[120] *See also* Foged, *supra* note 118.

[121] Consider the case of teenager Kris, living somewhere in Europe, who buys "Charlie's Angles" on DVD in a movie store while traveling to a foreign continent. Back home, Kris wants to watch the latest movie in her collection on her recently purchased laptop. However, her laptop refuses to play the DVD and displays a message that the DVD is designed to work in another region and not compatible with Kris' player. The teen calls her tech-savvy friend Jon to get advice. He suggests software available on the internet to work around the "Regional Coding Enhancement" that prevents the DVD from playing on the laptop's DVD-player. Kris follows the advice and is soon able to watch the movie. The question whether Kris is in conflict with applicable anti-circumvention laws, i.e., whether the act of "working around" the regional coding on the DVD is a prohibited circumvention of TPM, clearly depends on whether the respective legislator has taken a restrictive or a liberal approach to the definition of TPM. Under a comprehensive approach as applied in the copyright acts of the U.K., Germany and other Member States, which expressly stipulate that access control technology falls within the scope of protection, Kris would violate anti-circumvention law. By contrast, there is some likelihood that Kris could legally circumvent the regional coding of her newly purchased DVD if, for instance, Danish law were applicable. *See* Digital kopiering—hvad er lovligt?", *available at* http://www.kum.dk/sw5386.asp. The example is a shorter version of the one used by Gasser & Girsberger, *supra* note 71, at 12.

including it in the definition of TPM. Third, there are attempts in some jurisdictions to statutorily specify to some extent what effective technological measures are.

- The DMCA, for instance, belongs to the first category. Section 1201(b)(2)(B) of the DMCA, for example, states that "a technological measure 'effectively protects a right of a copyright owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts or otherwise limits the exercise of a right of a copyright owner under this title."[122] Thus, effectiveness simply "means that it hinders or prevents the relevant copyright-implicating act."[123] Against this backdrop, it is questionable whether the criterion has really added anything meaningful to the anti-circumvention provision.[124]

- A representative of the second category is Japan's anti-circumvention legislation.[125] The Japanese legislature defined technological protection measures in article 2(xx) of the Japanese Copyright Law without any reference to their effectiveness as "measures to prevent or deter acts such as constitute infringements on moral rights or copyright mentioned in Article 17, paragraph (1) or neighboring rights. . . ."[126] The term "to prevent" is not defined, while "'deter' means to deter such acts as constitute infringements on copyright, etc by causing considerable obstruction to the results of such acts . . . ."[127]

- The EU and several European Member States have taken a different approach to the definition problem by

---

[122] 17 U.S.C. § 1201(b)(2)(B).

[123] GINSBURG, *supra* note 11, at 4.

[124] *See*, *e.g.*, *id.* at 5.

[125] In Japan, the relevant provisions on TPM of the WIPO Internet Treaties have been implemented in 1999 amendments to the Copyright Law and to the Unfair Competition Prevention Law. *See, e.g.*, Cunard et al., *supra* note 58, at 91; de Werra, *supra* note 7, at 33.

[126] Cunard et al., *supra* note 58, at 91.

[127] *See* FICSOR, *supra* note 9, at C11.06.

> referring to the types of protected measures when defining the concept "effective" TPM.[128] However, the relevant article 6.3 of the EUCD remains vague. Similarly, the laws of Member States such as the U.K. and Germany that mimic the language of the EUCD also fail to provide clarification of what constitutes "effective" protection measures. However, some Member States have made some attempts to provide slightly more precise definitions. The Dutch Copyright Act, for instance, defines in article 29a(1) technological measures as effective "if the use of a protected work of the author or his successor in title is controlled by means of an access control or by application of a protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the intended protection."[129] Article 95(2) of the Hungarian Copyright Act, to take another example, states that a "technological measure shall be considered effective if as a result of its execution the work becomes accessible to the user through performing such actions—with the authorization of the author—as require the application of the procedure or the supply of the code necessary therefore."[130] However, a close reading of these definitions reveals that they have not added much to the proper understanding of the effectiveness criterion. Thus, here as elsewhere it remains a question to be answered by the courts as to what exactly qualifies as an effective measure.[131]

---

[128] EUCD, *supra* note 1, art. 6.3.

[129] *See* Kamiel Koelman & Menno Briët, Country Report Netherlands, http://eurorights.cdfreaks.com/index/1/34.

[130] Hungarian Copyright Act, No. LXXVI MK § 95(2) (1999).

[131] Again, the definition of the term "effective" has practical implications. Consider, for instance, a jurisdiction where an effective TPM would require that an average user is hindered from circumvention, as opposed to an alternative definition in another jurisdiction, where any technology would be qualified as "effective" as long as any activity towards circumvention must be undertaken in order to bypass the control system. Under the first regime, it would be at least doubtful whether the regional coding on a DVD that can easily be circumvented by average users—using a widely available piece

c) Acts prohibited: "circumvention"

As mentioned in Part I.A.1 of this Article, several important questions regarding the conduct that must be prohibited and the act of circumvention, respectively, remain unanswered under the WIPO regime. In this thematic context, the following three issues are of particular interest to national policy-makers.

- *Definition of "circumvention"*: As in the WIPO Internet Treaties, many subsequently developed national and regional laws do not specify what "circumvention" means. Neither the EUCD, for instance, nor the Japanese Copyright Law provide a definition of the term. Arguably, it has been sufficiently clear what acts constitute circumvention of a TPM.[132] The U.S. legislature, in contrast, has taken a different approach and provides a rather detailed definition of the terms "circumventing a technological measure" in section 1201(a)(3)(A) of the DMCA[133] concerning access controls and in section 1201(b)(2)(A) of the DMCA[134] concerning right controls. The definitions follow a functional approach and are not technology-specific due

of software—would fall under legal protection of TPM. When applying the lower threshold of the other jurisdiction, by contrast, it seems straightforward that regional coding would be deemed to be effective and, thus, within the scope of protection; illustrative of the latter type of regime is the U.S. case *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001). There, the district court concluded that the Content Scrambling System (CSS) on a DVD—protecting the DVD from being copied or played on non-compliant DVD players, and requiring a key that cannot be obtained without a license or the purchase of an authorized DVD player—effectively controlled access despite the fact that its weak encryption could be unlocked by a widely available software utility called DeCSS. The court held that the statute would be meaningless if it protected only successful TPM (*id.* at 457) and concluded that DeCSS was a circumvention device under section 1201(a)(2) since it was designed primarily to decrypt CSS. Consequently, Kris from the previous example could circumvent her DVD in the first jurisdiction without violation of anti-circumvention provision, even if access controls as such were protected (if effective!), but would be liable under the effectiveness-standard set forth by the relevant legislation of the second jurisdiction. *See supra*, note 121.

[132] *See* FICSOR, *supra* note 9, § C11.11.

[133] 17 U.S.C. § 1201(a)(3)(A).

[134] *Id.* § 1201(b)(2)(A).

to the rapid changes in the quicksilver technological environment.[135]

- *Prohibited conduct*: The uncertainty regarding the acts accomplished in connection with the circumvention of TPM that must be prohibited under the WIPO Internet Treaties has led to two clusters of anti-circumvention regimes. One the one hand, there are national implementations that outlaw both the act of circumvention itself as well as preparatory activities, i.e., the trafficking in circumvention devices and services. Apparently, the great majority of countries, including the U.S. and Europe, has taken this approach. However, it is important to note that laws that provide protection and remedies against both unauthorized acts of circumvention and preparatory activities may include further differentiation among acts of circumvention. It has been noted here that the DMCA, for instance, only prohibits acts of circumvention with regard to access controls, but not copy control technology. Under the EUCD, in contrast, acts against both types of protection measure are prohibited—similarly under the implementing legal regimes of the EU Member States, including the U.K., Germany, The Netherlands, Denmark, and Greece, to name only a few.[136] On the other hand, there are jurisdictions that only prohibit (certain) preparatory activities. The Japanese anti-circumvention laws, for instance, prohibit trafficking in circumventing tools as well as the offering of a circumventing service to the public, but do not specifically bar the act of circumvention.[137] However,

---

[135] *See* FICSOR, *supra* note 9 § C11.11.

[136] *See, e.g.*, Sjoera Nas, *Implementing the EU Copyright Directive, Foundation for Information Policy Research Report*, http://www.fipr.org/copyright/guide/eucd-guide.pdf.

[137] *See, e.g.*, Cunard, et al., *supra* note 58, at 91, 93; Cunard et al. as well as de Werra, however, point out that article 30 of the Copyright Law prohibits the reproduction of a work for private purposes through an act of circumvention with knowledge that the reproduction is made possible by the circumvention. *See, e.g.*, de Werra, *supra* note 7, at

it is noteworthy that Japanese copyright law does not allow the circumvention of a TPM to reproduce a work for private non-commercial purposes, although such a person making private copies would not face criminal sanctions under Japanese law.[138] Australia too, under its current copyright law, only prohibits the business of trafficking in circumventing tools (including manufacturing, selling, renting, offering for sale, promoting, advertising, marketing, distributing, and exhibiting a device), but does not prohibit the act of circumvention as such.[139]

- *Actual infringement*? As mentioned in Part I.A.1, the WIPO Internet Treaties do not require that all types of circumvention-relevant conduct must be prohibited. Only in cases where TPM restrict actions that are neither authorized by the rightsholders nor permitted by law, must acts of circumvention be declared illegal. In contrast, the text of the EUCD prohibits all acts of circumvention that are not authorized by rightholders. At the European level, the protection of TPM thus extends to situations where technology is used to prevent or restrain acts that would be exempted under the applicable copyright law, but have not been authorized by rightholders.[140] In other words, it does not matter whether any given act actually infringes a copyright or not—merely the conduct alone is relevant.[141] For this reason, several Member States

34, n. 155. Besek also contends that the act of circumvention carried out for business purposes is prohibited by the Japanese Copyright Law. Besek, *supra* note 104, at 432.

138 Cunard et al., *supra* note 58, at 92; FICSOR, *supra* note 9, § C11.22.

139 *See* Cunard, et al., *supra* note 58, at 89.

140 *See, e.g.*, de Werra, *supra* note 7, at 27; Brown, *supra* note 14.

141 *See, e.g.*, Fallenböck, *supra* note 76. Compare also the situation with the AUSFTA. In its preliminary report, the Australian House of Representatives noted that unlike the pre-existing definition of TPM under the Australian Copyright Act, the definition of TPM (aka ETM) under the AUSFTA was "not limited to devices that 'prevent or inhibit the infringement of copyright', but also includes devices that 'controls [sic] access' to protected copyright material." Several commentators were obviously disturbed by the proposed expansion of the term beyond measures aimed at preventing copyright infringement. *Report*, *supra* note 54, §§ 2.54–2.56.

> have amended their legislation to create such broad liability.[142] Hungary, however, has taken a different path. The Hungarian Copyright Act defines technological measures in article 95(2) as "all devices, products, components, procedures and methods which are designed to prevent or hinder the infringement of the copyright."[143] By using the phrase "designed to prevent or hinder the infringement of the copyright" rather than "designed to prevent or restrict acts, . . . which are not authorized by the rightholder", the Hungarian anti-circumvention provision—at least in its English version—only protects technological measures which prevent acts that are copyright infringements;[144] technologies aimed at blocking other acts which the rightholder did not authorize are not covered.

2. Limitations and Exceptions

a) Basic Approaches

All anti-circumvention frameworks that have been analyzed by the author contain, in one form or another, certain limitations and exceptions to the general proscription on circumvention. In fact, the WIPO Internet Treaties do not preclude contracting parties from creating exceptions.[145] However, implementing countries have taken approaches to limitations and exceptions that are significantly different in several respects. At a basic level, one might roughly distinguish between exceptions that follow the U.S. model versus exceptions that follow the EUCD model. The DMCA as well as anti-circumvention legislation in Australia and Japan, for instance, set out a number of limitations and exceptions to the liability for acts of circumvention and/or preparatory acts, respectively. These exceptions are essentially a defense to a

---

[142] *See* Gasser & Girsberger, *supra* note 71, at 16 (giving further references and explaining the Dutch implementation of the EUCD as a case in point).

[143] Hungarian Copyright Act, No. LXXVI MK § 95(2) (1999).

[144] *Id.*

[145] *See, e.g.*, Cunard et al., *supra* note 58, at 50.

prohibited circumvention-related act,[146] while there are no statutory obligations placed on rightholders to provide beneficiaries with the means of taking advantage of the exceptions and privileges.[147]

Article 6.4 of the EUCD, by contrast, "does not introduce exceptions to the liability of the circumvention of technological measures in a traditional sense, but rather introduces a unique legislative mechanism which foresees an ultimate responsibility on the rightholders to accommodate certain exceptions to copyright or related rights."[148] With regard to the public policy exceptions mentioned in Part I.B.1, article 6.4.1 of the EUCD invites rightsholders to take voluntary measures, including agreements between them and "other parties concerned" (e.g. consumer electronics manufacturers, consumers and vendors of TPM, etc.), in order to ensure that the beneficiary of an exception or limitation can benefit from the respective exceptions or limitations.[149] In the absence of such voluntary measures or agreements within a reasonable period of time,[150] Member States are obliged to "take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law . . . the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or

[146] *See, e.g.*, *id.* at 73. The EUCD, as discussed in the subsequent section, takes a different approach by suggesting that Member States may permit certain acts that TPM are supposed to accommodate. *Id.*

[147] *See, e.g.*, Besek, *supra* note 104, at 398. Section 1201(a)(1)(B)–(E) of the DMCA provides for a possible open-ended group of exceptions. *See* FICSOR, *supra* note 9, § C11.26.

[148] Braun, *supra* note 86, at 499. *See also* Cunard et al., *supra* note 58, at 72; de Werra, *supra* note 7, at 30.

[149] EUCD, *supra* note 1, art. 6.4.1.

[150] Recital 51 in part reads as follows: "Member States should promote voluntary measures taken by rightholders . . . to accommodate achieving the objectives of certain exceptions or limitations provided for in national law in accordance with this Directive. In the absence of such voluntary measures or agreements *within a reasonable period of time*, Member States should take appropriate measures. . . ." (emphasis added). Similarly, recital 52 states "[i]f, *within a reasonable period of time*, no such voluntary measures to make reproduction for private use possible have been taken, Member States may take measures to enable beneficiaries of the exception or limitation concerned to benefit from it. . . ." (emphasis added). EUCD, *supra* note 1, rec. 51.

limitation and where that beneficiary has legal access to the protected work or subject-matter concerned."[151]

Against this backdrop, the European framework leaves member states with two options. First, Member States might immediately take steps in order to ensure that the beneficiaries of copyright exceptions can in fact benefit from the exception despite technical protection measures and the lack of voluntary measures on the part of rightholders. Second, Member States—due to uncertainty with regard to future technological developments and business practices in the field of protection measures—might pursue a "wait-and-see" strategy and only intervene later on if practical need for legislation has become evident. The latter approach has been taken by both Austria and the Netherlands. The Dutch legislature, however, has provided more guidance with regard to possible exceptions. Article 29a(4) of the Dutch Copyright Act and, *mutatis mutandis*, article 19 of the Neighboring Rights Act,[152] empower (but do not oblige) the Minister of Justice to issue a decree setting forth obligations for rightsholders to provide means enabling certain uses such as usage by people with disabilities, uses for educational purposes, reprographic reproductions, reproduction for preservation purposes, use of judicial and administrative proceedings, etc.[153] Notably, the list also includes cross-references to the private-copy exceptions in the Dutch Copyright Act.[154]

With regard to the first approach, where Member States immediately establish mechanisms for the enforcement of copyright exceptions in absence of voluntary measures, there has been some variation in the methods applied by individual Member States. In the context of the EUCD's public policy exceptions,[155]

---

[151] *Id.* art. 6.4.

[152] Koelman & Briët, *supra* note 129.

[153] *Id.*

[154] *Id*. *See* Sjoera Nas, *Implementing the EU Copyright Directive, Foundation for Information Policy Research Report*, 102-05, http://www.fipr.org/copyright/guide/eucd-guide.pdf.

[155] As discussed below, a special regime governs the private copying exception set forth in article 6.4.4 of the EUCD.

one can distinguish three approaches:[156] mediation, administrative complaints procedure, and direct access to courts.[157]

- Greece and Lithuania, for example, rely on mediation for the enforcement of the rights of beneficiaries of exceptions in the absence of private agreements to facilitate those rights.[158] Similarly, the beneficiaries of an exception under Slovenian Law may also request mediation.[159]

- The United Kingdom, however, has introduced a special administrative procedure to ensure the observance of copyright exceptions. The relevant provision states that in cases "[w]here the application of any effective technological measure to a copyrighted work other than a computer program prevents a person from carrying out a permitted act in relation to that work then that person . . . may issue a notice of complaint to the Secretary of State."[160] The Secretary of State, acting through the U.K. Patent Office, will then open an investigation in order to explore "whether any voluntary measure or agreement relevant to the

[156] Other approaches exist outside the EU, *see, e.g.*, article 39b of the Swiss draft for the implementation of the WIPO Internet Treaties, which installs a TPM Panel ("Fachstelle") that observes the impact of technological protection measures. The Federal decision on the approval of WCT and WPPT in German or French is available at http://www.ige.ch/E/jurinfo/j103.shtm.

[157] The following paragraphs are derived from an earlier study conducted by the author, *see* Gasser & Girsberger, *supra* note 71, at 17–23.

[158] For Greece, see Article 66A(2) of the Law 3057/2002. For Lithuania see article 75(4) of the Copyright Act of the Republic of Lithuania ("When owners of copyright, related rights and *sui generis* rights do not take measures (i.e. do not provide with decoding devices, do not conclude agreements with the users of the rights, etc.) which would enable the users to benefit from the limitations . . . the users . . . may apply to the Council for mediation in such dispute. The mediator(s) shall present proposals and help the parties to reach agreement. . . . If the parties do not accept a proposal of the mediator(s), the dispute shall be settled by Vilnius regional court.") *See* Republic of Lithuania, Law amending the law on copyright and related rights, 5 March 2003, No. IX-1355, official translation (on file with author).

[159] *See* article 166c of the Copyright and Related Rights Act of the Republic of Slovenia, as amended by the Act Amending the Copyright and Related Rights Act, Official Gazette RS No. 43/04.

[160] Copyright and Related Rights Regulations, 2003, c. 48, § 296ZE(2) (Eng.).

copyright work the subject of the complaint subsists."[161] If this investigation leads to the conclusion that there is no subsisting voluntary measure or agreement, the Secretary of State may[162] give a direction requiring the copyright holder or the exclusive licensee to ensure that the complainant can benefit from the permitted act. According to section 296ZE(6) of the Copyright and Related Rights Regulations, the obligation to comply with the direction is a duty owed to the complainant or, where the complaint is made by a representative of a class, to the representative as well as each person in the body represented.[163] It is noteworthy that a failure to comply with a direction would result in a breach of statutory duty, which is actionable by the complainant or a representative of a body of complainants.[164]

- Ireland, in contrast, has implemented a procedure whereby the beneficiaries of exceptions apply directly to the Irish High Court. Section 374(3) of the Irish Copyright and Related Rights Act states: "In the event of a dispute arising, the beneficiary may apply to the High Court for an order requiring a person to do or to refrain from doing anything the doing or refraining from doing of which is necessary to ensure compliance by that person with the provisions of this section."[165] Although the Irish approach is quite unique among the

---

[161] *Id*. § 296ZE(3)(a).

[162] The Consulting Paper clarifies that the Secretary of State, despite the use of the word "may", has a duty to act, and that if he did not act when action should be taken the matter could be subject to judicial review. *See* UK Patent Office, *Consultation on UK Implementation of Directive 2001/29/EC on Copyright and Related Rights in the Information Society: Analysis of Responses and Government Conclusions*, at 13, http://www.patent.gov.uk/about/consultations/responses/copydirect/copydirect.pdf.

[163] Copyright and Related Rights Regulations, c. 48, § 296ZE(6) (Eng.).

[164] However, the procedure only applies where a complainant has lawful access to the copyrighted work, and it does not apply to works "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." *Id.* § 296ZE(9).

[165] As amended by S.I. No. 16 of 2004, European Communities (Copyright and Related Rights) Regulation 2004, http://www.entemp.ie/publications/sis/2004/si16.pdf.

EU Member States, Germany and Luxembourg have also provided beneficiaries with a statutory right to seek injunctive relief.[166]

b) Scope of limitations and exceptions

Anti-circumvention frameworks may provide both general limitations and specific exceptions to the prohibition of acts against TPM. With regard to general limitations, the U.S. legislation (DMCA) is illustrative. For the purposes of this Article, two limitations—among others—are particularly interesting: 1) the relationship between section 1201 and copyright infringement, including fair use; and 2) the so-called non-mandate provision.[167]

- "*Fair Use*": Section 1201(c)(2) of the DMCA states that the anti-circumvention regime does not affect rights, remedies, limitations or defenses to copyright infringement, including fair use. At a glance, the wording suggests that fair use activities will be protected, i.e., that fair use is a defense against a section 1201(a)(1) of the DMCA claim to argue that the circumvention was done for legal purpose covered by fair use. However, "as courts interpreting the provision have found, it is clear that any rights and defenses under copyright law are separate from and not affected by the new rights, remedies and exceptions of the anti-circumvention provisions."[168] Thus, there is no fair use defense in the sense just mentioned. However, a recently introduced bill by U.S. Representative Rick Boucher—The Digital Media Consumer's Rights Act of

[166] *See* Copyright Act § 95b(1) and Injunctions Act §§ 2a, 3a (Germ.) (English translation by Menno Briët & Alexander Peukert, http://www.euro-copyrights.org/index/14/51); Cunard et al., *supra* note 58, at 77–79; section 71quinquies(2) of the Luxembourgian Copyright Act (entitling the beneficiaries of an exception (or their representatives) to take injunction proceedings) (English translation by Corentin Poullet, available at http://www.euro-copyrights.org/index/10/22).

[167] *See* Cunard et al., *supra* note 58, at 49–52 (analyzing general limitations).

[168] *Id.* at 49 (referencing *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2nd Cir. 2001)).

2005 (H.R. 1201)[169]—seeks to restore the legal use of digital content and scientific research.[170]

- *"No mandate provision*": Section 1201(c)(3) of the DMCA contains a so-called "no mandate" provision[171] aimed at clarifying that the prohibition of circumvention devices does not require manufacturers of computers, consumer electronics, and telecommunications products to affirmatively design their products to respond to any particular technological measure. In other words, as long as a product does not affirmatively engage in circumventing a TPM or otherwise fall within the prohibitions, it will not violate section 1201 of the DMCA. However, commentators have argued that the meaning of this provision is not entirely clear. Furthermore, section 1201(k) of the DMCA mandates an affirmative response for a particular type of technology—analog videocassette recorders—which must be designed to

[169] The bill is available at http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.1201. For an overview, see, for example, Public Knowledge, http://www.publicknowledge.org/issues/hr1201.

[170] Sec. 5 (b) on Fair Use Restoration (*id*.) reads as follows:
Section 1201(c) of title 17, United States Code, is amended—
(1) in paragraph (1), by inserting before the period at the end the following: 'and it is not a violation of this section to circumvent a technological measure in order to obtain access to the work for purposes of making noninfringing use of the work'; and
(2) by adding at the end the following new paragraph:
(5) Except in instances of direct infringement, it shall not be a violation of the Copyright Act to manufacture or distribute a hardware or software product capable of substantial noninfringing uses.
Digital Media Consumers' Rights Act, H.R. 1201, 109th Cong. (2005). *See also* Timothy K. Armstrong, Digital Rights Management and the Process of Fair Use, 20 HARV. J.L. & TECH. ___ (forthcoming 2006) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=885371 (discussing the viability of a technological solution—i.e. that DRM systems may be designed to accomodate fair use rights).

[171] The EUCD, by contrast, does not include such a provision. See, however, recital 48: "Such legal protection implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6." EUCD, *supra* note 1, rec. 48.

> conform to certain defined technologies aimed at preventing unauthorized copying.[172]

As mentioned above, all anti-circumvention regimes contain several specific exceptions, which of course may vary significantly with regard to subject matter and scope. Depending on the particular design of the anti-circumvention framework,[173] these exceptions apply to acts of circumvention, to preparatory acts, or in some instances to both types of conduct. While the previous section has made clear that legislators across the world have taken different approaches to the enforcement of exceptions, the following paragraphs seek to categorize some of the most important exceptions from a substantive perspective. The focus is on the DMCA and the EUCD.

With regard to the exceptions under the DMCA, one has to distinguish between statutory exceptions on the one hand and exceptions to the prohibition of circumventing access control technologies concerning particular classes of works stipulated by the Librarian of Congress on the other hand. Section 1201 of the DMCA contains seven specific and narrow statutory exemptions that apply to the act of circumvention of access controls. Five of them also apply to provisions that prohibit the trafficking in circumvention technologies. The seven exceptions have been discussed elsewhere in great detail; in this Article, it suffices to enumerate them:

- Nonprofit libraries, archives and educational institutions, under certain conditions, may circumvent TPM solely for the purpose of gaining access to the work in order to determine whether the relevant institution wishes to purchase it.[174]

- Law enforcement, intelligence and other government agencies, where authorized, are not subject to either the ban on acts of circumvention nor the prohibition of

---

172 *See, e.g.*, de Werra, *supra* note 7, at 23.
173 *See supra* Section II.B.1.(c).
174 17 U.S.C. § 1201(d).

trafficking in circumvention technologies set out in sections 1201(a) and 1201(b).[175]

- Reverse engineering of a computer program by a person who has lawfully obtained a copy of that program is permitted under a series of restrictive conditions.[176]
- Encryption research is permitted if the researcher has lawfully obtained a copy, the act is necessary for research and does not constitute a copyright infringement, and the researcher made a good faith effort to obtain authorization.[177]
- Protection of minors can justify an exception to the prohibition on circumvention for a technology that has the sole purpose of preventing minors from accessing material on the Internet.[178]
- The act of circumvention is permitted where the TPM collects or disseminates personally identifying information gathered in the course of online activities if certain criteria are met.[179]
- Security testing of a computer, computer system, or network is permitted with the authorization of the owner. This exception, if other conditions are met, allows both the act of circumvention as well as the development, distribution, and use of technological means for the respective testing purpose.[180]

In response to concerns that section 1201(a)(1) of the DMCA would negatively affect traditional fair uses of copyrighted materials due to the ban on circumventing access controls, the U.S. Congress established a process that requires the Librarian of

---

[175] *See id*. § 1201(e).

[176] *Id*. § 1201(f). *See, e.g.*, Ginsburg, *supra* note 11, at 149.

[177] 17 U.S.C. § 1201(g); *see also* DMCA Section 104 Report, A Report of the Register of Copyrights Pursuant to § 104 of the Digital Millennium Copyright Act (August 2001), http://www.copyright.gov/reports/studies/dmca/sec-104-report-vol-1.pdf.

[178] 17 U.S.C. § 1201(h).

[179] *Id.* § 1201(i).

[180] *Id.* § 1201(j).

Congress to determine every three years whether certain classes of works and persons are likely to be adversely affected in their ability to make non-infringing uses by the respective provision.[181] The process also requires the Librarian of Congress to define particular classes of works as to which the act of circumvention by a particular person would be permitted.[182] Currently, under the second rulemaking proceeding,[183] the Librarian of Congress, upon the recommendation of the Copyright Office, has created exemptions for four classes of works—including computer programs, video games, and e-books—if very specific criteria are met.[184]

As discussed in the previous section, the EUCD has taken a significantly different approach to exceptions than that found in the DMCA. However, article 6.4 of the EUCD sets out a set of specific exceptions that should be accommodated by the rightsholders. From a design perspective, three issues are noteworthy:

- First, the EUCD does not distinguish between types of technical protections in those provisions aimed at obliging Member States to accommodate the beneficiary of exceptions.[185]

- Second, the exceptions listed in article 6.4.4 of the EUCD apply only to acts of circumvention as defined in article 6.4.1 of the EUCD, but not to preparatory acts. Thus, in sharp contrast to the DMCA, one must conclude that Member States are not entitled to introduce any exceptions to the anti-trafficking prohibition stated in article 6.2 of the EUCD.[186]

---

[181] *Id.* § 1201(a)(1)(B).

[182] *Id.* § 1201(a)(1)(D).

[183] The Copyright Office is about to conduct public hearings in the third anti-circumvention rulemaking proceeding in March 2006. *See generally* http://www.copyright.gov/1201/index.html.

[184] *See* Rulemaking on Anticircumvention, http://www.copyright.gov/1201/2003/index.html.

[185] *See, e.g.*, Braun, *supra* note 86, at 499.

[186] *Id.* However, note that computer software is protected under Directive 91/250/EEC, which imposes decompilation exceptions. Council Directive 91/250/EEC, art. 6(1), 1991

- Third, it is a special feature of the European legislation that it differentiates, as already noted, between public policy exceptions on the one hand and the private copying exception on the other hand.[187]

The public policy exceptions listed in article 6.4.1 of the EUCD include the following:[188]

- Reproduction on paper or a similar medium by photographic or other technique with similar results on the condition that rightholders receive fair compensation.[189]
- Specific acts of reproduction made by libraries, museums, educational institutions and archives, which are not for direct or indirect economic or commercial advantage.[190]
- Ephemeral recordings of works made by broadcasters.[191]
- Reproduction of broadcasts by social institutions such as hospitals and prisons for noncommercial purposes and provided that rightsholders receive fair compensation.[192]
- Use for the sole purpose of illustration for teaching or scientific research.[193]
- Uses for the benefit of people with a disability where the uses are directly related to the disability, non-

O.J. (L 122) 42 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:EN:HTML.

187 *See, e.g.*, Braun, *supra* note 86, at 500.

188 The first four exceptions involve the reproduction right. The last three involve both the reproduction right as well as the right of communication to the public.

189 EUCD art. 5.2(a).

190 *Id.* art. 5.2(c).

191 *Id.* art. 5.2(d).

192 *Id.* art. 5.2(e).

193 *Id.* art. 5.3(a).

commercial in nature, and to the extent required by the specific disability.[194]

- Uses for the purpose of public security or to ensure the proper performance of administrative, parliamentary or judicial proceedings.[195]

In addition, recital 48 of the EUCD states that TPM should not hinder research into cryptography,[196] and recital 51 of the EUCD clarifies that the legal protection of technological measures applies without prejudice to public policy as reflected in article 5 of the EUCD, or public security.

While the public policy exceptions are mandatory as noted above, private copying exceptions are not. As discussed elsewhere,[197] incumbent EU Member States have not made broad use of the possibility to take measures ensuring that private copying exceptions will survive technological protection measures. One of the most visible exceptions, however, is Italy,[198] where article 71sexies (4) of the Italian Copyright Act grants a limited "right" to make one copy—which can be in analog form—for personal use, notwithstanding the fact that the work is protected by technological measures, as long as the user has obtained legal access and under the condition that the act neither conflicts with the normal exploitation of the work nor unreasonably prejudices the legitimate interests of the rightholder.[199] The diagnosis of an overall trend against a "right to private copying" in the age of

---

194 *Id.* art. 5.3(b).

195 *Id.* art. 5.3(e).

196 Brown points out that "because of the obscure legal status of recitals, this requirement has only been given explicit effect in a small number of member states such as the UK." Brown, *supra* note 14, at 11.

197 *See* Gasser & Girsberger, *supra* note 71, at 17–25.

198 The Luxembourgian Copyright Act also exempts reproduction for private use, but the explanatory statement declares: "En relation avec l'exception pour copie privée . . . il est entendu que les titulaires de droits ne peuvent être empêchés d'adopter et de garder en place des mesures adéquates en ce qui concerne le nombre de reproductions." 71quinquies(1)(No. 2) of the Luxembourgian Copyright Act (Lux.), *available at* http://www.euro-copyrights.org/index/10/26; *see, e.g.*, Corentin Poullet, Country Report Luxembourg, http://www.euro-copyrights.org/index/10/20.

199 Decreto Legislativo 9 Aprile 2003, n.68, in Gazzetta Ufficiale 14 Aprile 2003, n.87 (Italy), *available at* http://www.parlamento.it/parlam/leggi/deleghe/03068dl.htm.

technological measures seems to be confirmed by recent court rulings in France,[200] Belgium,[201] and Germany.[202] Several of the new EU member states, by contrast, have implemented the private copying exception, among them, for instance, Lithuania,[203] Malta,[204] and Slovenia.[205]

Another unique (and, in the view of the author, highly problematic) feature of the EUCD is that both the public policy exceptions as well as the private copying exception do not apply to works "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."[206] Previous analyses have suggested that it remains unclear what the exact scope of this "interactive on-demand service" provision is, both at the level of the EUCD and the national implementations.[207]

3. Sanctions and Remedies

Under the WIPO regime, contracting parties have to provide adequate legal protection and effective legal remedies against the circumvention of TPM. As discussed in Part I of the Article, the WIPO Internet Treaties do not provide much guidance as to what types of sanctions and remedies should apply. Thus, it is particularly interesting to observe how signatories such as Australia, the EU and European Member States, Japan, and the U.S. have implemented the relevant provisions. Of particular interest are the questions of what ways and under what circumstances have the national legislators made use of civil and/or criminal sanctions.

---

[200] Cass. 1e civ., Feb. 28, 2006, Bull. civ. I, No. 549 (Fr.), *available at* http://www.zdnet.fr/i/edit/ne/2006/02/arretcassation.pdf.

[201] La cour d'appel de Bruxelles 9ème chambre, Sept. 9, 2005 (Belg.), *available at* http://www.droit-technologie.org/jurisprudences/appel_bruxelles_090905.pdf.

[202] Bundesverfassungsgericht [Federal Constitutional Court] July 25, 2005, 1 *BvR* 2182/04 (F.R.G.), *available at* http://www.bverfg.de/entscheidungen/frames/rk20050725_1bvr218204.html; *see also* http://constitutionalcode.blogspot.com/2005/09/german-constitutional-court-private.html.

[203] *See* Copyright Act of the Republic of Lithuania art. 75(1).

[204] *See* Maltese Copyright Act as amended by Act No. IX of 2003 art. 9(1)(c), 42(2)(a).

[205] *See* Copyright Act of the Republic of Slovenia art. 50(1), 166c(3)(3).

[206] EUCD, *supra* note 1, art. 6.4(4).

[207] *See*, *e.g.*, Gasser & Girsberger, *supra* note 71, at 25.

Copyright legislation in Australia and Japan, as noted above, primarily prohibits preparatory acts, i.e., the trafficking in circumvention devices and services, but not—or, in the case of Japan, only exceptionally—the act of circumvention itself. Despite this relative similarity, the two jurisdictions have established different liability rules. The current Australian Copyright Act provides for both civil actions and criminal sanctions in the case of trafficking in circumvention devices.[208] The civil remedies include an injunction and either damages or an accounting of profits.[209] Reportedly, punitive damages are also available in the case of flagrant breaches.[210] Further, rightsholders can bring actions for conversion or detention of circumvention devices that are used to make infringing copies.[211] Criminal sanctions include fines and imprisonment up to five years.[212] Under the Japanese Copyright Law, only criminal remedies are available.[213] However, certain civil remedies (including demand for cessation, disposal, and destruction of illegal circumvention tools) are available under Japan's unfair competition law.[214]

The DMCA provides for both civil remedies and criminal sanctions.[215] Principal civil remedies are temporary and permanent injunctions, as well as actual damages, in addition to the award of ill-gained profits and statutory damages. The latter may range from USD 200 to USD 2,500 for each act of circumvention or circumvention product for a violation of section 1201 of the DMCA and from USD 2,500 to USD 25,000 for a violation of section 1202 of the DMCA.[216] Further, awards can be adjusted in the case of repeat offenders.[217] Conversely, the court "may reduce

---

208 *See* Cunard et al, *supra* note 58, at 92.

209 *Id*.

210 *Id*.

211 *Id*.

212 *Id*.

213 The explanation is that no civil action is possible because at the time that a circumventing device is introduced, it would not be clear which works would be circumvented by it and, accordingly, which copyright owner would have the right to seek an injunction. *See id.* at 97.

214 *See*, *e.g.*, Besek, *supra* note 104, at 432.

215 17 U.S.C. §§ 1203, 1204.

216 *Id.* 17 U.S.C. § 1203 (c)(3); *see, e.g.*, Cunard et al., *supra* note 58, at 53.

217 17 U.S.C. § 1203 (c)(4).

or remit the total award of damages in any case in which the violator sustains the burden of proving, and the court finds, that the violator was not aware and had no reason to believe that its acts constituted a violation."[218] In addition, criminal sanctions in the form of a fine and/or imprisonment are available if someone violates section 1201 of the DMCA "willfully and for purpose of commercial advantage or private financial gain."[219]

The situation in Europe is less transparent and, from a design perspective, probably even more interesting. As noted, article 8 of the EUCD requires member states to provide for effective sanctions and remedies for infringements of rights and obligations as set out in the directive, but does not specify the details. Some clarification, however, comes from recital 58 of the EUCD, which states that the sanctions should be "effective, proportionate and dissuasive and should include the possibility of seeking damages and/or injunctive relief and, where appropriate, of applying for seizure of infringing material."[220] An analysis of some approaches to sanctions and remedies taken by EU Member States suggests that Member States have interpreted article 8 of the EUCD in different ways.[221] In fact, significant differences remain with regard to the interpretation of the Member States' obligation to provide for "appropriate sanctions and remedies" as laid down in article 8.1 of the EUCD.[222] While all countries impose civil sanctions in the case of a violation of anti-circumvention provisions, differences remain with regard to criminal sanctions. By and large, one might distinguish between three approaches on a spectrum from restrictive to liberal:[223]

- A comparatively *restrictive approach* has been taken, for instance, by Greece. The Greek Copyright Act prohibits the circumvention of effective technological protection measures and bans, in accordance with

[218] *Id.* § 1203 (c)(5)(A). *See, e.g.*, de Werra, *supra* note 7, at 17–18 (suggesting that the user of a circumventing deep link might be a good candidate for this "innocent violations" exception).

[219] 17 U.S.C. § 1204 (a).

[220] EUCD, *supra* note 1, rec. 58.

[221] Gasser & Girsberger, *supra* note 71, at 25-29.

[222] EUCD, *supra* note 1, art. 8.1.

[223] *See* Gasser & Girsberger, *supra* note 71, at 28–29.

article 6.2 of the EUCD, "the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes" of circumvention devices or services.[224] Article 66(4) of the Greek Copyright Act states that "the practice of activities in violation of the above provisions is punished by imprisonment of at least one year and a fine of 2,900–15,000 Euro."[225] It also entails civil sanctions, including payment of damages, pecuniary penalty, personal detention, restitution to the rightholder of illicit profits, etc.[226] The one-member First Instance Court may order an injunction in accordance with the Code of Civil Procedures."[227] Apparently, all these sanctions apply both to acts of circumvention and trafficking in circumvention devices.

- The United Kingdom, for example,[228] marks *middle ground* by providing civil remedies, but restricting criminal sanctions to acts of circumvention for non-private and commercial uses. More specifically, the Copyright, Designs and Patents Act provides a new civil remedy against a person who "does anything which circumvents [technological protection] measures knowing, or with reasonable grounds to know, that he is pursing that objective."[229] Remarkably, both the copyright owner (or her exclusive licensee) and a person issuing copies of the work to the public or communicating it to the public have the same rights[230]

---

[224] *See* Nomos (2121:1993) [Greek Copyright Act], 66A(2), 66(A)(3) (Greece).

[225] *Id.* at 66(4).

[226] *Id.* at 65; *see* Vassilis D. Maroulis, *Implementing The EU Copyright Directive, Foundation for Information Policy Research Report* at 79–84, http://www.fipr.org/copyright/guide/eucd-guide.pdf.

[227] The Code of Civil Procedures also allows seizure of the objects constituting proof of infringements or the creation of a detailed inventory of such objects. *See* Maroulis, *supra* note 226, at 82.

[228] Germany falls in the same category. *See, e.g.*, Gasser & Girsberger, *supra* note 71, at 26–27.

[229] Copyright and Related Rights Regulations, 2003, c. 48, § 296ZA(1)(b) (Eng.).

[230] *See id.* § 296ZA(4) (stating that copyright owner and person issuing copies have concurrent rights).

against an alleged infringer as those in an infringement action.[231] Apparently, the mere circumvention of technological protection measures, contrary to the Greek approach mentioned above, does not trigger any criminal sanctions as long as it is conducted for private and non-commercial use. Sections 107 and 198, however, make it a criminal offence to infringe copyright by communicating the work to the public in the course of business or to an extent that prejudicially affects the rightholder.[232] Sections 296ZB and 296ZD create a new offense and a new civil remedy, respectively, in relation to trafficking in devices and services which circumvent effective technological protection measures.

- Illustrative of a *relatively relaxed approach* to sanctions and remedies is Denmark. The Danish Copyright Act also prohibits the circumvention of effective technological measures and outlaws trafficking in circumvention devices or services.[233] A violation of the provisions of TPM creates both civil and criminal liability. As in other jurisdictions, rightholders might seek injunctions in order to prevent violation, or may claim damages according to the general tort rules that are applicable.[234] Moreover, section 78(1) states that anyone "who with intent or by gross negligence violates section . . . 75c is liable to a fine." Remarkably, however, the Danish law does not provide for

[231] *See id.* § 296ZA(3). Intent to infringe is not required, *see, e.g.*, Ian Brown, *Implementing the EU Copyright Directive*, Foundation for Information Policy Research Report, 123, http://www.fipr.org/copyright/guide/eucd-guide.pdf.

[232] Arguably, these provisions apply to situations where a "pirate" circumvents technological protection measures and, for instance, distributes the hacked file over P2P networks. In fact, the new offenses were designed with online piracy in mind; *see* The Patent Office, *Implementation of the Copyright Directive (2001/29/EC) and related matters, Transposition Note*, art. 8, http://www.patent.gov.uk/copy/notices/2003/copy_direct3a.htm.

[233] *See* Danish Copyright Act, Lov nr. 618 of June 27, 2001, as amended by Lov nr. 1051 of Dec. 17, 2002, § 75c(1)–(3).

[234] *See, e.g.*, Sorensen, *supra* note 118, at 39.

> imprisonment in the context of a violation of the anti-circumvention provisions. Reportedly, the Commission on Cyber Crime under the Ministry of Justice—supported by rightholders organizations—has recommended increasing these relatively mild sanctions.[235] It is expected that this proposal will be put forward once it has been discussed more broadly.[236]

In the context of remedies set out in the EUCD, it is noteworthy that the new Intellectual Property Enforcement Directive (EUIPD)[237] has introduced new enforcement measures across Europe to ensure a high, equivalent, and homogeneous level of protection of intellectual property rights in the EU common market. The directive, *inter alia*, requires that Member States provide measures for preserving evidence by plaintiff's agents ("Anton Piller orders"), precautionary seizure of the alleged infringer's property (including blocking bank accounts), and new powers to demand disclosure of personal and/or commercial information, along the lines of the subpoena powers granted by the DMCA in the US.[238] The directive applies to any intellectual property infringements, including non-commercial infringements, although some remedies only apply to commercial infringements. The EUIPD must be implemented by the Member States by April 29, 2006.[239] Additionally, the EU Council and Parliament have taken measures to introduce criminal sanctions to combat piracy and counterfeiting. In this regard, proposals for a Parliament and Council Directive as well as a Council Framework decision were

---

[235] *Id.*

[236] *Id.*

[237] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, Official Journal of the European Union, Nr. L 157 of 30 April 2004, 16–25, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_195/l_19520040602en00160025.pdf.

[238] In addition, committees of the EU Parliament and the Council are working on two pieces of legislation aimed at criminalizing piracy and counterfeiting. *See EU plant Strafen gegen "Urheberrechts-Piraten* (June 14, 2004), http://www.heise.de/newsticker/meldung/48232.

[239] EUIPD, *supra* note 237, art. 20.

published on July 12, 2005[240] and are expected to be debated in the EU Council by the end of April 2006.[241]

C. Conclusion

Part I of this Article has argued that the WIPO Internet Treaties and, to a lesser extent, international obligations under bilateral free trade agreements leave significant leeway regarding the implementing legislation and regulation aimed at legal protection of technological measures. Against this backdrop, three subject areas have been identified that should be of particular interest to national policy-makers. Part II of the Article, consequently, has identified, discussed and compared some of the design choices that have been made by implementing countries, especially the U.S. and the European Union as well as selected EU Member States.

The brief review of various approaches to definitions, exceptions, and sanctions/remedies that have been taken by governments around the world in connection with anti-circumvention legislation has confirmed the finding of Part I. In fact, the analysis illustrates that implementing countries have significant options in creating their legal TPM environment. Further, the analysis has demonstrated that the above-mentioned three elements are at the core of any anti-circumvention framework, and that these elements, to a great extent, shape the characteristics of a given legal and regulatory regime aimed at governing TPM. More precisely, the design of each core element

---

[240] Commission Proposal for a European Parliament and Council Directive and a Proposal for a Council Framework Decision, COM (2005) 276 final (July 12, 2005), *available at* http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0276en01.pdf. The Directive calls for the Member States to establish intentional infringement of intellectual property rights on a commercial scale as well as attempting, aiding, abetting, or inciting such an infringement as criminal offenses. It also outlines the type of penalties and law enforcement actions which should be implemented into national law for such offenses. The proposed Framework Decision provides more explicit instructions with regard to criminal penalties as well as potential changes to the national legal systems of the Member States that are deemed necessary for the facilitation of the Directive's goals. *Id.*

[241] *See Intellectual Property: Strengthening the Fight against Counterfeiting and Piracy, Criminal Measures Aimed at Ensuring the Enforcement of Rights*, http://www.europarl.eu.int/oeil/FindByProcnum.do?lang=2&procnum=COD/2005/0127 (describing the procedure announced by the European Parliament).

and the tuning of its interplay with the other elements determine the degree of openness/permissiveness or closeness/restrictiveness of a given anti-circumvention framework. Choosing narrow definitions of key terms such as "technological measures," "effectiveness," and restrictive interpretations of the prohibited conduct will generally lead to a more permissive legal framework. Broad exceptions, on the other hand, may also contribute in important ways to a relatively balanced protection framework where users are provided with more options with regard to digital content (for example, making a private copy, using content for research or creative expression, etc.) Finally, the conservative use of criminal sanctions at the legislative level also contributes to a more permissive environment—and vice versa, of course. Obviously, the three elements can be crafted in many different ways and balanced against each other to achieve (or better *approximate*) the desired policy equilibrium. Broad definitions of subject matter and scope, for instance, could be synchronized with broad exceptions, sanction regimes combined with narrow definitions, etc.

Thus, the fundamental question for policy-makers and legislators becomes what type of anti-circumvention frameworks they seek to craft: a relatively open/permissive regime or a relatively closed/restrictive one from the user's perspective? This policy question, due to its interdependencies with other elements of the digital ecosystem, is a very complex one. Its answer depends on a series of context-specific factors, including the underlying agenda of the anti-circumvention legislation; the features of existing copyright law and its interplay with anti-circumvention provisions; the relation and synchronization between anti-circumvention legislation and other pieces of legislation such as, for instance, unfair competition laws, contract law, criminal law, etc.; the tension with core values of a society such as free speech and privacy, and so forth. Obviously, the necessary determinations are country (and culture) specific and can not be generalized. However, before providing a "laundry list" of issues to be addressed while drafting anti-circumvention legislation,[242] it may

[242] *Supra* Part III.B.2.

prove helpful to have a quick look at current practical experiences that have been gained with anti-circumvention legislation such as section 1201 of the DMCA or Article 6 of the EUCD.

III. PRINCIPLES AND ELEMENTS OF A MODEL LEGISLATIVE FRAMEWORK

A. Experiences and Lessons Learned

The experiences with anti-circumvention provisions are limited. Although much has been written about the merits and demerits of TPM in general and anti-circumvention legislation in particular,[243] it remains unclear—as an empirical matter—what exactly the effects of the third layer of protection of copyrighted materials are. However, there is plenty of anecdotal evidence that suggests some lessons learned, although this type of evidence—depending on possible selection biases and the interpreters' viewpoints—often leads to conflicting assessments of the legislation's merits. Further, most of the qualitative analyses have to be read against the background of the core values of Western societies.[244] In fact, given the date of inception of anti-circumvention laws, most comments focus on experiences with the DMCA in the U.S. and, most recently, with the EUCD and corresponding national implementations in Europe.

As stated in the introduction, this Article purposefully does not focus on the question whether anti-circumvention legislation as

---

[243] *Compare* Stan Liebowitz, *Policing Pirates in the Networked Age*, Cato Policy Analysis, No. 438 (May 15 2002), *available at* http://www.cato.org/pubs/pas/pa-438es.html (affirming effectiveness of TPM, including DRM, and corresponding legal schemes aimed at fighting (online) piracy), *with* Peter Biddle, et al. *The Darknet and the Future of Content Distribution* (2002), *available at* http://crypto.stanford.edu/DRM2002/darknet5.doc, *and* Ed Felten, *DRM and the First Rule of Security Analysis*, Freedom to Tinker (Mar. 19 2003), at http://www.freedom-to-tinker.com/archives/000317.html, *and* Urs Gasser et al., *supra* note 38 (questioning the effectiveness of such measures) *with* Charles Nesson & Sarah Hsia, *Conference Overview and Background: Digital Media Distribution—Speedbumps Scenario*, at http://cyber.law.harvard.edu/digitalmedia/nesson_hsia_overview.html (stating a moderate position).

[244] For an exceptional view, see Electronic Frontier Foundation et al., *Digital Rights Management: A Failure in the Developed World, a Danger to the Developing World*, 14–15, http://www.eff.org/IP/DRM/drm_paper.php [hereinafter *Failure*].

such is necessary, appropriate or desirable at all. Rather, the starting point is pragmatic in the sense that it acknowledges legal obligations and political pressures which have led and will lead to widespread implementation of third layer protection in the laws of nation-states. Against this backdrop, it seems appropriate to use anecdotal evidence in order to flag problem areas that are associated with DMCA- and EUCD-like pieces of legislation. Scholars and practitioners alike have identified a significant number of unintended consequences and problems associated with this type of legislation. Anti-circumvention laws on both sides of the Atlantic have shown a tendency, *inter alia*, to

- promote digital "lock up";
- inhibit fair use, fair dealing, and other copyright privileges;
- limit access to public domain works;
- prevent legitimate research, including reverse engineering and encryption research;
- generally inhibit the free flow of information and freedom of expression;
- be misused to prevent legitimate competition;
- disadvantage disabled users;
- decrease consumer autonomy; and
- threaten privacy.[245]

This Article, however, touches upon three—in part overlapping—areas of concern with regard to the (side-)effects of anti-circumvention provisions such as section 1201 of the DMCA and article 6 of the EUCD: concerns that relate to what we might call autonomy and participation; issues related to innovation; and (negative) impacts on competition. The summary below does not seek to provide a detailed analysis of each issue,[246] but shall draw

[245] *See, e.g.*, Besek, *supra* note 104, at 467–69. For an excellent overview with critical commentary and further references, see Brown, *supra* note 14 (discussing the problematic implications of the DMCA and, to the extent possible, the EUCD on issues such as legitimate competition and competition law, the interests of disabled persons, security research, freedom of expression, consumer protection, and privacy).

[246] *See, e.g.*, Christophe Geiger, *The Private Copy Exception, An Area of Freedom (Temporarily) Preserved in the Digital Environment*, 37 Int'l Rev. Intell. Prop. &

attention to fundamental challenges associated with the design of anti-circumvention laws and may provide some guidance as to how the contours of such a framework should look in order to avoid, minimize or at least manage problematic—usually spillover—effects of anti-circumvention legislation.

- *Autonomy and Expression*: As discussed elsewhere,[247] user autonomy is among the basic values of Western democratic societies. Autonomy in the Internet age includes at least three elements. First, an individual must have the freedom to make choices among alternative sets of information, ideas, and opinions. Second, informational autonomy necessitates that everyone has the right to express their own beliefs and opinions. Third, autonomy in the digitally networked environment arguably requires that every user can participate in the creation of information, knowledge, and entertainment. Against the backdrop of this notion of user autonomy, experiences with the DMCA and the EUCD have given rise to the claim that anti-circumvention legislation inhibits free speech. It does not come as a surprise that this concern has been emphasized in the U.S. with its extensive constitutional free speech protection. Anecdotal evidence suggests that the DMCA in particular has been used to stifle free speech, e.g. in the context of the publication of security standards, vulnerability research, and the like. (Here, the concern for freedom of expression overlaps with innovation as a policy goal, see below.)[248] Further, user autonomy in the sense outlined above is impaired by

Competition L. 74 (2006); Nimmer, *supra* note 96; Koelman & Helberger, *supra* note 20; *see also infra* notes 241–253 and accompanying text.

[247] Urs Gasser, *The Good, The Bad, and The Ugly: Information Quality on the Internet* (unpublished manuscript, on file with author).

[248] *See, e.g.*, Electronic Frontier Foundation, *Unintended Consequences: Five Years under the DMCA*, 2–7 (Sept. 24, 2003), http://www.eff.org/IP/DMCA/unintended_consequences.pdf [hereinafter "Unintended Consequences"] (citing illustrative examples involving Section 1201 of the DMCA); *see also* Besek, *supra* note 104, at 484–85 (discussing U.S. cases that have presented the argument that the DMCA violates the Free Speech Clause of the First Amendment of the U.S. Constitution by limiting the distribution of anti-circumvention software).

the fact that anti-circumvention provisions often inhibit fair uses of copyrighted materials through the protection of access control technologies that restrict the ability to access materials and take advantage of fair use and similar privileges.[249] Similarly, user's autonomy (e.g. the ability to engage in creative expression) is hampered in cases where the access to public domain works is limited based on TPM and supplementing legislation.[250] Furthermore, TPM and corresponding legislation can exclude certain users such as, for instance, disabled people, where code prevents them from enjoying the same commercial products available to the non-disabled.[251]

- *Competition:* Another area of concern relates to potentially anti-competitive effects of anti-circumvention legislation.[252] Manufacturers and

[249] *See, e.g.*, *Unintended Consequences*, *supra* note 248, at 7–9; Julie Cohen, *Call it the Digital Millennium Censorship Act—Unfair Use*, THE NEW REPUBLIC, May 23, 2000 (discussing Microsoft's threats against the online forum Slashdot.com); *see also* Besek, *supra* note 104, at 480–84 (noting that fair use concerns with regard to the DMCA are "overstated" but that "an area of genuine concern" remains); Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. ___ (forthcoming 2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=885371. If DRM design policy could be reoriented toward including consideration for the preservation of users' rights, a DRM system which both protected the interests of rightsholders and preserved fair use might emerge. In such a manner, fair use concerns might be addressed without resorting to the problematic overhaul of the current international legal framework surrounding TPM. *See id.*

[250] *See, e.g.*, *Comments of Peter Decherney, Assistant Professor at the University of Pennsylvania's Cinema Studies Program, Michael Delli Carpini, Professor and Annenberg Dean, and Katherine Sender, Assistant Professor at the University of Pennsylvania's Annenberg School of Communication, In the Matter of Rule Making: Exemption to Prohibition on Circumvention of Copyright Systems for Access Control Technologies,* Docket No. RM 2005-11, at 11, *available at* http://www.copyright.gov/1201/2006/comments/decherney_upenn.pdf; Besek, *supra* note 104, at 499–500.

[251] *See, e.g.*, *Failure*, *supra* note 244, at 14–15; *Comments of the American Foundation for the Blind, In the Matter of Rule Making: Exemption to Prohibition on Circumvention of Copyright Systems for Access Control Technologies*, Docket No. RM 2005-11, *available at* http://www.copyright.gov/1201/2006/comments/discipio_afb.pdf.

[252] For a recent analysis of the DMCA's anti-competitive effects, see Timothy B. Lee, *Circumventing Competition, The Perverse Consequences of the Digital Millennium*

vendors of goods such as toner cartridges, garage door openers, video game consoles, and video games, among others, have used the anti-circumvention provisions of the DMCA and the EUCD in attempts to reinforce their dominant market positions by preventing the interoperability of products on alternative systems.[253] Although most of these attempts have not been successful in the end, the cases—and some rulings by lower courts—give reason to consider the danger of potential strategic misuses of the anti-circumvention provisions by rightholders aimed at hindering their legitimate competitors. However, the *intended use* of anti-circumvention provisions might additionally have important ramifications for competition. A prime case-in-point is the business model developed by Apple with its iTunes Music Store (iTMS).[254] Anti-circumvention provisions support Apple's particular business strategy in at least two respects. First, it prevents Apple's competitors from reverse engineering the DRM system FairPlay to create competing portable players. Second, due to the preservation of the exclusive DRM, free-riding of the iTMS by compatible players is prevented. As a consequence, the product enhancing benefits of the iTMS with regard to iPod are preserved. Although beneficial from the business angle, Apple's ability to limit interoperability in order to increase iPod sales, from a policy perspective, might arguably not render

Copyright Act, (Cato Policy Analysis, No. 564, March 21, 2006), *available at* http://www.cato.org/pub_display.php?pub_id=6025.

[253] *See, e.g.*, *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004); *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 253 F. Supp. 2d 943 (E.D. Ky. 2003); *see also* Urs Gasser, *Copyright in a Post-Napster World: International Supplement*, at 20, http://cyber.law.harvard.edu/media/files/wpsupplement2005.pdf, (discussing the Italian decision of the Tribunale di Bolzano, 31 Dec. 2003, involving Sony Playstation consoles); John Palfrey, *Holding Out for an Interoperable DRM Standard in* DIGITAL RIGHTS MANAGEMENT: THE END OF COLLECTING SOCIETIES? (Christoph Beat Graber et al. eds., 2005) (discussing interoperability issues).

[254] *See* Gasser et al., *supra* note 38, at 40–44.

the optimal welfare enhancing result, and it is likely to harm consumers.[255]

- *Research and Innovation:* A series of cases and stories involving section 1201 of the DMCA intensifies the concern that TPM, in tandem with legal protection regimes, might have negative impacts on legitimate scientific research and, ultimately, may impede innovation. This concern, of course, is a particularly serious one in countries (like the U.S.) where copyright law attempts to achieve a delicate balance between creators' interests in controlling and profiting from their works on the one hand and the public's interest in using those works and fostering innovation on the other hand. Many commentators have pointed out, for example, that anti-circumvention laws like the DMCA—largely due to overly narrow exceptions—prevent legitimate research activities involving reverse engineering and the investigation of improved encryption methods.[256] The development of encryption science and the building of advanced encryption methods, for example, requires testing activities by scientists of existing encryption methods—acts which could involve attempts to circumvent or defeat TPM for the purpose of identifying flaws and developing more secure systems.[257] Illustrative (and rather dramatic) examples in this context are liability threats by a multi-industry group against a team of Princeton researchers[258] and criminal sanctions against a Russian programmer working on a software tool to copy e-books without the

[255] The mere existence of different DRM and codec standards imposes additional costs on consumer and hardware producers. Further, in many cases, several economies of scale are forgone through the separation of consumers into different incompatible subgroups. *See id.* at 44–48.

[256] *See, e.g.*, Besek, *supra* note 104, at 469.

[257] *Id.* at 509.

[258] *See Unintended Consequences*, *supra* note 248, at 2; *see also* Pamela Samuelson, *Anti-Circumvention Rules: Threat to Science*, Science, Sept. 14, 2001,Vol. 293. no.5537, at 2028–31, available at http://www.sciencemag.org/cgi/content/abstract/293/5537/2028.

> rightholder's permission.[259] In the context of scientific and educational (but also cultural) information, further concerns have emerged with regard to negative effects of DMCA-like legislation on libraries in their role as important access providers. Arguably, anti-circumvention provisions tend to preclude libraries (like other beneficiaries) from making use of traditional exceptions to copyright protection, which have allowed them to copy, share, or lend materials and, instead, may force them (e.g., under the EUCD regime) into negotiations with rightholders to obtain TPM-free materials or the permission to circumvent TPM in restricted circumstances.[260] In the same category—and overlapping with the issues mentioned under the heading of autonomy/expression, especially fair use—fall restrictions on *teaching* activities, if one considers teaching/learning to be a key prerequisite for and driver of innovation. It has been argued that anti-circumvention laws enable rightholders to prevent educational uses that have been exempted under the analog regime.[261]

In conclusion, the previous remarks have made clear that DMCA-like legislation has produced significant spillover effects in important policy areas such as informational autonomy and user participation, competitiveness of markets, and research and innovation, among others. Given experiences and analyses so far, it is not speculative to conclude that anti-circumvention laws in the tradition of the WIPO Internet Treaties have shown an inherent tendency to endanger certain social values as noted above.

---

[259] *See Unintended Consequences*, *supra* note 248, at 4.

[260] *See Failure*, *supra* note 244, at 16.

[261] *See, e.g.*, Jeff Sharp, *Coming Soon to Pay-Per-View: How the Digital Millennium Copyright Act Enables Digital Content Owners to Circumvent Educational Fair Use*, 40 AM. BUS. L.J. 1, 38–39 (2002). Thus, for instance, it would be illegal under the DMCA for film studies professors—despite fair use, the classroom use exemption, and the TEACH Act—to circumvent the TPM (CSS) on a DVD to create clip compilations from different DVDs to show, say, how movie makers have conceptualized different emotions during class. *See* Jacqueline Harlow, *Draft Case Study: Film Studies and the Law of the DVD*, Berkman Center (2005) (on file with author).

Whatever the assessment of these unintended consequences may be, it is important that policy-makers facing the challenge of introducing (or reforming) anti-circumvention legislation are aware of these areas of concern and seek to minimize unintended consequences of such legislation based on the past experiences of other jurisdictions.

B. Design Principles and Outline of a Model Law

1. Basic Principles

Part II of this Article and the previous section have analyzed, *inter alia*, what approaches to TPM legislation have been taken and what consequences (intended as well as unintended) certain design choices might have. For the reasons discussed in Part II.C. above, it is not feasible to provide detailed substantive guidance as to how an anti-circumvention framework should look without knowing the specifics of the legislative, judicial, cultural, economic, and political environment of the implementing country. However, it is possible, based on the analysis in this Article, to suggest three basic subject-matter design principles that should be taken into account by policy-makers when drafting and enacting anti-circumvention laws:

> *Principle 1: Get the terminology right (i.e., provide precise, clear, and unambiguous definitions of key concepts and terms such as "technological (protection) measures," "effective" TPM, "acts of circumvention," etc.).* The analysis of existing anti-circumvention laws in different jurisdictions across continents suggests that legislators, by and large, have done a poor job in defining core terms of anti-circumvention. Although it is true that laws often use abstract terms that require interpretation, it is striking how many vague concepts and ambiguous terms have been identified within the context of TPM legislation. The EUCD, as it has been transposed into the laws of the EU Member States, is particularly illustrative of this point since it leaves it up to the national courts and, ultimately, to the European Court of Justice to define some of the basic terms

used in the respective pieces of legislation.[262] In particular, legislators should avoid merely "copying and pasting" provisions as set out by international treaties or other sources of norms without making deliberative choices about the concepts and terms that are used. As demonstrated in the previous Parts of this Article, definitions of terms are crucial for achieving a certain level of legal certainty and limiting the scope of the anti-circumvention laws.

Principle 2: Recite traditional limitations and exceptions to copyright in the context of anti-circumvention provisions. The review of exception-regimes under various legal frameworks, as well as the overview of initial experiences with anti-circumvention legislation in the U.S. and in Europe, has suggested that anti-circumvention provisions tend to change the carefully balanced allocation of rights and limitations previously embodied in the respective national copyright laws. Particularly significant shifts can be observed in areas such as research (including reverse engineering), teaching, and traditional user privileges such as fair use or the "right" to make private copies. Apparently, not all of these shifts have been intended or anticipated by policy-makers.[263] Thus, it is crucial to carefully design the exception-framework applicable to TPM, provide appropriate mechanisms for the effective enforcement of exceptions, analyze the interplay of the exception-regime with the other core elements of the anti-circumvention framework, and conduct an in-depth impact analysis.

Principle 3: Use discretion with regard to sanctions and remedies and adhere to the principle of proportionality. International legal frameworks provide some degree of

---

[262] *See* Gasser & Girsberger, *supra* note 71, pp. 16 et seq.

[263] *See, e.g.*, Digital Media Consumers' Rights Act, H.R. 1201, 109th Cong. (2005) (considering reform proposals). Hearings on the effects of anti-circumvention legislation have been held in several EU member states, including the U.K. *See, e.g.*, http://www.theregister.co.uk/2006/02/02/apig_hears_evidence/.

> flexibility in drafting civil and criminal penalties. Implementing countries should carefully consider the available design choices under the applicable framework, thereby following the principle of proportionality. Among the usual options to be considered are limitations on criminal and civil liability for non-profit institutions such as libraries, archives, and educational institutions, flexible sanctions for innocent infringers, and limitations on sanctions for legitimate purposes such as scientific research and teaching. Again, the interplay among the liability provisions and the other elements of the framework, including scope and exceptions, must be equilibrated.

The review of various controversies—both in practice and theory—surrounding the implementation and application of anti-circumvention frameworks suggests, as noted above, that both the intended effects (e.g., on piracy, enabling certain business models)[264] as well as the unintended consequences of third layer protection of copyright (e.g. on competition, innovation, etc.) remain uncertain and contested. In this situation of uncertainty and in light of anecdotal evidence suggesting spillover effects, policy-makers are well advised to complement the three principles outlined above by two more general principles.

> *Principle 4: Incorporate procedures and tools that permit the monitoring and review of the effects of the anti-circumvention provisions on core values of a given society.* Given the degrees of uncertainty mentioned above, it is crucial to establish mechanisms that enable policy-makers and stakeholders to systematically identify and assess the effects of TPM and corresponding legislation and, thus, to incorporate what we might call the ability to learn and improve based on "law in action." Such processes and tools might include legislative, administrative, or academic review and might focus, among others things, on the core

[264] For an overview of DRM-enabled content services, see Business Software Alliance, *DRM-Enabled Online Content Services in Europe and the USA*, Oct. 2005, http://www.contentconference.at/images/bsa.pdf.

zones of concern outlined above with special attention on the exception regime.[265]

Principle 5: Set the default rule in such a way that the proponents of a more protective anti-circumvention regime bear the burden of proof. As noted, experiences with anti-circumvention legislation so far have not (or at best, only partly) been aligned with its raison d'être. Instead, attention has been drawn to unintended consequences. This situation requires that the proponents advocating in favor of a more protective regime (i.e., a regime that increases, along the spectrum set by international obligations, the constraints on a user's behavior) must provide evidence why additional protections for TPM—e.g., in the form of broader scope, narrower exceptions, more severe penalties, or the like—are necessary.

With these principles in mind, the following outline of a model anti-circumvention law might provide a helpful structure for policy-makers that allows them to systematically discuss the availability[266] and feasibility of the various options and approaches, and to make deliberative determinations about the design of the complex and intertwined components of the TPM protection framework.

2. Contours of a Model Law[267]

Overview

Section 1: Definitions

Section 2: Protection of technological measures protecting works other than software

---

[265] *See* Gwen Hinze, *Seven Lessons from a Comparison of the Technological Protection Measure Provisions of the FTAA, the DMCA, and Recent Bilateral Free Trade Agreements*, http://www.eff.org/IP/FTAA/?f=tpm_implementation.html (including a suggestion regarding the appropriate standard for the burden of proof for exemption proponents).

[266] *See supra* Part II.B.

[267] The following outline must be read in the context of the design principles mentioned in the previous section and against the set of options and approaches outlined in Part II of this Article.

Section 3: Protection of technological measures protecting software

Section 4: Prohibition of certain acts preparatory to acts prohibited under Sections 2 and 3

Section 5: Common exception

Section 6: Protection of rights-management information

Section 7: Civil and criminal sanctions

Section 8: Prohibition against the derogation from permitted circumventions

Section 9: Liability for technical protection measures

Section 10: Consumer information

Section 11: Specific limitations on the use of technological protection measures

Section 12: Market abuse by the use of technical protection measures

Section 13: Review processes and reporting

Section 1: Definitions

The definition of core concepts and terms is among the core elements of any anti-circumvention law. The specification of concepts and terms should be in accordance with Principle 1 outlined above. The definitions of the following terms require special attention:

(a) "Technical Protection Measures"

The definition of this term is crucial in order to determine the scope of protection of technical measures. If necessary, the definition must differentiate between access controls and the protection of other rights of a copyright owner, including copy controls. Another question is whether analog measures should also be included.

(b) "Effectiveness"

The concept of an "effective" TPM should be specified. Substantively, a TPM should only be deemed effective:

(1) if it functions properly,

(2) if it can only be disabled intentionally and with considerable difficulty, and

(3) if no easier means exist to achieve the effect the measure attempts to prevent.

(c) "Circumvention"

Elements:

(1) purpose of gaining access to or using a copyrighted work;

(2) act is not authorized by the rightholder; nor

(3) permitted by law.

Section 2: Protection of technological measures protecting works other than software

This section sets out under what circumstances the circumvention of technological protection measures is prohibited. Subsection (a) defines the circumstances under which circumvention is prohibited, whereas subsection (b) enumerates a list of possible exceptions in accordance with design Principle 2 mentioned above.

(a) Principle

Prohibition of acts of circumvention of all or some types of effective technological protection measures which protect copyrighted works. In addition, the following issues, among others, must be considered:

(1) What types of effective technical protection measures (e.g., access controls or copy protection) should be protected?

(2) Should the protection be congruent with the scope of copyright protection?

(b) Exceptions

In accordance with Principle 2, it is crucial to specify the exceptions applicable to anti-circumvention provisions. In

civil law jurisdictions, exceptions may include, inter alia, the following ones:

(1) Reproduction:

– On paper or a similar medium, including the printing out of digital works

– On any medium made by a natural person for private use and for non-commercial purposes

– On any medium for making back-up copies

(2) Particular uses:

– Circumvention for format shifting of copyrighted material

(3) Educational and other social uses:

– Circumvention for use within educational and non-commercial scientific institutions

– Circumvention for the benefit of the disabled

– Circumvention for use by private or public non-profit libraries, museums and archives

– Circumvention for broadcasting on the part of social institutions, such as hospitals and prisons

(4) Uses in a cultural and free speech context:

– Circumvention for producing derivative works, including mash-ups, fan fiction, etc., provided that the latter are not exploited commercially

– Circumvention for producing caricatures, parodies, pastiches

– Circumvention for quotations, for purposes such as criticism, review or news reporting

– Circumvention for the inclusion of copyrighted material in broadcasts and the reproduction of copyrighted material for broadcasting purposes

– Circumvention for use during religious celebrations

(5) Uses in the interest of the State, e.g.:

– Circumvention in order to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings

– Circumvention for use during official celebrations

(6) Useless or harmful TPM:

– Circumvention for the use of seemingly abandoned works

– Circumvention where a TPM is obsolete, lost, damaged, defective, malfunctioning, or unusable, and where support or a replacement TPM is not provided

– Circumvention where a TPM interferes with, damages, or causes damage or a malfunction to a product

– Circumvention for the purposes of repairing a product

Section 3: Protection of technological measures protecting software

(a) Principle

See above, comment to section 2(a)

(b) Exceptions

(1) Copying

– Circumvention for making back-up copies of computer programs

– Circumvention for temporary copying

(2) Software engineering

– Circumvention for achieving interoperability between computer programs or computer programs and data

– Circumvention for error correction

– Circumvention for reverse engineering

(3) Circumvention for the use of seemingly abandoned computer programs ("abandonware")

Section 4: Prohibition of certain acts preparatory to acts prohibited under Sections 2 and 3

This section should be drafted very carefully, as it is the most likely to produce unintended effects on autonomy and participation, competition, and innovation.

(a) Prohibition of preparatory acts

The prohibited acts shall be defined and specified, respectively, in great detail and unambiguous terms (see Principle 1.)

(b) No mandate provision

This provision—similar to section 1201(c)(3) of the DMCA and recital 48 of the EUCD—clarifies that the prohibition of circumvention devices does not require manufacturers of computers, consumer electronics, and telecommunications products to design their products affirmatively to respond to any particular technological measure.

Section 5: General non-infringing or legitimate purpose exception

Acts of circumvention of effective TPM and the preparatory acts mentioned in section 4 should not be illegal if they are conducted for legitimate and non-infringing uses of protected works (including, e.g., research into encryption).

Section 6: Protection of rights-management information

Excluded from the scope of this study, but mentioned *pro memoria*.

Section 7: Civil and criminal sanctions

The sanctions for the circumvention of effective TPM prohibited under sections 2 and 3 should be carefully crafted according to Principle 3 outlined above and synchronized with existing (civil or criminal) sanctions for copyright infringement.

This section should also incorporate an actual knowledge standard. As to preparatory acts, criminal sanctions should only apply to willful and commercial preparatory acts, whereas negligent or non-commercial acts should only be subject to civil liability. In designing appropriate and proportionate sanctions, it is absolutely necessary to take the particular features of the applicable procedural law into account.

Section 8: Prohibition against the derogation from permitted circumventions

Rightsholders often use their bargaining power to prohibit the circumvention of TPM via terms of service agreements, end-user license agreements (EULAs), or other contractual agreements in situations where the law does not prohibit an act of circumvention. In order to restore the balance, it is necessary to address the copyright-TPM-contract interface and make sure that contractual agreements cannot waive the available copyright exceptions and defenses.

Section 9: Liability for technical protection measures

Those who use technical measures protected by this law should be held liable for the damage such measures may cause to those using products protected by them. This section thus complements the prevailing law of torts. As in the previous section, it is of utmost importance to take into account the remedies available and the applicable procedural law when designing these rules. More concretely, liability for TPM should be established if a technical protection measure (be it effective or not) causes harm to the work protected by it or to a device normally used to exercise enjoyment of the TPM-protected work.

Section 10: Consumer information

In order to ensure consumer choice, users must be informed if a product or service is protected by technological measures. This section defines minimum information requirements for vendors and providers, respectively.

Section 11: Specific limitations on the use of technological protection measures

This section sets out under what circumstances the application of technological protection measures is limited. A good example of such a provision is the interoperability clause in the revised French Copyright Law, which requires that:

> …[t]out éditeur de logiciel, tout fabricant de système technique et tout exploitant de service peut, en cas de refus d'accès aux informations essentielles à l'interopérabilité, demander à l'Autorité de régulation des mesures techniques de garantir l'interopérabilité des systèmes et des services existants, dans le respect des droits des parties, et d'obtenir du titulaire des droits sur la mesure technique les informations essentielles à cette interopérabilité.[268]

Section 12: Market abuse by the use of technical protection measures

As discussed above, TPM in combination with anti-circumvention provisions can be strategically misused by rightholders to hinder legitimate competition. Thus, it is necessary to provide for measures to combat such abuses in accordance with the principles of the general competition law of the relevant jurisdiction.

Section 13: Review process and reporting

As noted in the previous section and in the context of design Principle 4, it is crucial to incorporate a review process. Possible options are: legislative, administrative, or academic reviews and reporting obligations. The review, inter alia, shall examine whether the desired level of protection is achieved, whether acts that are traditionally permitted by law are adversely affected under the TPM regime, and what the regime's impact on competition and innovation is.

---

[268] *See* Assemblée Nationale, art. 14, http://www.assemblee-nationale.fr/12/ta/ta0596.asp. Roughly translated:

> …software editors, manufacturers of technical systems and service owners may, when refused access to essential interoperability information, petition the Authority for the regulation of technical measures to guarantee the interoperability of systems and existing services, with respect to parties' rights, and obtain from the rightsholder of the technical measure the essential information for this interoperability.

C. Conclusion

Societies and governments around the globe are currently in the process of revisiting their national policies and legal regimes that govern the respective information environments as components of a global information ecosystem. In this process, the question of "ownership" of and "control" over information, knowledge, and entertainment plays an important role. The past ten years have been characterized by an intense and intensifying struggle over the reallocation of monopoly rights in information among the various stakeholders under the post-modern conditions of cyberspace. In response to the disruptive power of the new information and communication technology, rightholders have developed and, on a large scale applied, new technological methods of content protection, also known as technological protection measures. In addition, the rightsholders—exposed to an arms race between copyright and copyleft—have successfully lobbied both at the international as well as the national level for a third layer of protection, i.e., anti-circumvention legislation, which in important respects has changed the traditional balance between the interests of rightholders on the one hand and users as well as the public at large on the other hand. Although it might not be realistic at this point in time to abolish this new type of legislation, it is crucial for policy-makers to understand that *choices can be made*. Choices have been the theme of this Article. First, it has demonstrated that countries, even if bound by international Internet treaty law or bilateral trade agreements, in fact do have significant discretion as to how they craft their respective legal frameworks. Second, it has mapped and discussed in some detail the key options that are available and compared alternative approaches that have been taken so far. As a contribution towards the quest for the best legislative practice model, the Article finally suggested basic design principles and provided the outline of a model law with issues that need to be addressed by national legislators in a situation of increased uncertainty regarding the (side-)effects of legislative action.